



Guía GuardDuty del usuario de Amazon

# Amazon GuardDuty



# Amazon GuardDuty: Guía GuardDuty del usuario de Amazon

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

# Table of Contents

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| ¿Qué es GuardDuty? .....                                                                     | 1  |
| Características de GuardDuty .....                                                           | 2  |
| Conformidad con DSS de PCI .....                                                             | 7  |
| Precios en GuardDuty .....                                                                   | 7  |
| Uso de una GuardDuty prueba gratuita de 30 días .....                                        | 7  |
| Uso de la protección contra malware para S3 con la capa gratuita .....                       | 9  |
| Accediendo GuardDuty .....                                                                   | 9  |
| Conceptos y términos clave .....                                                             | 11 |
| Introducción .....                                                                           | 17 |
| Antes de empezar .....                                                                       | 17 |
| Paso 1: Habilita Amazon GuardDuty .....                                                      | 20 |
| Paso 2: generación de resultados de muestra y exploración de las operaciones básicas .....   | 22 |
| Paso 3: Configurar la exportación de GuardDuty los resultados a un bucket de Amazon S3 ..... | 23 |
| Paso 4: Configurar la GuardDuty búsqueda de alertas a través de las redes sociales .....     | 29 |
| Siguiendo pasos .....                                                                        | 31 |
| Orígenes de datos fundamentales .....                                                        | 33 |
| AWS CloudTrail eventos de gestión .....                                                      | 33 |
| ¿Cómo GuardDuty gestiona los eventos AWS CloudTrail globales .....                           | 34 |
| Logs de flujo de VPC .....                                                                   | 35 |
| Registros de consultas de DNS de Route53 Resolver .....                                      | 36 |
| Detección Extendida de Amenazas .....                                                        | 37 |
| Ejemplos de escenarios de amenazas en la secuencia de ataque .....                           | 37 |
| Cómo funciona la Detección Extendida de Amenazas .....                                       | 38 |
| Habilitar planes de protección para maximizar la detección de amenazas .....                 | 39 |
| Detección de secuencias de ataque en clústeres de Amazon EKS .....                           | 40 |
| Detección de secuencias de ataques en los buckets de Amazon S3 .....                         | 41 |
| Detección de secuencias de ataques en clústeres de Amazon ECS .....                          | 42 |
| Detección de secuencias de ataques en grupos de instancias de Amazon EC2 .....               | 43 |
| Detección de amenazas ampliada en la consola GuardDuty .....                                 | 44 |
| Descripción y administración de resultados de secuencias de ataques .....                    | 44 |
| Recursos adicionales .....                                                                   | 44 |
| Planes de protección .....                                                                   | 46 |
| Descripción general de .....                                                                 | 46 |
| Configuración de todos los planes de protección .....                                        | 47 |

|                                                                                                                            |     |
|----------------------------------------------------------------------------------------------------------------------------|-----|
| Auto-enable opciones .....                                                                                                 | 47  |
| Configuración de supervisión del tiempo de ejecución .....                                                                 | 48  |
| Restricciones bidireccionales .....                                                                                        | 48  |
| Estadísticas de la organización .....                                                                                      | 49  |
| Integración de la página de cuentas .....                                                                                  | 49  |
| EKS Protection .....                                                                                                       | 50  |
| Registros de auditoría de EKS en EKS Protection .....                                                                      | 51  |
| Habilitar EKS Protection en entornos de varias cuentas .....                                                               | 52  |
| Habilitar EKS Protection para una cuenta independiente .....                                                               | 59  |
| S3 Protection .....                                                                                                        | 61  |
| AWS CloudTrail eventos de datos para S3 .....                                                                              | 62  |
| ¿Cómo GuardDuty utiliza CloudTrail los eventos de datos para S3? .....                                                     | 62  |
| GuardDuty usar eventos CloudTrail de datos de S3 para secuencias de ataque .....                                           | 63  |
| Habilitar la protección de S3 en entornos de varias cuentas .....                                                          | 63  |
| Habilitar la S3 Protection para una cuenta independiente .....                                                             | 71  |
| Supervisión en tiempo de ejecución .....                                                                                   | 73  |
| Funcionamiento .....                                                                                                       | 74  |
| Con clústeres de Amazon EKS .....                                                                                          | 76  |
| Con instancias de Amazon EC2 .....                                                                                         | 81  |
| Con Fargate (solo Amazon ECS) .....                                                                                        | 84  |
| Después de habilitar la supervisión en tiempo de ejecución .....                                                           | 87  |
| Prueba gratuita de 30 días .....                                                                                           | 88  |
| Estoy utilizando el período de GuardDuty prueba o nunca he activado EKS Runtime Monitoring .....                           | 89  |
| Habilité la supervisión en tiempo de ejecución de EKS antes del lanzamiento de la supervisión en tiempo de ejecución ..... | 90  |
| Requisitos previos .....                                                                                                   | 91  |
| Para la instancia de EC2 .....                                                                                             | 91  |
| Para el clúster de Fargate (solo ECS) .....                                                                                | 97  |
| Para el clúster de EKS .....                                                                                               | 103 |
| Habilitación de la supervisión en tiempo de ejecución .....                                                                | 108 |
| Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas .....                                   | 108 |
| Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente .....                                        | 113 |
| Administrar agentes GuardDuty de seguridad .....                                                                           | 114 |
| Agente automatizado en el recurso de Amazon EC2 .....                                                                      | 114 |
| Administración manual del agente para el recurso de Amazon EC2 .....                                                       | 128 |



|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Agente automatizado en Fargate (solo Amazon ECS) .....                           | 144 |
| Agente automatizado en el recurso de Amazon EKS .....                            | 180 |
| Administración manual del agente para el clúster de Amazon EKS .....             | 218 |
| Configurar los parámetros del complemento de EKS .....                           | 227 |
| Validar la configuración del punto de conexión de VPC .....                      | 230 |
| Problemas de la cobertura en tiempo de ejecución y resolución de problemas ..... | 232 |
| Cobertura y resolución de problemas para los recursos de Amazon EC2 .....        | 233 |
| Cobertura y solución de problemas para clústeres de Amazon ECS .....             | 250 |
| Cobertura y resolución de problemas para los clústeres de Amazon EKS .....       | 266 |
| Configuración de la supervisión de la CPU y la memoria .....                     | 282 |
| Uso de VPC compartida .....                                                      | 283 |
| Funcionamiento .....                                                             | 284 |
| Requisitos previos .....                                                         | 286 |
| Utilizar laC con agentes automatizados .....                                     | 287 |
| Información general sobre el gráfico de dependencia de recursos de laC .....     | 287 |
| Problema común: eliminar recursos en laC .....                                   | 288 |
| Tipos de eventos de tiempo de ejecución recopilados .....                        | 289 |
| Eventos de procesos .....                                                        | 290 |
| Eventos de contenedores .....                                                    | 292 |
| AWS Fargate Eventos de tareas (solo en Amazon ECS) .....                         | 292 |
| Eventos de pod de Kubernetes .....                                               | 293 |
| Eventos del sistema de nombres de dominio (DNS) .....                            | 294 |
| Eventos abiertos .....                                                           | 295 |
| Evento de carga de módulo .....                                                  | 295 |
| Eventos de Mprotect .....                                                        | 295 |
| Eventos de montaje .....                                                         | 296 |
| Eventos de enlace .....                                                          | 296 |
| Eventos de enlace simbólico .....                                                | 297 |
| Eventos duplicados .....                                                         | 297 |
| Evento de mapa de memoria .....                                                  | 298 |
| Eventos de socket .....                                                          | 298 |
| Eventos de conexión .....                                                        | 299 |
| Eventos de Readv de VM de proceso .....                                          | 300 |
| Eventos de Writev de VM de proceso .....                                         | 300 |
| Eventos de rastreo de procesos (Ptrace) .....                                    | 301 |
| Enviar de vinculación .....                                                      | 301 |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| Eventos de escucha .....                                                                             | 302 |
| Eventos de cambio de nombre .....                                                                    | 303 |
| Eventos de establecimiento de ID de usuario (UID) .....                                              | 303 |
| Eventos chmod .....                                                                                  | 304 |
| Agente de alojamiento GuardDuty de repositorios Amazon ECR .....                                     | 304 |
| Repositorio ECR para EKS v1.15.0 - 1.8.1 (eks.build.2) .....                                         | 304 |
| Repositorio ECR para la versión EKS 1.8.1.eks.build.1 .....                                          | 310 |
| Repositorio de ECR para el agente de seguridad en AWS Fargate (solo Amazon ECS) .....                | 312 |
| Agentes de seguridad en el mismo host .....                                                          | 316 |
| Descripción general de .....                                                                         | 316 |
| Impact .....                                                                                         | 317 |
| ¿Cómo GuardDuty gestiona varios agentes .....                                                        | 317 |
| Supervisión en tiempo de ejecución de EKS .....                                                      | 318 |
| Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas (API) ..... | 319 |
| Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente (API) .....    | 361 |
| Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución ..... | 368 |
| GuardDuty versiones de lanzamiento del agente de seguridad .....                                     | 373 |
| Recursos adicionales: próximos pasos .....                                                           | 409 |
| Desactivar, desinstalar y limpiar recursos .....                                                     | 409 |
| Desinstalar manualmente el agente de seguridad para los recursos de Amazon EC2 .....                 | 411 |
| Limpiar los recursos de los agentes de seguridad .....                                               | 413 |
| Malware Protection for EC2 .....                                                                     | 415 |
| Comparación entre el escaneo de GuardDuty-initiated malware y el escaneo de On-demand malware .....  | 416 |
| ¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware? .....                            | 419 |
| Volúmenes de EBS compatibles .....                                                                   | 420 |
| Modificar el ID de clave de KMS predeterminada .....                                                 | 421 |
| Configure la retención de instantáneas y la cobertura de análisis de EC2 .....                       | 422 |
| Retención de instantáneas .....                                                                      | 423 |
| Opciones de análisis con etiquetas definidas por el usuario .....                                    | 424 |
| Etiqueta GuardDutyExcluded global .....                                                              | 428 |
| GuardDuty-initiated análisis de malware .....                                                        | 429 |
| Prueba gratuita de 30 días .....                                                                     | 430 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Habilitar la detección de GuardDuty-initiated malware en entornos con varias cuentas .....       | 431 |
| Habilitar el análisis de GuardDuty-initiated malware para una cuenta independiente .....         | 442 |
| Hallazgos que invocan un análisis de GuardDuty-initiated malware .....                           | 444 |
| On-demand escaneo de malware .....                                                               | 446 |
| Cómo funciona el análisis de On-demand malware .....                                             | 447 |
| Iniciar el análisis de On-demand malware .....                                                   | 448 |
| Re-scanning instancia de Amazon EC2 previamente escaneada .....                                  | 451 |
| Supervisión de los estados y resultados de los análisis de malware .....                         | 451 |
| GuardDuty cuenta de servicio .....                                                               | 453 |
| Cuotas en la protección contra malware de EC2 .....                                              | 457 |
| Protección contra malware para S3 .....                                                          | 462 |
| Precios y costo de uso .....                                                                     | 464 |
| Revisar el costo de uso .....                                                                    | 465 |
| Funcionamiento .....                                                                             | 466 |
| Descripción general de .....                                                                     | 466 |
| Permisos de roles de IAM .....                                                                   | 466 |
| Etiquetado opcional de objetos en función del resultado del análisis .....                       | 466 |
| Proceso posterior a la habilitación de la protección contra malware para S3 para un bucket ..... | 467 |
| Capacidades de la protección contra malware para S3 .....                                        | 469 |
| (Opcional) Comience a utilizar la protección contra malware para S3 únicamente (consola) .....   | 471 |
| Configurar la protección contra malware para S3 para el bucket .....                             | 472 |
| Habilitar la protección contra malware para la detección de amenazas de S3 para el bucket .....  | 473 |
| Permisos de roles de IAM .....                                                                   | 479 |
| Solución de problemas de errores de permisos de roles de IAM .....                               | 485 |
| Pasos a seguir tras habilitar la protección contra malware para S3 .....                         | 486 |
| On-demand Escaneo de malware S3 .....                                                            | 487 |
| Requisitos previos .....                                                                         | 488 |
| Inicie un análisis de malware bajo demanda .....                                                 | 488 |
| Utilizar el control de acceso basado en etiquetas (TBAC) .....                                   | 489 |
| Agregar TBAC en el recurso del bucket de S3 .....                                                | 489 |
| Ver y entender el estado del bucket protegido .....                                              | 492 |
| Supervisión de los análisis de objetos de S3 .....                                               | 493 |
| Estado potencial de análisis de objeto de S3 y estado del producto .....                         | 493 |
| Uso de Amazon EventBridge .....                                                                  | 497 |

|                                                                                   |     |
|-----------------------------------------------------------------------------------|-----|
| Utilizar etiquetas de objetos de S3 .....                                         | 507 |
| Uso de CloudWatch alarmas y métricas .....                                        | 508 |
| Resolución de problemas .....                                                     | 511 |
| Solución de problemas sobre el estado del plan de protección contra malware ..... | 512 |
| Solución de problemas de análisis de malware bajo demanda .....                   | 516 |
| Editar el plan de protección contra malware para un bucket protegido .....        | 516 |
| Desactivar la protección contra malware para S3 para un bucket protegido .....    | 518 |
| Compatibilidad con las características de Amazon S3 .....                         | 519 |
| Protección contra malware para las cuotas de S3 .....                             | 528 |
| Protección contra malware para AWS Backup .....                                   | 532 |
| Descripción general de .....                                                      | 532 |
| Funcionamiento .....                                                              | 535 |
| Descripción general de .....                                                      | 532 |
| Se requiere el rol de IAM para el escaneo .....                                   | 537 |
| Revisión del estado y el resultado del análisis de los recursos .....             | 537 |
| Revisar los resultados generados .....                                            | 537 |
| Permisos de rol de IAM .....                                                      | 538 |
| Se proporcionó un rol de cliente para el análisis de malware .....                | 538 |
| Detalles sobre los permisos .....                                                 | 539 |
| Asegurar el rol .....                                                             | 540 |
| Cómo utiliza GuardDuty Malware Protection las subvenciones en AWS KMS .....       | 540 |
| GuardDuty Contexto de cifrado y protección contra malware .....                   | 541 |
| Política de permisos y confianza para el rol .....                                | 542 |
| Comience de forma independiente .....                                             | 546 |
| Pasos para empezar a usar Malware Protection for Backup .....                     | 546 |
| Inicio de escaneos bajo demanda .....                                             | 547 |
| Consola .....                                                                     | 547 |
| API/CLI .....                                                                     | 548 |
| Supervisión de los estados y resultados de los análisis de malware .....          | 548 |
| Protección contra malware para Backup Quotas .....                                | 557 |
| Protección de RDS .....                                                           | 561 |
| Bases de datos compatibles .....                                                  | 563 |
| Actividad de inicio de sesión de RDS .....                                        | 564 |
| Habilitar RDS Protection en entornos de varias cuentas .....                      | 564 |
| Habilitar RDS Protection para una cuenta independiente .....                      | 571 |
| Solución de problemas de monitoreo de protección de RDS .....                     | 572 |

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Almacenamiento de RDS completo .....                                                   | 572 |
| Versiones no compatibles en la base de datos principal de RDS para PostgreSQL .....    | 573 |
| Consideraciones adicionales de seguridad .....                                         | 574 |
| Protección de Lambda .....                                                             | 575 |
| Supervisión de la actividad de red de Lambda .....                                     | 576 |
| Habilitar la protección de Lambda en entornos de varias cuentas .....                  | 576 |
| Habilitar la protección de Lambda para una cuenta independiente .....                  | 584 |
| Proteger las cargas de trabajo de IA .....                                             | 586 |
| Varias cuentas en GuardDuty .....                                                      | 587 |
| Relaciones entre la cuenta de administrador y la cuenta de miembro .....               | 588 |
| Administración de cuentas con AWS Organizations .....                                  | 592 |
| Recomendaciones y consideraciones .....                                                | 593 |
| Permisos necesarios para designar una cuenta de GuardDuty administrador delegado ..... | 595 |
| Designación de una cuenta de administrador delegado GuardDuty .....                    | 597 |
| Configuración de las preferencias de habilitación automática de la organización .....  | 599 |
| Cómo agregar miembros a la organización .....                                          | 603 |
| (Opcional) Habilitar planes de protección para cuentas de miembro existentes .....     | 605 |
| Administre continuamente sus cuentas de miembros dentro GuardDuty .....                | 606 |
| Suspensión GuardDuty para la cuenta de un miembro .....                                | 607 |
| Desasociar (eliminar) la cuenta de miembro de la cuenta de administrador .....         | 609 |
| Eliminar las cuentas de los miembros de GuardDuty la organización .....                | 611 |
| Cambiar la cuenta de administrador delegado GuardDuty .....                            | 612 |
| Administración de cuentas por invitación .....                                         | 615 |
| Agregar cuentas por invitación .....                                                   | 616 |
| Consolidación de cuentas de administrador bajo una sola organización .....             | 621 |
| GuardDuty consideraciones sobre la opción Exportar CSV en las cuentas .....            | 624 |
| Tipos de resultados .....                                                              | 625 |
| Tipos de resultados de EC2 .....                                                       | 625 |
| Backdoor:EC2/C&CAActivity.B .....                                                      | 627 |
| Backdoor:EC2/C&CAActivity.B!DNS .....                                                  | 628 |
| Backdoor:EC2/DenialOfService.Dns .....                                                 | 629 |
| Backdoor:EC2/DenialOfService.Tcp .....                                                 | 630 |
| Backdoor:EC2/DenialOfService.Udp .....                                                 | 631 |
| Backdoor:EC2/DenialOfService.UdpOnTcpPorts .....                                       | 631 |
| Backdoor:EC2/DenialOfService.UnusualProtocol .....                                     | 632 |
| Backdoor:EC2/Spambot .....                                                             | 633 |

|                                                       |     |
|-------------------------------------------------------|-----|
| Behavior:EC2/NetworkPortUnusual .....                 | 633 |
| Behavior:EC2/TrafficVolumeUnusual .....               | 634 |
| CryptoCurrency:EC2/BitcoinTool.B .....                | 634 |
| CryptoCurrency:EC2/BitcoinTool.B!DNS .....            | 635 |
| DefenseEvasion:EC2/UnusualDNSResolver .....           | 636 |
| DefenseEvasion:EC2/UnusualDoHActivity .....           | 636 |
| DefenseEvasion:EC2/UnusualDoTActivity .....           | 637 |
| Impact:EC2/AbusedDomainRequest.Reputation .....       | 638 |
| Impact:EC2/BitcoinDomainRequest.Reputation .....      | 638 |
| Impact:EC2/MaliciousDomainRequest.Reputation .....    | 639 |
| Impact:EC2/MaliciousDomainRequest.Custom .....        | 640 |
| Impact:EC2/PortSweep .....                            | 640 |
| Impact:EC2/SuspiciousDomainRequest.Reputation .....   | 641 |
| Impact:EC2/WinRMBruteForce .....                      | 642 |
| Recon:EC2/PortProbeEMRUnprotectedPort .....           | 642 |
| Recon:EC2/PortProbeUnprotectedPort .....              | 643 |
| Recon:EC2/Portscan .....                              | 644 |
| Trojan:EC2/BlackholeTraffic .....                     | 645 |
| Trojan:EC2/BlackholeTraffic!DNS .....                 | 645 |
| Trojan:EC2/DGADomainRequest.B .....                   | 646 |
| Trojan:EC2/DGADomainRequest.C!DNS .....               | 647 |
| Trojan:EC2/DNSDataExfiltration .....                  | 647 |
| Trojan:EC2/DriveBySourceTraffic!DNS .....             | 648 |
| Trojan:EC2/DropPoint .....                            | 649 |
| Trojan:EC2/DropPoint!DNS .....                        | 649 |
| Trojan:EC2/PhishingDomainRequest!DNS .....            | 650 |
| UnauthorizedAccess:EC2/MaliciousIPCaller.Custom ..... | 650 |
| UnauthorizedAccess:EC2/MetadataDNSRebind .....        | 651 |
| UnauthorizedAccess:EC2/RDPBruteForce .....            | 652 |
| UnauthorizedAccess:EC2/SSHBruteForce .....            | 653 |
| UnauthorizedAccess:EC2/TorClient .....                | 654 |
| UnauthorizedAccess:EC2/TorRelay .....                 | 655 |
| Tipos de resultados de IAM .....                      | 655 |
| CredentialAccess:IAMUser/AnomalousBehavior .....      | 656 |
| CredentialAccess:IAMUser/CompromisedCredentials ..... | 657 |
| DefenseEvasion:IAMUser/AnomalousBehavior .....        | 658 |

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| DefenseEvasion:IAMUser/BedrockLoggingDisabled .....                        | 659 |
| Discovery:IAMUser/AnomalousBehavior .....                                  | 659 |
| Exfiltration:IAMUser/AnomalousBehavior .....                               | 660 |
| Impact:IAMUser/AnomalousBehavior .....                                     | 661 |
| InitialAccess:IAMUser/AnomalousBehavior .....                              | 661 |
| PenTest:IAMUser/KaliLinux .....                                            | 662 |
| PenTest:IAMUser/ParrotLinux .....                                          | 663 |
| PenTest:IAMUser/PentooLinux .....                                          | 663 |
| Persistence:IAMUser/AnomalousBehavior .....                                | 664 |
| Policy:IAMUser/RootCredentialUsage .....                                   | 664 |
| Policy:IAMUser/ShortTermRootCredentialUsage .....                          | 665 |
| PrivilegeEscalation:IAMUser/AnomalousBehavior .....                        | 666 |
| Recon:IAMUser/MaliciousIPCaller .....                                      | 667 |
| Recon:IAMUser/MaliciousIPCaller.Custom .....                               | 667 |
| Recon:IAMUser/TorIPCaller .....                                            | 668 |
| Stealth:IAMUser/CloudTrailLoggingDisabled .....                            | 668 |
| Stealth:IAMUser/PasswordPolicyChange .....                                 | 669 |
| UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B .....                     | 669 |
| UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS ..... | 670 |
| UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS ..... | 672 |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller .....                         | 673 |
| UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom .....                  | 674 |
| UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS ..... | 674 |
| UnauthorizedAccess:IAMUser/TorIPCaller .....                               | 675 |
| Tipos de resultados de secuencias de ataque .....                          | 676 |
| AttackSequence:EKS/CompromisedCluster .....                                | 677 |
| AttackSequence:ECS/CompromisedCluster .....                                | 678 |
| AttackSequence:EC2/CompromisedInstanceGroup .....                          | 678 |
| AttackSequence:IAM/CompromisedCredentials .....                            | 680 |
| AttackSequence:S3/CompromisedData .....                                    | 680 |
| Tipos de resultados de la S3 Protection .....                              | 681 |
| Discovery:S3/AnomalousBehavior .....                                       | 683 |
| Discovery:S3/MaliciousIPCaller .....                                       | 683 |
| Discovery:S3/MaliciousIPCaller.Custom .....                                | 684 |
| Discovery:S3/TorIPCaller .....                                             | 684 |
| Exfiltration:S3/AnomalousBehavior .....                                    | 685 |

|                                                             |     |
|-------------------------------------------------------------|-----|
| Exfiltration:S3/MaliciousIPCaller .....                     | 686 |
| Impact:S3/AnomalousBehavior.Delete .....                    | 686 |
| Impact:S3/AnomalousBehavior.Permission .....                | 687 |
| Impact:S3/AnomalousBehavior.Write .....                     | 688 |
| Impact:S3/MaliciousIPCaller .....                           | 689 |
| PenTest:S3/KaliLinux .....                                  | 689 |
| PenTest:S3/ParrotLinux .....                                | 690 |
| PenTest:S3/Pentoolinux .....                                | 690 |
| Policy:S3/AccountBlockPublicAccessDisabled .....            | 691 |
| Policy:S3/BucketAnonymousAccessGranted .....                | 692 |
| Policy:S3/BucketBlockPublicAccessDisabled .....             | 692 |
| Policy:S3/BucketPublicAccessGranted .....                   | 693 |
| Stealth:S3/ServerAccessLoggingDisabled .....                | 694 |
| UnauthorizedAccess:S3/MaliciousIPCaller.Custom .....        | 694 |
| UnauthorizedAccess:S3/TorIPCaller .....                     | 695 |
| Tipos de resultados de la protección de EKS .....           | 695 |
| CredentialAccess:Kubernetes/MaliciousIPCaller .....         | 697 |
| CredentialAccess:Kubernetes/MaliciousIPCaller.Custom .....  | 698 |
| CredentialAccess:Kubernetes/SuccessfulAnonymousAccess ..... | 699 |
| CredentialAccess:Kubernetes/TorIPCaller .....               | 699 |
| DefenseEvasion:Kubernetes/MaliciousIPCaller .....           | 700 |
| DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom .....    | 701 |
| DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess .....   | 701 |
| DefenseEvasion:Kubernetes/TorIPCaller .....                 | 702 |
| Discovery:Kubernetes/MaliciousIPCaller .....                | 703 |
| Discovery:Kubernetes/MaliciousIPCaller.Custom .....         | 704 |
| Discovery:Kubernetes/SuccessfulAnonymousAccess .....        | 704 |
| Discovery:Kubernetes/TorIPCaller .....                      | 705 |
| Execution:Kubernetes/ExecInKubeSystemPod .....              | 706 |
| Impact:Kubernetes/MaliciousIPCaller .....                   | 706 |
| Impact:Kubernetes/MaliciousIPCaller.Custom .....            | 707 |
| Impact:Kubernetes/SuccessfulAnonymousAccess .....           | 708 |
| Impact:Kubernetes/TorIPCaller .....                         | 708 |
| Persistence:Kubernetes/MaliciousIPCaller .....              | 709 |
| Persistence:Kubernetes/MaliciousIPCaller.Custom .....       | 710 |
| Persistence:Kubernetes/SuccessfulAnonymousAccess .....      | 710 |



|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| Persistence:Kubernetes/TorIPCaller .....                                  | 711 |
| Policy:Kubernetes/AdminAccessToDefaultServiceAccount .....                | 712 |
| Policy:Kubernetes/AnonymousAccessGranted .....                            | 713 |
| Policy:Kubernetes/ExposedDashboard .....                                  | 713 |
| Policy:Kubernetes/KubeflowDashboardExposed .....                          | 714 |
| CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed .....       | 714 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated ..... | 715 |
| Execution:Kubernetes/AnomalousBehavior.ExecInPod .....                    | 716 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!        |     |
| PrivilegedContainer .....                                                 | 717 |
| Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!                |     |
| ContainerWithSensitiveMount .....                                         | 718 |
| Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed .....             | 719 |
| PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated .....        | 720 |
| Discovery:Kubernetes/AnomalousBehavior.PermissionChecked .....            | 721 |
| Tipos de resultados de la supervisión en tiempo de ejecución .....        | 722 |
| CryptoCurrency:Runtime/BitcoinTool.B .....                                | 724 |
| Backdoor:Runtime/C&CActivity.B .....                                      | 725 |
| UnauthorizedAccess:Runtime/TorRelay .....                                 | 726 |
| UnauthorizedAccess:Runtime/TorClient .....                                | 727 |
| Trojan:Runtime/BlackholeTraffic .....                                     | 728 |
| Trojan:Runtime/DropPoint .....                                            | 728 |
| CryptoCurrency:Runtime/BitcoinTool.B!DNS .....                            | 729 |
| Backdoor:Runtime/C&CActivity.B!DNS .....                                  | 730 |
| Trojan:Runtime/BlackholeTraffic!DNS .....                                 | 731 |
| Trojan:Runtime/DropPoint!DNS .....                                        | 732 |
| Trojan:Runtime/DGADomainRequest.C!DNS .....                               | 732 |
| Trojan:Runtime/DriveBySourceTraffic!DNS .....                             | 733 |
| Trojan:Runtime/PhishingDomainRequest!DNS .....                            | 734 |
| Impact:Runtime/AbusedDomainRequest.Reputation .....                       | 735 |
| Impact:Runtime/BitcoinDomainRequest.Reputation .....                      | 736 |
| Impact:Runtime/MaliciousDomainRequest.Reputation .....                    | 737 |
| Impact:Runtime/SuspiciousDomainRequest.Reputation .....                   | 737 |
| UnauthorizedAccess:Runtime/MetadataDNSRebind .....                        | 738 |
| Execution:Runtime/NewBinaryExecuted .....                                 | 740 |
| PrivilegeEscalation:Runtime/DockerSocketAccessed .....                    | 741 |

|                                                                    |     |
|--------------------------------------------------------------------|-----|
| PrivilegeEscalation:Runtime/RuncContainerEscape .....              | 741 |
| PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified .....      | 742 |
| DefenseEvasion:Runtime/ProcessInjection.Proc .....                 | 743 |
| DefenseEvasion:Runtime/ProcessInjection.Ptrace .....               | 744 |
| DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite .....   | 744 |
| Execution:Runtime/ReverseShell .....                               | 745 |
| DefenseEvasion:Runtime/FilelessExecution .....                     | 746 |
| Impact:Runtime/CryptoMinerExecuted .....                           | 746 |
| Execution:Runtime/NewLibraryLoaded .....                           | 747 |
| PrivilegeEscalation:Runtime/ContainerMountsHostDirectory .....     | 748 |
| PrivilegeEscalation:Runtime/UserfaultfdUsage .....                 | 748 |
| Execution:Runtime/SuspiciousTool .....                             | 749 |
| Execution:Runtime/SuspiciousCommand .....                          | 750 |
| DefenseEvasion:Runtime/SuspiciousCommand .....                     | 751 |
| DefenseEvasion:Runtime/PtraceAntiDebugging .....                   | 752 |
| Execution:Runtime/MaliciousFileExecuted .....                      | 753 |
| Execution:Runtime/MaliciousFileExecuted.Custom .....               | 753 |
| Execution:Runtime/SuspiciousShellCreated .....                     | 754 |
| PrivilegeEscalation:Runtime/ElevationToRoot .....                  | 755 |
| Discovery:Runtime/SuspiciousCommand .....                          | 756 |
| Persistence:Runtime/SuspiciousCommand .....                        | 757 |
| PrivilegeEscalation:Runtime/SuspiciousCommand .....                | 758 |
| DefenseEvasion:Runtime/KernelModuleLoaded .....                    | 758 |
| Tipos de resultados de la protección contra malware para EC2 ..... | 759 |
| Execution:EC2/MaliciousFile .....                                  | 760 |
| Execution:ECS/MaliciousFile .....                                  | 760 |
| Execution:Kubernetes/MaliciousFile .....                           | 761 |
| Execution:Container/MaliciousFile .....                            | 761 |
| Execution:EC2/SuspiciousFile .....                                 | 762 |
| Execution:ECS/SuspiciousFile .....                                 | 762 |
| Execution:Kubernetes/SuspiciousFile .....                          | 763 |
| Execution:Container/SuspiciousFile .....                           | 764 |
| Tipo de resultado de la protección contra malware para S3 .....    | 765 |
| Object:S3/MaliciousFile .....                                      | 765 |
| Tipos de búsqueda de Malware Protection for Backup .....           | 765 |
| Execution:EC2/MaliciousFile!Snapshot .....                         | 766 |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| Execution:EC2/MaliciousFile!AMI .....                             | 766 |
| Execution:EC2/MaliciousFile!RecoveryPoint .....                   | 767 |
| Execution:S3/MaliciousFile!RecoveryPoint .....                    | 767 |
| Tipos de resultados de la protección de RDS .....                 | 768 |
| CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin .....      | 768 |
| CredentialAccess:RDS/AnomalousBehavior.FailedLogin .....          | 770 |
| CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce ..... | 771 |
| CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin .....      | 772 |
| CredentialAccess:RDS/MaliciousIPCaller.FailedLogin .....          | 772 |
| Discovery:RDS/MaliciousIPCaller .....                             | 773 |
| CredentialAccess:RDS/TorIPCaller.SuccessfulLogin .....            | 774 |
| CredentialAccess:RDS/TorIPCaller.FailedLogin .....                | 774 |
| Discovery:RDS/TorIPCaller .....                                   | 775 |
| Tipos de resultados de la protección de Lambda .....              | 776 |
| Backdoor:Lambda/C&CActivity.B .....                               | 776 |
| CryptoCurrency:Lambda/BitcoinTool.B .....                         | 777 |
| Trojan:Lambda/BlackholeTraffic .....                              | 778 |
| Trojan:Lambda/DropPoint .....                                     | 778 |
| UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom .....          | 779 |
| UnauthorizedAccess:Lambda/TorClient .....                         | 779 |
| UnauthorizedAccess:Lambda/TorRelay .....                          | 780 |
| Tipos de resultados retirados .....                               | 780 |
| PrivilegeEscalation:Kubernetes/PrivilegedContainer .....          | 781 |
| Persistence:Kubernetes/ContainerWithSensitiveMount .....          | 782 |
| Exfiltration:S3/ObjectRead.Unusual .....                          | 783 |
| Impact:S3/PermissionsModification.Unusual .....                   | 783 |
| Impact:S3/ObjectDelete.Unusual .....                              | 784 |
| Discovery:S3/BucketEnumeration.Unusual .....                      | 785 |
| Persistence:IAMUser/NetworkPermissions .....                      | 786 |
| Persistence:IAMUser/ResourcePermissions .....                     | 786 |
| Persistence:IAMUser/UserPermissions .....                         | 787 |
| PrivilegeEscalation:IAMUser/AdministrativePermissions .....       | 788 |
| Recon:IAMUser/NetworkPermissions .....                            | 789 |
| Recon:IAMUser/ResourcePermissions .....                           | 790 |
| Recon:IAMUser/UserPermissions .....                               | 790 |
| ResourceConsumption:IAMUser/ComputeResources .....                | 791 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Stealth:IAMUser/LoggingConfigurationModified .....                             | 792 |
| UnauthorizedAccess:IAMUser/ConsoleLogin .....                                  | 793 |
| UnauthorizedAccess:EC2/TorIPCaller .....                                       | 793 |
| Backdoor:EC2/XORDDOS .....                                                     | 794 |
| Behavior:IAMUser/InstanceLaunchUnusual .....                                   | 794 |
| CryptoCurrency:EC2/BitcoinTool.A .....                                         | 795 |
| UnauthorizedAccess:IAMUser/UnusualASNCaller .....                              | 795 |
| GuardDuty buscar tipos por recursos potencialmente afectados .....             | 796 |
| GuardDuty tipos de búsqueda activos .....                                      | 796 |
| Comprender y generar resultados .....                                          | 820 |
| GuardDuty formato de búsqueda .....                                            | 821 |
| Propósitos de amenaza .....                                                    | 823 |
| GuardDuty motor de escaneo de detección de malware .....                       | 826 |
| Ejemplos de hallazgos .....                                                    | 826 |
| Generar ejemplos de resultados a través de la GuardDuty consola o la API ..... | 827 |
| GuardDuty Resultados de las pruebas .....                                      | 828 |
| Consideraciones .....                                                          | 829 |
| GuardDuty hallazgos que el script del probador puede generar .....             | 830 |
| Paso 1: Requisitos previos .....                                               | 832 |
| Paso 2: Despliegue AWS los recursos .....                                      | 833 |
| Paso 3: Ejecute los scripts de la herramienta de pruebas .....                 | 835 |
| Paso 4: Limpiar los recursos AWS de prueba .....                               | 837 |
| Solución de problemas comunes de .....                                         | 838 |
| Página de hallazgos en la GuardDuty consola .....                              | 839 |
| Navegación en la página Resultados .....                                       | 841 |
| Niveles de gravedad de los resultados .....                                    | 842 |
| Gravedad crítica .....                                                         | 843 |
| Gravedad alta .....                                                            | 843 |
| Gravedad media .....                                                           | 843 |
| Gravedad baja .....                                                            | 844 |
| Detalles de los resultados .....                                               | 844 |
| Información general de los resultados .....                                    | 845 |
| Recurso .....                                                                  | 846 |
| Detalles de los resultados de la secuencia de ataque .....                     | 854 |
| Detalles de usuario de la base de datos (DB) de RDS .....                      | 861 |
| Detalles del resultado de la supervisión en tiempo de ejecución .....          | 862 |

|                                                                           |     |
|---------------------------------------------------------------------------|-----|
| Detalles del análisis de volúmenes de EBS .....                           | 864 |
| Detalles de los resultados de Malware Protection for EC2 .....            | 865 |
| Detalles de los resultados de la protección contra malware para S3 .....  | 866 |
| Action .....                                                              | 867 |
| Actor u objetivo .....                                                    | 869 |
| Detalles de geolocalización .....                                         | 870 |
| Información adicional .....                                               | 870 |
| Evidencia .....                                                           | 870 |
| Comportamiento anómalo .....                                              | 871 |
| GuardDuty encontrar agregación .....                                      | 876 |
| Gestionar GuardDuty los hallazgos .....                                   | 878 |
| GuardDuty Panel de resumen .....                                          | 879 |
| Descripción general de .....                                              | 880 |
| Hallazgos .....                                                           | 881 |
| Tipos de resultados más comunes .....                                     | 882 |
| Resultados por gravedad .....                                             | 882 |
| Cuentas con la mayoría de los resultados .....                            | 883 |
| Recursos con resultados .....                                             | 883 |
| Resultados menos frecuentes .....                                         | 884 |
| Cobertura de los planes de protección .....                               | 884 |
| Filtrar GuardDuty los hallazgos .....                                     | 885 |
| Crear y guardar el conjunto de filtros en la GuardDuty consola .....      | 886 |
| Crear y guardar un conjunto de filtros mediante GuardDuty API y CLI ..... | 888 |
| La propiedad filtra GuardDuty .....                                       | 890 |
| Reglas de supresión .....                                                 | 924 |
| Uso de reglas de supresión con Detección Extendida de Amenazas .....      | 925 |
| Casos de uso comunes para reglas de supresión y ejemplos .....            | 925 |
| Crear reglas de supresión .....                                           | 929 |
| Actualización de las reglas de supresión .....                            | 934 |
| Eliminación de reglas de supresión .....                                  | 937 |
| Listas de entidades y listas de direcciones IP .....                      | 938 |
| Comprender las listas de entidades y listas de direcciones IP .....       | 939 |
| Consideraciones importantes para GuardDuty las listas .....               | 940 |
| Formatos de las listas .....                                              | 941 |
| Explicación de los estados de las listas .....                            | 950 |

|                                                                                                       |      |
|-------------------------------------------------------------------------------------------------------|------|
| Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP ..... | 950  |
| Añadir y activar una lista de entidades o una lista de IP .....                                       | 953  |
| Actualización de una lista de entidades o una lista de direcciones IP .....                           | 959  |
| De-activating lista de entidades o lista de direcciones IP .....                                      | 964  |
| Eliminar la lista de entidades o la lista de direcciones IP .....                                     | 967  |
| Exportar los resultados generados a Amazon S3 .....                                                   | 970  |
| Consideraciones .....                                                                                 | 970  |
| Paso 1: Permisos necesarios para la exportación de resultados .....                                   | 971  |
| Paso 2: Asociar la política a la clave de KMS .....                                                   | 972  |
| Paso 3: Asociar la política al bucket de Amazon S3 .....                                              | 974  |
| Paso 4: Exportar resultados a un bucket de S3 (consola) .....                                         | 978  |
| Paso 5: Frecuencia de exportación de los resultados .....                                             | 979  |
| Procesando los hallazgos con EventBridge .....                                                        | 980  |
| EventBridge frecuencia de notificación en GuardDuty .....                                             | 981  |
| Configuración de un punto de conexión y un tema de Amazon SNS .....                                   | 982  |
| Utilizándolo EventBridge con GuardDuty .....                                                          | 983  |
| Creación de una regla de EventBridge .....                                                            | 985  |
| EventBridge regla para entornos con varias cuentas .....                                              | 992  |
| Comprenda CloudWatch los registros y los motivos por los que se omiten recursos .....                 | 993  |
| Los registros de auditoría en Malware Protection for EC2 CloudWatch GuardDuty .....                   | 993  |
| GuardDuty Protección contra malware para la retención de registros de EC2 .....                       | 995  |
| Motivos para omitir un recurso .....                                                                  | 995  |
| Reportar un falso positivo en el producto del análisis de malware de EC2 .....                        | 1002 |
| Reportar un producto de análisis de objetos de S3 como falso positivo .....                           | 1003 |
| Informar de un resultado de escaneo de malware de Backup falso positivo .....                         | 1004 |
| Corrección de resultados .....                                                                        | 1006 |
| Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida ...                | 1006 |
| Corregir un bucket de S3 potencialmente comprometido .....                                            | 1008 |
| Recomendaciones basadas en las necesidades específicas de acceso al bucket de S3 ....                 | 1010 |
| Corregir un objeto de S3 potencialmente malicioso .....                                               | 1011 |
| Corregir una instantánea de EBS potencialmente comprometida .....                                     | 1011 |
| Corregir una AML de EC2 potencialmente comprometida .....                                             | 1012 |
| Corregir un punto de recuperación de EC2 potencialmente comprometido .....                            | 1013 |
| Corregir un punto de recuperación de S3 potencialmente comprometido .....                             | 1014 |
| Corregir un clúster de ECS potencialmente comprometido .....                                          | 1015 |

|                                                                                                                                            |      |
|--------------------------------------------------------------------------------------------------------------------------------------------|------|
| Corregir las credenciales potencialmente comprometidas AWS .....                                                                           | 1016 |
| Corregir un contenedor independiente potencialmente comprometido .....                                                                     | 1018 |
| Corregir los resultados de EKS Protection .....                                                                                            | 1019 |
| Posibles problemas de configuración .....                                                                                                  | 1020 |
| Corregir usuarios de Kubernetes potencialmente comprometidos .....                                                                         | 1020 |
| Corregir pods de Kubernetes potencialmente comprometidos .....                                                                             | 1023 |
| Corregir imágenes de contenedores potencialmente comprometidas .....                                                                       | 1025 |
| Corregir nodos de Kubernetes potencialmente comprometidos .....                                                                            | 1026 |
| Corregir los resultados de la Supervisión en tiempo de ejecución .....                                                                     | 1026 |
| Corrección de imágenes de contenedor en peligro .....                                                                                      | 1028 |
| Corregir una base de datos potencialmente comprometida .....                                                                               | 1029 |
| Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos .....                                  | 1029 |
| Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos .....                                   | 1030 |
| Corrección de credenciales potencialmente en peligro .....                                                                                 | 1031 |
| Restricción del acceso a la red .....                                                                                                      | 1032 |
| Corregir una función de Lambda potencialmente comprometida .....                                                                           | 1032 |
| Monitorear el uso y estimar los costos .....                                                                                               | 1034 |
| Métricas CloudWatch de uso de Amazon .....                                                                                                 | 1034 |
| Detalles de las métricas .....                                                                                                             | 1034 |
| Protección contra malware para S3 .....                                                                                                    | 1037 |
| Comprensión GuardDuty del uso .....                                                                                                        | 1038 |
| GuardDuty Procesamiento de eventos .....                                                                                                   | 1038 |
| GuardDuty Los cargos de procesamiento de registros de flujo de VPC para las instancias monitoreadas por GuardDuty Runtime Monitoring ..... | 1039 |
| Estimación del costo GuardDuty .....                                                                                                       | 1039 |
| Uso de la calculadora de precios AWS .....                                                                                                 | 1040 |
| Clientes de Security Hub .....                                                                                                             | 1040 |
| Nombres de características para planes de protección en la API .....                                                                       | 1042 |
| Cambio de orígenes de datos a características .....                                                                                        | 1042 |
| GuardDuty Cambios en la API .....                                                                                                          | 1042 |
| Características en comparación con los orígenes de datos .....                                                                             | 1043 |
| Comprender cómo funcionan las API con características .....                                                                                | 1044 |
| Incorporar cambios de características en las API .....                                                                                     | 1044 |
| Función mapeada GuardDuty .....                                                                                                            | 1045 |

|                                                                            |      |
|----------------------------------------------------------------------------|------|
| Seguridad .....                                                            | 1048 |
| Protección de datos .....                                                  | 1049 |
| Cifrado en reposo .....                                                    | 1050 |
| Cifrado en tránsito .....                                                  | 1050 |
| Desactivación del uso de los datos para mejorar el servicio .....          | 1050 |
| Iniciar sesión con CloudTrail .....                                        | 1052 |
| GuardDuty información en CloudTrail .....                                  | 1052 |
| GuardDuty eventos del plano de control en CloudTrail .....                 | 1053 |
| GuardDuty eventos de datos en CloudTrail .....                             | 1053 |
| Ejemplo: entradas de archivos de GuardDuty registro .....                  | 1055 |
| Gestión de identidad y acceso .....                                        | 1057 |
| Público .....                                                              | 1058 |
| Autenticación con identidades .....                                        | 1058 |
| Administración del acceso con políticas .....                              | 1060 |
| Cómo GuardDuty funciona Amazon con IAM .....                               | 1061 |
| Identity-based ejemplos de políticas .....                                 | 1067 |
| Cómo utilizar roles vinculados a servicios .....                           | 1076 |
| AWS políticas gestionadas .....                                            | 1087 |
| Resolución de problemas .....                                              | 1102 |
| Validación de conformidad .....                                            | 1104 |
| Resiliencia .....                                                          | 1105 |
| Seguridad de la infraestructura .....                                      | 1105 |
| Puntos de conexión de VPC (AWS PrivateLink) .....                          | 1106 |
| Consideraciones sobre los puntos GuardDuty finales de VPC .....            | 1106 |
| Creación de un punto final de VPC de interfaz para GuardDuty .....         | 1106 |
| Crear una política de puntos de conexión de VPC para GuardDuty .....       | 1107 |
| Subredes compartidas .....                                                 | 1107 |
| Integración con los servicios AWS de seguridad .....                       | 1109 |
| Integrarse GuardDuty con AWS Security Hub CSPM .....                       | 1109 |
| Integración GuardDuty con Amazon Detective .....                           | 1109 |
| AWS Security Hub CSPM integración .....                                    | 1109 |
| Cómo GuardDuty envía Amazon los resultados a AWS Security Hub CSPM .....   | 1110 |
| GuardDuty Visualización de los resultados en AWS Security Hub CSPM .....   | 1111 |
| Habilitación y configuración de la integración .....                       | 1131 |
| Uso de GuardDuty controles en Security Hub (CSPM) .....                    | 1131 |
| Cómo detener la publicación de resultados en el CSPM de Security Hub ..... | 1131 |



|                                                                                                                                                                                                              |          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Integración con Amazon Detective .....                                                                                                                                                                       | 1132     |
| Habilitación de la integración .....                                                                                                                                                                         | 1132     |
| Pasar de un hallazgo a Amazon Detective GuardDuty .....                                                                                                                                                      | 1133     |
| Uso de la integración con un entorno de GuardDuty múltiples cuentas .....                                                                                                                                    | 1133     |
| Suspensión o deshabilitación .....                                                                                                                                                                           | 1134     |
| GuardDuty anuncios .....                                                                                                                                                                                     | 1136     |
| Formato de los mensajes de Amazon SNS .....                                                                                                                                                                  | 1142     |
| GuardDuty cuotas .....                                                                                                                                                                                       | 1148     |
| Managed Instances Support .....                                                                                                                                                                              | 1154     |
| Resolución de problemas .....                                                                                                                                                                                | 1155     |
| Exportar resultados a Amazon S3: error de acceso .....                                                                                                                                                       | 1155     |
| Problemas de la protección contra malware para EC2 .....                                                                                                                                                     | 1156     |
| Falta el permiso AWS Organizations de administración necesario al habilitar el análisis de GuardDuty-initiated malware .....                                                                                 | 1156     |
| Estoy iniciando un análisis de On-demand software malicioso, pero se produce un error de falta de permisos necesarios. ....                                                                                  | 1156     |
| Recibo un error iam:GetRole al trabajar con la protección contra malware para EC2. ....                                                                                                                      | 1156     |
| Soy un GuardDuty administrador de cuentas que necesito habilitar el escaneo de GuardDuty-initiated malware, pero no uso una política AWS administrada: AmazonGuardDutyFullAccess administrar GuardDuty. .... | 1157     |
| Problemas de supervisión en tiempo de ejecución .....                                                                                                                                                        | 1157     |
| Problemas de cobertura en tiempo de ejecución .....                                                                                                                                                          | 1157     |
| Solución de problemas de memoria insuficiente .....                                                                                                                                                          | 1157     |
| Mi AWS Step Functions flujo de trabajo está fallando inesperadamente .....                                                                                                                                   | 1158     |
| Otras cuestiones de solución de problemas .....                                                                                                                                                              | 1159     |
| Regiones y puntos de conexión .....                                                                                                                                                                          | 1160     |
| Region-specific disponibilidad de funciones .....                                                                                                                                                            | 1160     |
| Acciones y parámetros heredados .....                                                                                                                                                                        | 1163     |
| Historial de revisión .....                                                                                                                                                                                  | 1165     |
| Actualizaciones anteriores .....                                                                                                                                                                             | 1273     |
| .....                                                                                                                                                                                                        | mcclxxiv |

# ¿Qué es Amazon GuardDuty?

Amazon GuardDuty es un servicio de detección de amenazas que supervisa, analiza y procesa de forma continua las fuentes de AWS datos y los registros de su AWS entorno. GuardDuty utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, códigos hash de archivos y modelos de aprendizaje automático (ML) para identificar actividades sospechosas y potencialmente maliciosas en su AWS entorno. La siguiente lista proporciona una descripción general de los posibles escenarios de amenazas que GuardDuty pueden ayudarle a detectarlos:

- Credenciales comprometidas y filtradas. AWS
- Filtración y destrucción de datos que puede conducir a un evento de ransomware. Patrones inusuales de eventos de inicio de sesión en versiones de motor compatibles de bases de datos de Amazon Aurora y Amazon RDS, que indican un comportamiento anómalo.
- Actividad de minería de criptomonedas no autorizada en las instancias y cargas de trabajo de contenedores de Amazon Elastic Compute Cloud (Amazon EC2).
- Presencia de malware en las instancias de Amazon EC2 y en las cargas de trabajo de contenedores, así como en los archivos recién cargados en los buckets de Amazon Simple Storage Service (Amazon S3).
- Eventos a nivel de sistema operativo, redes y archivos que indiquen un comportamiento no autorizado en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), tareas de AWS Fargate Amazon Elastic Container Service (Amazon ECS) e instancias y cargas de trabajo de contenedores de Amazon EC2 .

El siguiente vídeo proporciona una descripción general de cómo puede GuardDuty detectar las amenazas en su AWS entorno.

## [Qué es Amazon GuardDuty](#)

### Contenido

- [Características de GuardDuty](#)
- [Conformidad con DSS de PCI](#)
- [Precios en GuardDuty](#)
- [Accediendo GuardDuty](#)

## Características de GuardDuty

Estas son algunas de las formas clave en las que Amazon GuardDuty puede ayudarle a supervisar, detectar y gestionar las posibles amenazas en su AWS entorno.

Supervisa continuamente orígenes de datos y registros de eventos específicos

- Detección básica de amenazas: cuando habilita GuardDuty una Cuenta de AWS, comienza a ingerir GuardDuty automáticamente las fuentes de datos fundamentales asociadas a esa cuenta. Estos orígenes de datos incluyen eventos de administración de AWS CloudTrail , registros de flujo de VPC (de instancias de Amazon EC2) y registros de DNS. No necesita

habilitar ninguna otra opción para empezar GuardDuty a analizar y procesar estas fuentes de datos y generar las correspondientes conclusiones de seguridad. Para obtener más información, consulte [GuardDuty fuentes de datos fundamentales](#).

- **Detección ampliada de amenazas:** esta capacidad detecta ataques en varias etapas que abarcan fuentes de datos fundamentales, varios tipos de AWS recursos y tiempo, en un mismo momento. Cuenta de AWS Es posible que haya varios eventos en su cuenta que, por separado, no se presenten como una amenaza clara. Sin embargo, cuando estos eventos se observan en una secuencia que indica una actividad sospechosa, la GuardDuty identifica como una secuencia de ataque. GuardDuty lo notifica generando el tipo de búsqueda de la secuencia de ataque asociada para proporcionar detalles sobre la secuencia de ataque observada.

Sin coste adicional, la detección extendida de amenazas se activa automáticamente para cada una de ellas Cuenta de AWS cuando se activa GuardDuty. Esta capacidad no requiere que habilite ningún plan de protección centrado en los casos de uso. Sin embargo, para aumentar el alcance de la seguridad de sus recursos de Amazon S3, le recomendamos que GuardDuty habilite S3 Protection en su cuenta. Esto ayudará a que la Detección Extendida de Amenazas identifique los ataques en varias etapas que podrían afectar a sus recursos de Amazon S3.

Para obtener más información acerca de cómo funciona esta característica y qué escenarios de amenaza cubre, consulte [GuardDuty Detección de amenazas extendida](#).

- **Use-case planes de GuardDuty protección específicos:** para mejorar la visibilidad de la detección de amenazas y la seguridad de su AWS entorno, GuardDuty ofrece planes de protección específicos que puede elegir habilitar. Los planes de protección le ayudan a supervisar los registros y eventos de otros AWS servicios. Estas fuentes incluyen los registros de auditoría de EKS, la actividad de inicio de sesión de RDS, los eventos de datos de Amazon S3 CloudTrail, los volúmenes de EBS, la supervisión del tiempo de ejecución en Amazon EKS, Amazon EC2 y Amazon, y los registros de actividad de la red Lambda. ECS-Fargate GuardDuty[consolida estas fuentes de registros y eventos bajo el término Características](#). Puede activar uno o más planes de protección dedicados de forma compatible Región de AWS en cualquier momento. GuardDuty empezará a supervisar, procesar y analizar las actividades en función del plan de protección que active. Para obtener más información sobre cada plan de protección y su funcionamiento, consulte el documento del plan de protección correspondiente.

| Plan de protección                                        | Description (Descripción)                                                                                                                                                                                                               |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">S3 Protection</a>                             | Identifica posibles riesgos de seguridad, como intentos de filtración y destrucción de datos en los buckets de Amazon S3.                                                                                                               |
| <a href="#">EKS Protection</a>                            | La supervisión de registros de auditoría de EKS analiza los registros de auditoría de Kubernetes de los clústeres de Amazon EKS en busca de actividades potencialmente sospechosas y maliciosas.                                        |
| <a href="#">Supervisión en tiempo de ejecución</a>        | Supervisa y analiza eventos a nivel de sistema operativo en Amazon EKS, Amazon EC2 y Amazon ECS (incluido AWS Fargate) para detectar posibles amenazas en tiempo de ejecución.                                                          |
| <a href="#">Malware Protection for EC2</a>                | Detecta la posible presencia de malware mediante el análisis de los volúmenes de Amazon EBS asociados a las instancias de Amazon EC2. Existe la opción de utilizar esta característica bajo demanda.                                    |
| <a href="#">Protección contra malware para S3</a>         | Detecta la posible presencia de malware en los objetos recién cargados en los buckets de Amazon S3. Existe la opción de utilizar esta característica bajo demanda.                                                                      |
| <a href="#">Protección contra malware para AWS Backup</a> | Detecta la posible presencia de malware escaneando los recursos de backup, incluidas las instantáneas de EBS, las AMI de EC2 y los puntos de recuperación de AWS Backup. Existe la opción de utilizar esta característica bajo demanda. |
| <a href="#">Protección de RDS</a>                         | Analiza la actividad de inicio de sesión en RDS y elabora perfiles para detectar posibles amenazas de acceso a las bases de datos compatibles de Amazon Aurora y Amazon RDS.                                                            |

| Plan de protección                   | Description (Descripción)                                                                                                                                                                                                                                                         |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Protección de Lambda</a> | Supervisa los registros de actividad de red de Lambda, a partir de los registros de flujo de VPC, con el fin de detectar amenazas a las funciones de AWS Lambda . Entre las amenazas potenciales figuran la minería de criptomonedas y la comunicación con servidores maliciosos. |

### Habilitar la protección contra malware para S3 de forma independiente

GuardDuty ofrece flexibilidad para utilizar Malware Protection for S3 de forma independiente, sin necesidad de activar el GuardDuty servicio Amazon. Para obtener más información sobre cómo comenzar a utilizar únicamente la protección contra malware para S3, consulte [GuardDuty Protección contra malware para S3](#). Para usar todos los demás planes de protección, debe habilitar el GuardDuty servicio.

## Administre un entorno de varias cuentas

Puede administrar un AWS entorno de varias cuentas mediante el método de invitación AWS Organizations (recomendado) o el tradicional. Para obtener más información, consulte [Varias cuentas en GuardDuty](#).

## Genera resultados de seguridad para las amenazas detectadas

Cuando GuardDuty detecta posibles amenazas de seguridad asociadas a sus AWS recursos, comienza a generar resultados de seguridad que proporcionan información sobre el recurso potencialmente comprometido. Después de activarla GuardDuty en tu cuenta, genera [Ejemplos de hallazgos](#) para ver la asociada [Detalles de los resultados](#). Para obtener una lista completa de los resultados de seguridad, consulte [GuardDuty buscar tipos](#).

También puede utilizar un script de prueba que genere conclusiones de GuardDuty seguridad específicas para comprender cómo revisarlas y responder a ellas GuardDuty . GuardDuty Para obtener más información, consulte [Pruebe GuardDuty los resultados en cuentas dedicadas](#).

## Evaluar y administrar los resultados de seguridad

GuardDuty consolida las conclusiones de seguridad de todas las cuentas y muestra los resultados en el panel de resumen de la GuardDuty consola. También puede recuperar los resultados a través de la AWS Security Hub CSPM API o AWS Command Line Interface el AWS

SDK. Gracias a una perspectiva integral del estado actual de la seguridad, podrá identificar tendencias y posibles problemas, además de implementar las medidas correctivas necesarias. Para obtener más información, consulte [Gestionar GuardDuty los hallazgos](#).

Intégrelo con los servicios AWS de seguridad relacionados

Para seguir analizando e investigando las tendencias de seguridad de su AWS entorno, considere la posibilidad de utilizar los siguientes servicios AWS relacionados con la seguridad en combinación con GuardDuty

- **AWS Security Hub CSPM**— Este servicio le ofrece una visión completa del estado de seguridad de sus AWS recursos y le ayuda a comprobar si su AWS entorno se ajusta a los estándares y las mejores prácticas del sector de la seguridad. Esto lo consigue, en parte, consumiendo, agrupando, organizando y priorizando las conclusiones de seguridad de varios AWS servicios (incluido Amazon Macie) y de los productos AWS compatibles de Partner Network (APN). Security Hub CSPM le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios en todo su AWS entorno.

Para obtener información sobre el uso GuardDuty conjunto de CSPM de Security Hub, consulte [Integrarse GuardDuty con AWS Security Hub CSPM](#). Para obtener más información sobre Security Hub CSPM, consulte la Guía del [AWS Security Hub usuario](#).

- **Amazon Detective**: este servicio ayuda a analizar, investigar e identificar rápidamente la causa raíz de los resultados de seguridad o las actividades sospechosas. Detective recopila automáticamente los datos de registro de sus AWS recursos. A continuación, utiliza el machine learning, el análisis estadístico y la teoría de grafos para generar visualizaciones que lo ayuden a realizar investigaciones sobre la seguridad con mayor rapidez y de forma más eficaz. Las agregaciones de datos, resúmenes y contexto predefinidos de Detective ayudan a analizar los posibles problemas de seguridad, así como a determinar su naturaleza y alcance.

Para obtener información sobre el uso GuardDuty conjunto de Detective, consulte [Integración GuardDuty con Amazon Detective](#). Para obtener más información sobre Detective, consulte la [Guía del usuario de Amazon Detective](#).

- **Amazon EventBridge**: este servicio le ayuda a recibir notificaciones y responder a los hallazgos GuardDuty de seguridad casi en tiempo real. GuardDuty crea un evento cuando hay un cambio en los resultados. Puede elegir la frecuencia de la que desea recibir las notificaciones EventBridge. Para obtener más información, consulta [Qué es Amazon EventBridge](#) en la Guía del EventBridge usuario de Amazon.

## Conformidad con DSS de PCI

GuardDuty admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios, y se ha comprobado que cumple con el estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI). Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Compliance Package, consulte [PCI DSS Level 1](#).

Para obtener más información, consulte una [nueva prueba de terceros que compara Amazon con GuardDuty los sistemas de detección de intrusiones en la red](#) en el blog AWS de seguridad.

## Precios en GuardDuty

Esta sección se centra en el capa gratuita de AWS modelo que se GuardDuty utiliza para los distintos planes de protección y en cómo puede ver los costes de uso estimados y reales. Si busca información detallada sobre los precios asociados a todos los planes de protección de las regiones compatibles, consulte [GuardDuty los precios](#).

### capa gratuita de AWS

capa gratuita de AWS le ayuda a explorar y probar de Servicios de AWS forma gratuita hasta los límites especificados para cada servicio. Existen tres categorías: 12 meses gratis, siempre gratis y pruebas gratuitas de corta duración. Amazon GuardDuty pertenece a la categoría de prueba gratuita a corto plazo y ofrece una prueba gratuita de 30 días. Si continúa utilizándolo GuardDuty después de que finalice la prueba gratuita, empezará a incurrir en costes en función de la forma en que utilice este servicio.

#### <sup>1</sup> Excepción a la GuardDuty prueba gratuita de 30 días

On-demand El análisis de malware (en Malware Protection for EC2) y Malware Protection for S3 no entran en la categoría de prueba gratuita de GuardDuty 30 días a corto plazo. La protección contra malware para S3 incluye una capa gratuita, mientras que el análisis de On-demand malware sigue un modelo de pago por uso. No hay una prueba gratuita de 30 días ni un modelo de coste por niveles gratuitos con análisis de malware. On-demand

## Uso de una GuardDuty prueba gratuita de 30 días

Al usarlo GuardDuty por primera vez en una región Región de AWS, Cuenta de AWS se inscribe automáticamente en una prueba gratuita de 30 días en esa región. Algunos de los planes de



protección también se habilitarán automáticamente y están incluidos en la prueba gratuita de 30 días. Como GuardDuty se trata de un servicio regional, cuando lo habilites por primera vez en una región diferente, tu cuenta tendrá una prueba gratuita de 30 días GuardDuty en esa región. Al trabajar con varias cuentas de una GuardDuty organización, cada una de ellas tiene su propia versión de prueba gratuita de 30 días.

Utilice la siguiente tabla para revisar los planes de protección con GuardDuty los que están habilitados de forma predeterminada y su disponibilidad de prueba gratuita.

| Plan de protección                                                                   | Habilitado de forma predeterminada con GuardDuty | Disponibilidad de prueba gratuita independiente <sup>2</sup> |  |
|--------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------|--|
| <a href="#">EKS Protection</a>                                                       | Sí                                               | Sí                                                           |  |
| <a href="#">S3 Protection</a>                                                        | Sí                                               | Sí                                                           |  |
| <a href="#">Supervisión en tiempo de ejecución</a>                                   | No                                               | Sí                                                           |  |
| <a href="#">Malware Protection for EC2 – GuardDuty-initiated análisis de malware</a> | Sí                                               | Sí                                                           |  |
| <a href="#">Malware Protection for EC2 – On-demand escanea el malware GuardDuty</a>  | No                                               | No <sup>1</sup>                                              |  |
| <a href="#">GuardDuty Protección contra malware para S3</a>                          | No                                               | No <sup>1</sup>                                              |  |
| <a href="#">Protección de RDS</a>                                                    | Sí                                               | Sí                                                           |  |
| <a href="#">Protección de Lambda</a>                                                 | Sí                                               | Sí                                                           |  |

<sup>2</sup> Cuando se activa GuardDuty por primera vez, los planes de protección (excepto Runtime Monitoring) se activan automáticamente y se incluyen en la prueba gratuita inicial de 30 días. Cuando una GuardDuty cuenta existente habilita un nuevo plan de protección después de que la prueba GuardDuty gratuita inicial haya expirado, ese plan de protección incluye su propia prueba gratuita de 30 días. Para obtener más información sobre las pruebas gratuitas de los planes de protección, consulte el documento relacionado con cada plan de protección.

Consulta el coste de uso estimado durante la prueba gratuita: durante la prueba gratuita de 30 días GuardDuty y, si es posible, un plan de protección, GuardDuty proporciona el coste de uso estimado de tu cuenta. Si es una cuenta de GuardDuty administrador delegado, puede ver el coste total de uso estimado y el desglose a nivel de cuenta de todas las cuentas de miembros que estén habilitadas. GuardDuty Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#).

Coste de uso una vez finalizada la prueba gratuita: si sigues utilizando GuardDuty alguno de sus planes de protección una vez finalizada la prueba gratuita, empezarás a incurrir en los costes de uso asociados. Para ver su factura, vaya a Cost Explorer en la <https://console.aws.amazon.com/costmanagement/> consola. Para obtener más información sobre la facturación de la AWS cuenta, consulte la [Guía del AWS Billing usuario](#).

## Uso de la protección contra malware para S3 con la capa gratuita

La protección contra malware para S3 incluye una capa gratuita asociada a su Cuentas de AWS. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

## Accediendo GuardDuty

Amazon GuardDuty está disponible en la mayoría Regiones de AWS. Para ver una lista de las regiones en las GuardDuty que está disponible actualmente, consulta [Regiones y puntos de conexión](#).

Puede usarlo GuardDuty de cualquiera de las siguientes maneras:

GuardDuty consola

<https://console.aws.amazon.com/guardduty/>

La consola es una interfaz basada en navegador para obtener acceso y usar GuardDuty. La GuardDuty consola proporciona acceso a su GuardDuty cuenta, datos y recursos.

## AWS Command Line Interface

Con AWS Command Line Interface (AWS CLI), puede emitir comandos en la línea de comandos de su sistema para realizar GuardDuty tareas y AWS tareas. Los AWS CLI comandos son útiles si desea crear scripts que realicen tareas.

Para obtener información sobre la instalación y el uso AWS CLI, consulte la [Guía AWS Command Line Interface del usuario](#). Para ver los AWS CLI comandos disponibles GuardDuty, consulte la [Referencia de AWS CLI comandos](#).

## GuardDuty API HTTPS

Puedes acceder GuardDuty y AWS programar mediante la API GuardDuty HTTPS, que te permite enviar solicitudes HTTPS directamente al servicio. Para obtener más información, consulta la [referencia de la GuardDuty API de Amazon](#).

## AWS SDK

AWS proporciona kits de desarrollo de software (SDK) que constan de bibliotecas y código de muestra para varios lenguajes de programación y plataformas (Java, Python, Ruby, .NET, iOS, Android y más). Los SDK permiten crear cómodamente acceso mediante programación a GuardDuty. Para obtener información sobre los SDK de AWS (por ejemplo, cómo descargarlos e instalarlos), consulte [Herramientas para Amazon Web Services](#).

# Conceptos y términos clave en Amazon GuardDuty

Al empezar con Amazon GuardDuty, podrás beneficiarte de conocer sus conceptos y los términos clave asociados.

## Cuenta

Una cuenta estándar de Amazon Web Services (AWS) que contiene tus AWS recursos. Puede iniciar sesión AWS con su cuenta y activarla GuardDuty.

También puedes invitar a otras cuentas a que activen tu AWS cuenta GuardDuty y se asocien a ella GuardDuty. Si se aceptan tus invitaciones, tu cuenta se designará como cuenta GuardDuty de administrador y las cuentas añadidas pasarán a ser tus cuentas de miembro. A continuación, podrá ver y gestionar los GuardDuty resultados de esas cuentas en su nombre.

Los usuarios de la cuenta de administrador pueden configurar GuardDuty , ver y gestionar GuardDuty los resultados de su propia cuenta y de todas las cuentas de sus miembros. Para obtener información sobre la cantidad de cuentas de miembro que puede administrar la cuenta de administrador, consulte [GuardDuty cuotas](#).

Los usuarios de las cuentas de los miembros pueden configurar GuardDuty , ver y gestionar GuardDuty los hallazgos en su cuenta (a través de la consola GuardDuty de administración o de la GuardDuty API). Los usuarios de cuentas de miembros no pueden ver ni administrar los resultados de las cuentas de otros miembros.

Una no Cuenta de AWS puede ser una cuenta de GuardDuty administrador y una cuenta de miembro al mismo tiempo. Una Cuenta de AWS solo puede aceptar una invitación de membresía. La aceptación de una invitación de suscripción es opcional.

Para obtener más información, consulte [Varias cuentas en Amazon GuardDuty](#).

## Secuencia de ataque

Una secuencia de ataque es una correlación de varios eventos que, según lo observado GuardDuty, ocurrieron en una secuencia específica que coincide con el patrón de una actividad sospechosa. GuardDuty utiliza su [Detección Extendida de Amenazas](#) capacidad para detectar estos ataques en varias etapas que abarcan las fuentes de datos, los AWS recursos y el cronograma fundamentales de su cuenta.

La siguiente lista explica brevemente los términos clave asociados a las secuencias de ataque:

- **Indicadores:** proporcionan información sobre por qué una secuencia de eventos se alinea con una posible actividad sospechosa.
- **Señales:** una señal es una actividad de la API GuardDuty observada o un GuardDuty hallazgo ya detectado en tu cuenta. Al correlacionar los eventos observados en una secuencia específica en tu cuenta, GuardDuty identifica una secuencia de ataque.

Hay eventos en su cuenta que no son indicativos de una amenaza potencial. GuardDuty los considera señales débiles. Sin embargo, cuando se observan señales y GuardDuty hallazgos débiles en una secuencia específica que, cuando se correlacionan, se alinean con una actividad potencialmente sospechosa, se GuardDuty genera un hallazgo en la secuencia de ataque.

- **Puntos de conexión:** información sobre los puntos de conexión de la red que un actor de amenazas podría utilizar en una secuencia de ataque.

## Detector

Amazon GuardDuty es un servicio regional. Cuando habilitas GuardDuty un detector específico Región de AWS, Cuenta de AWS se te asocia a un identificador de detector. Este identificador alfanumérico de 32 caracteres es único para la cuenta en esa región. Por ejemplo, si habilitas GuardDuty la misma cuenta en una región diferente, tu cuenta se asociará a un ID de detector diferente. El formato de un detectorId es 12abc34d567e8fa901bc2d34e56789f0.

Todos los GuardDuty hallazgos, cuentas y acciones relacionados con la gestión de los hallazgos y el GuardDuty servicio utilizan el ID del detector para ejecutar una operación de API.

Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

### Note

En entornos multicuenta, todos los resultados para las cuentas de miembro se agregan al detector de la cuenta de administrador.

Algunas GuardDuty funciones se configuran a través del detector, como la configuración de la frecuencia de notificación de los CloudWatch eventos y la activación o desactivación de los planes de protección opcionales GuardDuty para su procesamiento.

## Uso de la protección contra malware para S3 en GuardDuty

Al habilitar la protección contra malware para S3 en una cuenta que GuardDuty esté habilitada, las acciones de Malware Protection para S3, como habilitar, editar y deshabilitar un recurso protegido, no se asocian al ID del detector.

Si no activas GuardDuty ni eliges la opción de detección de amenazas Malware Protection for S3, no se crea ningún identificador de detector para tu cuenta.

## Orígenes de datos fundamentales

El origen o la ubicación de un conjunto de datos. Para detectar una actividad no autorizada o inesperada en su AWS entorno. GuardDuty analiza y procesa datos de registros de AWS CloudTrail eventos, eventos AWS CloudTrail de administración, eventos de AWS CloudTrail datos para S3, registros de flujo de VPC, registros de DNS, consulte [GuardDuty fuentes de datos fundamentales](#)

## Característica

Un objeto de función configurado para su plan de GuardDuty protección ayuda a detectar una actividad no autorizada o inesperada en su AWS entorno. Cada plan de GuardDuty protección configura el objeto de función correspondiente para analizar y procesar los datos. Algunos de los objetos de características son los registros de auditoría de EKS, la supervisión de la actividad de inicio de sesión en RDS, los registros de actividad de red de Lambda y los volúmenes de EBS. Para obtener más información, consulte [Nombres de funciones de los planes de protección en la GuardDuty API](#).

## Resultado

Un problema potencial de seguridad descubierto por GuardDuty. Para obtener más información, consulte [Comprender y generar los GuardDuty hallazgos de Amazon](#).

Los resultados se muestran en la GuardDuty consola y contienen una descripción detallada del problema de seguridad. También puedes recuperar las conclusiones generadas llamando a las operaciones [GetFindings](#) y a la [ListFindingsAPI](#).

También puedes ver tus GuardDuty hallazgos a través de los CloudWatch eventos de Amazon. GuardDuty envía los resultados a Amazon CloudWatch a través del protocolo HTTPS. Para obtener más información, consulte [Procesando GuardDuty las conclusiones con Amazon EventBridge](#).

## Rol de IAM

Este es el rol de IAM con los permisos requeridos para analizar el objeto de S3. Cuando el etiquetado de objetos escaneados está activado, los PassRole permisos de IAM ayudan a GuardDuty añadir etiquetas al objeto escaneado.

## Recurso del plan de protección contra malware

Tras habilitar la protección contra malware para S3 en un bucket, GuardDuty crea un recurso de plan de protección contra malware. Este recurso está asociado al ID del plan de protección contra malware, que es un identificador único del bucket protegido. Utilice el recurso del plan de protección contra malware para realizar operaciones de la API en un recurso protegido.

## Bucket protegido (recurso protegido)

Se considera que un bucket de Amazon S3 está protegido cuando habilita la protección contra malware para S3 para este bucket y su estado de protección cambia a Activo.

GuardDuty solo admite un bucket de S3 como recurso protegido.

## Estado de protección

El estado asociado al recurso del plan de protección contra malware. Después de habilitar la protección contra malware para S3 para el bucket, este estado representa si el bucket está configurado correctamente o no.

## Prefijo del objeto de S3

En un bucket de Amazon Simple Storage Service (Amazon S3), puede utilizar prefijos para organizar el almacenamiento. Un prefijo es una agrupación lógica de los objetos de un bucket de S3. Para obtener más información, consulte [Organización y enumeración de objetos](#) en la Guía del usuario de Amazon S3.

## Opciones de análisis

Cuando la protección contra GuardDuty malware para EC2 está habilitada, le permite especificar qué instancias de Amazon EC2 y volúmenes de Amazon Elastic Block Store (EBS) debe escanear u omitir. Esta característica le permite agregar las etiquetas existentes que están asociadas a las instancias de EC2 y al volumen de EBS a una lista de etiquetas de inclusión o a una lista de etiquetas de exclusión. Los recursos asociados a las etiquetas que agregue a una lista de etiquetas de inclusión se analizan en busca de malware y los que se agregan a una lista de etiquetas de exclusión no se analizan. Para obtener más información, consulte [Opciones de análisis con etiquetas definidas por el usuario](#).

## Retención de instantáneas

Cuando la protección contra GuardDuty malware para EC2 está habilitada, ofrece la opción de conservar las instantáneas de los volúmenes de EBS en su cuenta. AWS GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de sus volúmenes de EBS. Puede retener las instantáneas de los volúmenes de EBS solo si el análisis de Malware Protection for EC2 detecta malware en las réplicas de los volúmenes de EBS. Si no se detecta ningún malware en las réplicas de los volúmenes de EBS, elimina GuardDuty automáticamente las instantáneas de sus volúmenes de EBS, independientemente de la configuración de retención de las instantáneas. Para obtener más información, consulte [Retención de instantáneas](#).

## Regla de supresión de

Las reglas de supresión permiten crear combinaciones de atributos muy específicas para suprimir los resultados. Por ejemplo, puede definir una regla a través del GuardDuty filtro para archivar automáticamente solo las instancias Recon:EC2/Portscan de una VPC específica, que ejecuten una AMI específica o que tengan una etiqueta EC2 específica. Esta regla daría lugar a que los resultados del escaneo de puertos se archivaran automáticamente desde las instancias que cumplan los criterios. Sin embargo, sigue permitiendo emitir alertas si GuardDuty detecta instancias que estén llevando a cabo otras actividades maliciosas, como la minería de criptomonedas.

Las reglas de supresión definidas en la cuenta de GuardDuty administrador se aplican a las cuentas de los GuardDuty miembros. GuardDuty las cuentas de los miembros no pueden modificar las reglas de supresión.

Con las reglas de supresión, GuardDuty sigue generando todos los hallazgos. Las reglas de supresión facilitan la eliminación de resultados, mientras mantienen un historial completo e inmutable de todas las actividades.

Normalmente, las reglas de supresión se utilizan para ocultar los hallazgos del entorno que se consideran falsos positivos y reducir así el ruido de los resultados con poco valor para que pueda centrarse en amenazas más importantes. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

## Lista de IP de confianza

Una lista de direcciones IP confiables para una comunicación altamente segura con su AWS entorno. GuardDuty no genera resultados basados en listas de IP confiables. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).



## Lista de IP de amenazas

Una lista de direcciones IP maliciosas conocidas. Además de generar hallazgos debido a una actividad potencialmente sospechosa, GuardDuty también genera hallazgos basados en estas listas de amenazas. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).

# Empezar con GuardDuty

Este tutorial proporciona una introducción práctica a GuardDuty. Los requisitos mínimos para GuardDuty habilitarla como cuenta independiente o como GuardDuty administrador se describen en el paso 1. AWS Organizations Los pasos 2 a 5 incluyen el uso de las funciones adicionales recomendadas por usted GuardDuty para aprovechar al máximo sus hallazgos.

## Temas

- [Antes de empezar](#)
- [Paso 1: Habilita Amazon GuardDuty](#)
- [Paso 2: generación de resultados de muestra y exploración de las operaciones básicas](#)
- [Paso 3: Configurar la exportación de GuardDuty los resultados a un bucket de Amazon S3](#)
- [Paso 4: Configurar la GuardDuty búsqueda de alertas a través de las redes sociales](#)
- [Siguiendo pasos](#)

## Antes de empezar

GuardDuty es un servicio de detección de amenazas que [Orígenes de datos fundamentales](#) monitorea eventos AWS CloudTrail de administración, registros de flujo de Amazon VPC y registros de consultas de Amazon Route 53 Resolver DNS. GuardDuty también analiza las funciones asociadas a sus tipos de protección solo si las habilita por separado. Las [características](#) incluyen los registros de auditoría de Kubernetes, la actividad de inicio de sesión de RDS, AWS CloudTrail los eventos de datos para Amazon S3, los volúmenes de Amazon EBS, Runtime Monitoring y los registros de actividad de red Lambda. El uso de estas fuentes de datos y funciones (si están habilitadas) GuardDuty genera conclusiones de seguridad para su cuenta.

Una vez habilitada GuardDuty, comienza a monitorear tu cuenta para detectar posibles amenazas en función de las actividades de las fuentes de datos fundamentales. De forma predeterminada, [Detección Extendida de Amenazas](#) está habilitada para todas las personas Cuentas de AWS que la tengan habilitada GuardDuty. Esta capacidad detecta secuencias de ataques en varias etapas que abarcan varios orígenes de datos fundamentales, recursos de AWS y el tiempo en su cuenta. Para detectar posibles amenazas a AWS recursos específicos, puede optar por habilitar los planes de protección que GuardDuty ofrece, centrados en los casos de uso. Para obtener más información, consulte [Características de GuardDuty](#).

No necesita habilitar ninguno de los orígenes de datos fundamentales de forma explícita. Al habilitar la S3 Protection, no es necesario habilitar explícitamente el registro de eventos de datos de Amazon S3. Del mismo modo, al habilitar EKS Protection, no es necesario habilitar explícitamente los registros de auditoría de Amazon EKS. Amazon GuardDuty extrae flujos de datos independientes directamente de estos servicios.

En el caso de una GuardDuty cuenta nueva, algunos de los tipos de protección disponibles que se admiten en una Región de AWS están habilitados e incluidos en el período de prueba gratuito de 30 días de forma predeterminada. Puede excluirse voluntariamente de uno o de todos ellos. Si ya tiene una opción Cuenta de AWS GuardDuty habilitada, puede optar por habilitar alguno o todos los planes de protección disponibles en su región. Para obtener información general sobre los planes de protección y qué planes de protección se habilitarán de forma predeterminada, consulte [Precios en GuardDuty](#).

Al habilitarlo GuardDuty, tenga en cuenta lo siguiente:

- GuardDuty es un servicio regional, lo que significa que cualquiera de los procedimientos de configuración que siga en esta página debe repetirse en cada región con la que desee realizar el monitoreo GuardDuty.

Le recomendamos encarecidamente que lo habilite GuardDuty en todas AWS las regiones compatibles. Esto te permitirá GuardDuty obtener información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utilices activamente. Esto también permite GuardDuty monitorear AWS CloudTrail los eventos para AWS servicios globales como IAM. Si no GuardDuty está habilitada en todas las regiones compatibles, se reduce su capacidad para detectar actividades que involucren servicios globales. Para obtener una lista completa de las regiones en las GuardDuty que está disponible, consulte [Regiones y puntos de conexión](#).

- Cualquier usuario con privilegios de administrador en una AWS cuenta puede habilitarlos GuardDuty; sin embargo, siguiendo las prácticas recomendadas de seguridad en materia de privilegios mínimos, se recomienda crear un rol, usuario o grupo de IAM para administrarlo de GuardDuty forma específica. Para obtener información sobre los permisos necesarios para habilitarlos, GuardDuty consulte [Permisos necesarios para habilitarla GuardDuty](#).
- Cuando se habilita GuardDuty por primera vez en una región Región de AWS, de forma predeterminada, también se habilitan todos los tipos de protección disponibles y compatibles en esa región, incluida la protección contra malware para EC2. GuardDuty crea un rol vinculado a un servicio para su cuenta denominado. `AWSServiceRoleForAmazonGuardDuty` Esta función incluye los permisos y las políticas de confianza que permiten GuardDuty consumir y analizar los eventos directamente desde ellos [GuardDuty fuentes de datos fundamentales](#) para generar

conclusiones de seguridad. Malware Protection for EC2 crea otro rol vinculado al servicio para la cuenta denominado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Esta función incluye los permisos y las políticas de confianza que permiten a Malware Protection for EC2 realizar análisis sin agentes para detectar malware en su cuenta. GuardDuty Permite GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la cuenta de servicio. GuardDuty Para obtener más información, consulte [Service-linked permisos de rol para GuardDuty](#). Para obtener más información acerca de los roles vinculados a servicios, consulte [Uso de roles vinculados a servicios](#).

- Cuando lo habilita GuardDuty por primera vez en una región, su AWS cuenta se inscribe automáticamente en una prueba GuardDuty gratuita de 30 días para esa región.

En el siguiente vídeo se explica cómo una cuenta de administrador puede empezar a utilizar una cuenta de administrador GuardDuty y habilitarla en varias cuentas de miembros.

[Primeros pasos: habilitar Amazon GuardDuty para entornos independientes o de cuentas múltiples](#)

# Paso 1: Habilita Amazon GuardDuty

El primer paso para usarlo GuardDuty es habilitarlo en su cuenta. Una vez activado, GuardDuty comenzará inmediatamente a monitorear las amenazas a la seguridad en la región actual.

Si, como GuardDuty administrador, desea gestionar GuardDuty los resultados de otras cuentas de su organización, debe añadir las cuentas de GuardDuty los miembros y activarlas también.

## Note

Si desea activar la protección contra GuardDuty malware para S3 sin habilitarla GuardDuty, consulte los pasos a seguir en [GuardDuty Protección contra malware para S3](#).

### Standalone account environment

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>
2. Selecciona la opción Amazon GuardDuty - Todas las funciones.
3. Elija Comenzar.
4. En la GuardDuty página de bienvenida, consulta las condiciones del servicio. Seleccione Habilitar GuardDuty.

### Multi-account environment

## Important

Como requisitos previos para este proceso, debe estar en la misma organización que todas las cuentas que desee administrar y tener acceso a la cuenta de AWS Organizations administración para delegar un administrador GuardDuty en su organización. Es posible que se necesiten permisos adicionales para delegar un administrador. Para más información, consulte [Permisos necesarios para designar una cuenta de GuardDuty administrador delegado](#).

### Para designar una cuenta de administrador delegado GuardDuty

1. Abra la AWS Organizations consola en <https://console.aws.amazon.com/organizations/>, mediante la cuenta de administración.

2. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

¿ GuardDuty Ya está habilitada en tu cuenta?

- Si aún no GuardDuty está habilitada, puede seleccionar Comenzar y, a continuación, designar un administrador GuardDuty delegado en la GuardDuty página de bienvenida.
  - Si GuardDuty está habilitada, puede designar un administrador GuardDuty delegado en la página de configuración.
3. Introduzca el ID de AWS cuenta de doce dígitos de la cuenta que desee designar como administrador GuardDuty delegado de la organización y seleccione Delegado.

 Note

Si aún no GuardDuty está activado, la designación de un administrador delegado habilitará esa cuenta en GuardDuty su región actual.

## Agregación de cuentas de miembro

Este procedimiento abarca la adición de cuentas de miembros a una cuenta de administrador GuardDuty delegado mediante. AWS Organizations También existe la opción de agregar miembros mediante invitación. Para obtener más información sobre ambos métodos para asociar miembros GuardDuty, consulte. [Varias cuentas en Amazon GuardDuty](#)

1. Inicie sesión en la cuenta de administrado delegado
2. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
3. En el panel de navegación, elija Settings (Configuración) y Accounts (Cuentas).

En la tabla de cuentas aparecen todas las cuentas de la organización.

4. Para elegir las cuentas que desea agregar como miembros, seleccione la casilla situada junto al ID de la cuenta. A continuación, en el menú Acción, seleccione Agregar miembro.

 Tip

Puedes automatizar la adición de nuevas cuentas como miembros activando la Auto-enablefunción; sin embargo, esto solo se aplica a las cuentas que se unen a tu organización una vez habilitada la función.

## Paso 2: generación de resultados de muestra y exploración de las operaciones básicas

Cuando GuardDuty descubre un problema de seguridad, genera un hallazgo. Un GuardDuty hallazgo es un conjunto de datos que contiene detalles relacionados con ese problema de seguridad único. Los detalles del resultado se pueden utilizar para ayudarle a investigar el problema.

GuardDuty permite generar ejemplos de hallazgos con valores indicativos, que se pueden utilizar para probar la GuardDuty funcionalidad y familiarizarse con los hallazgos antes de tener que responder a un problema de seguridad real descubierto por GuardDuty la persona. Siga la guía que aparece a continuación para generar ejemplos de resultados para cada tipo de hallazgo disponible. Si desea conocer otras formas de generar ejemplos de resultados, incluida la generación de un evento de seguridad simulado en su cuenta, consulte. GuardDuty [Ejemplos de hallazgos](#)

### Creación y exploración de los resultados de muestra

1. En el panel de navegación, seleccione Configuración.
2. En la página Settings, en Sample findings, elija Generate sample findings.
3. En el panel de navegación, elija Resumen para ver la información sobre los hallazgos generados en su AWS entorno. Para obtener más información acerca de los componentes del panel de resumen, consulte [Panel de resumen en Amazon GuardDuty](#).
4. En el panel de navegación, seleccione Resultados. Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].
5. Seleccione un resultado de la lista para ver sus detalles.
  - Puede revisar los distintos campos de información disponibles en el panel de detalles del resultado. Los distintos tipos de resultados pueden tener campos diferentes. Para obtener más información acerca de los campos disponibles en todos los tipos de resultados, consulte [Detalles de los resultados](#). Puede llevar a cabo las siguientes acciones en el panel de detalles:
    - Seleccione el ID de resultado en la parte superior del panel para abrir los detalles JSON completos del resultado. El archivo JSON completo también se puede descargar desde este panel. El JSON contiene información adicional que no se incluye en la vista de consola y es el formato que pueden incorporar otras herramientas y servicios.
    - Consulte la sección Recurso afectado. Si se trata de una conclusión real, la información que aparece aquí le ayudará a identificar un recurso de su cuenta que debería

investigarse e incluirá enlaces a los recursos adecuados Consola de administración de AWS para poder utilizar las acciones pertinentes.

- Seleccione los iconos de la lupa con el signo + o - para crear un filtro inclusivo o exclusivo para ese detalle. Para obtener más información acerca de los filtros de resultados, consulte [Filtrar los hallazgos en GuardDuty](#).

## 6. Archivado de todos los resultados de muestra

- Para seleccionar todos los resultados, marque la casilla de verificación situada en la parte superior de la lista.
- Anule la selección de los resultados que desee conservar.
- Seleccione el menú Acciones y, a continuación, seleccione Archivar para ocultar los resultados de muestra.

### Note

Para ver los resultados archivados, seleccione Actual y, a continuación, Archivado para cambiar la vista de los resultados.

## Paso 3: Configurar la exportación de GuardDuty los resultados a un bucket de Amazon S3

GuardDuty recomienda configurar los ajustes para exportar los hallazgos, ya que le permite exportar los hallazgos a un bucket de S3 para su almacenamiento indefinido más allá del período de retención de GuardDuty 90 días. Esto le permite mantener un registro de los hallazgos o realizar un seguimiento de los problemas en su AWS entorno a lo largo del tiempo. GuardDuty cifra los datos de los hallazgos en su depósito de S3 mediante AWS Key Management Service (AWS KMS key). Para configurar los ajustes, debe asignar GuardDuty al permiso una clave KMS. Para ver más pasos detallados, consulte [Exportar los resultados generados a Amazon S3](#).

Para exportar GuardDuty los resultados al bucket de Amazon S3

### 1. Adjunte la política a la clave de KMS

- Inicio sesión en la consola AWS Key Management Service (AWS KMS) Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/kms>.



- b. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
- c. En el panel de navegación, elija Claves administradas por el cliente.
- d. Seleccione una clave de KMS existente o siga los pasos para [crear una clave de KMS de cifrado simétrico](#) que se indican en la Guía para desarrolladores de AWS Key Management Service .

La región de su clave de KMS y de su bucket de Amazon S3 debe ser la misma.

Copie la clave de ARN en un bloc de notas para utilizarla en los pasos posteriores.

- e. En la sección Política de claves, elija Editar. Si aparece Cambiar a vista de política, elíjala para mostrar la Política de claves y, a continuación, elija Editar.
- f. Copie el siguiente bloque de política en la política de clave de KMS:

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

Edite la política sustituyendo los siguientes valores que están formateados *red* en el ejemplo de política:

1. *KMS key ARN* Sustitúyala por el nombre de recurso de Amazon (ARN) de la clave KMS. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .
2. *123456789012* Sustitúyalo por el Cuenta de AWS ID propietario de la GuardDuty cuenta que exporta los resultados.

3. **Region2** Sustitúyalo por el Región de AWS lugar donde se generan los GuardDuty hallazgos.
4. **SourceDetectorID** Sustitúyalo por el detectorID de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

## 2. Asociar la política al bucket de Amazon S3

Si aún no dispone de un bucket de Amazon S3 al que desee exportar estos resultados, consulte [Crear un bucket](#) en la Guía del usuario de Amazon S3.

- a. Siga los pasos descritos en [Para crear o editar una política de bucket](#) en la Guía del usuario de Amazon S3, hasta que aparezca la página Editar política de bucket.
- b. La política de ejemplo muestra cómo conceder GuardDuty permisos para exportar los resultados a su bucket de Amazon S3. Si cambia la ruta después de configurar la exportación de resultados, deberá modificar la política para conceder permiso a la nueva ubicación.

Copie la siguiente política de ejemplo y péguela en el Editor de políticas de bucket.

Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Política de ejemplo de bucket de S3

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
    },
  ],
}
```

```

        "Action": "s3:GetBucketLocation",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012",
                "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"
            }
        }
    },
    {
        "Sid": "Allow PutObject",
        "Effect": "Allow",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012",
                "aws:SourceArn": "arn:aws:guardduty:us-
east-2:123456789012:detector/SourceDetectorID"
            }
        }
    },
    {
        "Sid": "Deny unencrypted object uploads",
        "Effect": "Deny",
        "Principal": {
            "Service": "guardduty.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
        "Condition": {
            "StringNotEquals": {
                "s3:x-amz-server-side-encryption": "aws:kms"
            }
        }
    }
},

```

```

    {
      "Sid": "Deny incorrect encryption header",
      "Effect": "Deny",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption-aws-kms-key-id":
"arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
      }
    },
    {
      "Sid": "Deny non-HTTPS access",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional
prefix]/*",
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}

```

- c. Edite la política sustituyendo los siguientes valores que están formateados *red* en el ejemplo de política:
1. *Amazon S3 bucket ARN* Sustitúyalo por el nombre de recurso de Amazon (ARN) del bucket de Amazon S3. Puedes encontrar el ARN del bucket en la página de edición de la política del bucket de la <https://console.aws.amazon.com/s3/console>.
  2. *123456789012* Sustitúyalo por el Cuenta de AWS ID propietario de la GuardDuty cuenta que exporta los resultados.

3. *Region2* Sustitúyalo por el Región de AWS lugar donde se generan los GuardDuty hallazgos.
4. *SourceDetectorID* Sustitúyalo por el detectorID de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

5. Sustituya *[optional prefix]* parte del valor del *S3 bucket ARN/[optional prefix]* marcador de posición por una ubicación de carpeta opcional a la que desee exportar los resultados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos mediante prefijos](#) en la Guía del usuario de Amazon S3.

Cuando proporciones una ubicación de carpeta opcional que aún no exista, la GuardDuty creará solo si la cuenta asociada al depósito de S3 es la misma que la cuenta que exporta los resultados. Al exportar resultados a un bucket de S3 que pertenece a otra cuenta, la ubicación de la carpeta ya debe existir.

6. *KMS key ARN* Sustitúyala por el nombre de recurso de Amazon (ARN) de la clave de KMS asociada al cifrado de los hallazgos exportados al bucket de S3. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .

### 3. Pasos en la consola GuardDuty

- a. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
- b. En el panel de navegación, seleccione Configuración.
- c. En la página Configuración, bajo Opciones de exportación de resultados, en Bucket de S3, elija Configurar ahora (o Editar, según sea necesario).
- d. Para el ARN del bucket S3, introduzca el lugar **bucket ARN** al que desea enviar los resultados. Para ver el ARN del bucket, consulte [Ver las propiedades de un bucket de S3](#) en la Guía del usuario de Amazon S3.
- e. En ARN de la clave de KMS, ingrese el **key ARN**. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .
- f. Seleccione Save.

## Paso 4: Configurar la GuardDuty búsqueda de alertas a través de las redes sociales

GuardDuty se integra con Amazon EventBridge, que se puede utilizar para enviar los datos de los resultados a otras aplicaciones y servicios para su procesamiento. Con EventBridge él, puede utilizar GuardDuty los hallazgos para iniciar respuestas automáticas a sus hallazgos conectando los eventos de búsqueda con objetivos, como AWS Lambda las funciones, la automatización de Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) y más.

En este ejemplo, creará un tema de SNS para que sea el objetivo de una regla y, a continuación, lo utilizará EventBridge para crear una EventBridge regla a partir de la cual se recopilen los datos de los hallazgos. GuardDuty La regla resultante reenvía los detalles de los resultados a una dirección de correo electrónico. Para obtener información sobre cómo enviar resultados a Slack o Amazon Chime y cómo modificar los tipos de resultados por los que se envían las alertas, consulte [Configuración de un punto de conexión y un tema de Amazon SNS](#).

### Creación de un tema de SNS para sus alertas de resultados

1. Abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
2. En el panel de navegación, elija Temas.
3. Elija Create Topic (Crear tema).
4. En Tipo, seleccione Estándar.
5. En Nombre, escriba **GuardDuty**.
6. Elija Create Topic (Crear tema). Se abrirán los detalles del nuevo tema.
7. En la sección Suscripciones, elija Crear suscripción.
8. En Protocolo, elige Correo electrónico.
9. En Punto de conexión, introduzca la dirección de correo electrónico a la que desea enviar notificaciones.
10. Seleccione Crear suscripción.

Después de crear su suscripción, debe confirmarla a través de su dirección de correo electrónico.

11. Para comprobar si hay un mensaje de suscripción, vaya a la bandeja de entrada de su correo electrónico y, en el mensaje de suscripción, seleccione Confirmar suscripción.

 Note

Para comprobar el estado de la confirmación de correo electrónico, vaya a la consola de SNS y seleccione Suscripciones.

Para crear una EventBridge regla que recoja los GuardDuty hallazgos y les dé formato

1. Abra la EventBridge consola en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, seleccione Reglas.
3. Elija Creación de regla.
4. Escriba un nombre y una descripción para la regla.

Una regla no puede tener el mismo nombre que otra regla de la misma región y del mismo bus de eventos.

5. En Bus de eventos, elija Predeterminado.
6. En Tipo de regla, elija Regla con un patrón de evento.
7. Seleccione Siguiente.
8. En Origen de eventos, seleccione (Eventos de AWS ).
9. En la sección Patrón de eventos, seleccione Formulario de patrón de eventos.
10. En Origen de evento, seleccione Servicios de AWS .
11. En Servicio de AWS , seleccione GuardDuty.
12. En Tipo de evento, elija GuardDutyBuscar.
13. Elija Siguiente.
14. En Tipos de destino, seleccione Servicio de AWS .
15. En Seleccionar un destino, elija Tema de SNS y, en Tema, elija el nombre del tema de SNS que creó anteriormente.
16. En la sección Additional settings, en Configurar la entrada de destino, elija Transformador de entrada.

Al añadir un transformador de entrada, los datos de búsqueda de JSON enviados se GuardDuty convierten en un mensaje legible para las personas.

17. Elija Configurar transformador de entrada.

18. En la sección Transformador de entrada de destino, en Ruta de entrada, pegue el siguiente código:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

19. Para formatear el correo electrónico, en Plantilla, pegue el siguiente código y asegúrese de sustituir el texto que aparece en rojo por los valores que correspondan a la región:

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the
<region> region."
"Finding Description:"
"<Finding_Description>."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

20. Seleccione Confirmar.
21. Elija Siguiente.
22. (Opcional) Introduzca una o varias etiquetas para la regla. Para obtener más información, consulta las [EventBridge etiquetas de Amazon](#) en la Guía del EventBridge usuario de Amazon.
23. Elija Siguiente.
24. Revise los detalles de la regla y seleccione Creación de regla.
25. (Opcional) Pruebe la nueva regla generando resultados de muestra con el proceso descrito en el paso 2. Recibirá un correo electrónico por cada resultado de muestra que se genere.

## Siguientes pasos

A medida que continúe utilizándolas GuardDuty, comprenderá los tipos de hallazgos que son relevantes para su entorno. Cada vez que reciba un nuevo resultado, podrá encontrar información, como recomendaciones para corregir dicho resultado, al seleccionar Más información en la



descripción del resultado en el panel de detalles del resultado o al buscar el nombre del resultado en [GuardDuty buscar tipos](#).

Las siguientes funciones le ayudarán a GuardDuty ajustarlo para que pueda proporcionar los hallazgos más relevantes para su AWS entorno:

- Para ordenar fácilmente los resultados en función de criterios específicos, como el ID de la instancia, el ID de la cuenta, el nombre del bucket de S3, etc., puede crear filtros y guardarlos en ellos GuardDuty. Para obtener más información, consulte [Filtrar los hallazgos en GuardDuty](#).
- Si recibe resultados sobre el comportamiento esperado de su entorno, puede archivarlos automáticamente en función de los criterios que defina con las [reglas de supresión](#).
- Para evitar que las conclusiones se generen a partir de un subconjunto de direcciones IP fiables o para que las IP de los GuardDuty monitores queden fuera del ámbito de supervisión habitual, puedes configurar [listas de IP fiables y de amenazas](#).

# GuardDuty fuentes de datos fundamentales

GuardDuty utiliza las fuentes de datos fundamentales para detectar la comunicación con dominios y direcciones IP maliciosos conocidos e identificar posibles comportamientos anómalos y actividades no autorizadas. Todos los datos de registro se cifran cuando GuardDuty se transfieren de estas fuentes a otras. GuardDuty extrae varios campos de estas fuentes de registros para crear perfiles y detectar anomalías y, a continuación, descarta estos registros.

Cuando se activa GuardDuty por primera vez en una región, se ofrece una prueba gratuita de 30 días que incluye la detección de amenazas para todas las fuentes de datos fundamentales. Durante esta prueba gratuita, podrá supervisar un uso mensual estimado desglosado por cada origen de datos fundamental. Como cuenta de GuardDuty administrador delegado, puede ver el coste de uso mensual estimado desglosado por cada cuenta de miembro que pertenezca a su organización y que tenga habilitada. GuardDuty Una vez finalizada la prueba de 30 días, puede utilizarla AWS Billing para obtener información sobre el coste de uso.

El GuardDuty acceso a los eventos y registros desde estas fuentes de datos fundamentales no conlleva ningún coste adicional.

Una vez que lo GuardDuty habilite Cuenta de AWS, comenzará a monitorear automáticamente las fuentes de registro que se explican en las siguientes secciones. No necesita activar ninguna otra opción para empezar GuardDuty a analizar y procesar estas fuentes de datos y generar las correspondientes conclusiones de seguridad.

## Temas

- [AWS CloudTrail eventos de gestión](#)
- [Logs de flujo de VPC](#)
- [Registros de consultas de DNS de Route53 Resolver](#)

## AWS CloudTrail eventos de gestión

AWS CloudTrail te proporciona un historial de las llamadas a la AWS API de tu cuenta, incluidas las llamadas a la Consola de administración de AWS API realizadas con los AWS SDK, las herramientas de línea de comandos y determinados AWS servicios. CloudTrail también te ayuda a identificar qué usuarios y cuentas invocaron AWS las API de los servicios compatibles CloudTrail, la dirección IP de origen desde la que se invocaron las llamadas y el momento en que se invocaron las llamadas.

Para obtener más información, consulte [What is AWS CloudTrail](#) en la Guía del usuario de AWS CloudTrail .

GuardDuty supervisa los eventos CloudTrail de administración, también conocidos como eventos del plano de control. Estos eventos proporcionan información sobre las operaciones de gestión que se llevan a cabo con los recursos de su empresa Cuenta de AWS.

Los siguientes son ejemplos de eventos de CloudTrail administración que se GuardDuty supervisan:

- Configuración de la seguridad (operaciones de la API `AttachRolePolicy` de IAM)
- Configuración de reglas para el direccionamiento de datos (operaciones de la API `CreateSubnet` de Amazon EC2)
- Configuración del registro (operaciones AWS CloudTrail `CreateTrail` de API)

Cuando lo habilitas GuardDuty, comienza a consumir los eventos de CloudTrail administración directamente CloudTrail a través de un flujo de eventos independiente y duplicado y analiza tus registros de CloudTrail eventos.

GuardDuty no gestiona sus CloudTrail eventos ni afecta a sus CloudTrail configuraciones existentes. Del mismo modo, sus CloudTrail configuraciones no afectan a la forma en GuardDuty que consume y procesa los registros de eventos. Para gestionar el acceso y la retención de tus CloudTrail eventos, usa la consola CloudTrail de servicio o la API. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos en la](#) Guía AWS CloudTrail del usuario.

## ¿Cómo GuardDuty gestiona los eventos AWS CloudTrail globales

En la mayoría de AWS los servicios, los CloudTrail eventos se registran en el Región de AWS lugar donde se crearon. En el caso de servicios globales como AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon y CloudFront Amazon Route 53 (Route 53), los eventos solo se generan en la región en la que se producen, pero tienen una importancia mundial.

Cuando GuardDuty consume [eventos de servicio CloudTrail global](#) (GSE) con valores de seguridad, como configuraciones de red o permisos de usuario, replica esos eventos y los procesa en cada región en la que los haya activado. GuardDuty Este comportamiento ayuda a GuardDuty mantener los perfiles de usuario y rol en cada región, lo cual es vital para detectar eventos anómalos.

 Note

En el caso de los hallazgos generados a partir de estos eventos de servicio globales, el valor regional del hallazgo puede diferir del de la región en la que se GuardDuty produce la detección. Por ejemplo, un hallazgo puede mostrarse us-east-1 como la región incluso si GuardDuty crea la detección en una región diferente.

Le recomendamos que active GuardDuty todas las opciones Regiones de AWS disponibles en su Cuenta de AWS. Aunque no tengas recursos desplegados en determinadas regiones, activarlos te GuardDuty ayudará a proteger tu cuenta de posibles amenazas. Los actores de amenazas pueden lanzar ataques a través de servicios globales (como IAM o Amazon CloudFront). AWS STS Pueden intentar crear recursos no autorizados para explotar regiones en las que tu presencia es limitada. GuardDuty procesa los eventos de servicio globales en todas las regiones en las que ha activado el servicio, incluidas las regiones predeterminadas y las que están habilitadas. Esto ayuda a GuardDuty detectar actividades potencialmente sospechosas en todas sus regiones Cuenta de AWS, incluidas las regiones en las que no utiliza los recursos de forma activa.

## Logs de flujo de VPC

La característica de registros de flujo de la VPC de Amazon VPC captura información acerca del tráfico IP entrante y saliente de las interfaces de red asociadas a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de su entorno de AWS .

Cuando lo habilita GuardDuty, comienza a analizar inmediatamente los datos del registro de flujo de VPC de las instancias de Amazon EC2 de su cuenta. GuardDuty consume estos datos a través de un flujo de registros de flujo independiente y duplicado. No necesitas crear ni configurar registros de flujo de VPC en tu cuenta para acceder GuardDuty a estos datos. Este proceso no afecta a ninguna configuración de los registros de flujo existentes.

### [Protección de Lambda](#)

Lambda Protection es una mejora opcional de Amazon. GuardDuty En la actualidad, la supervisión de la actividad de la red de Lambda en GuardDuty incluye los registros de flujo de Amazon VPC de todas las funciones de Lambda de su cuenta, incluso los registros que no utilizan redes de VPC. Para proteger su función Lambda de posibles amenazas de seguridad, tendrá que configurar Lambda Protection en su cuenta. GuardDuty Para obtener más información, consulte [Protección de Lambda](#).

## GuardDuty Supervisión del tiempo de ejecución

Si administra el agente de seguridad (de forma manual o a través de él GuardDuty) en EKS Runtime Monitoring o Runtime Monitoring for EC2, y si actualmente GuardDuty está desplegado en una instancia de Amazon EC2 y recibe [Tipos de eventos de tiempo de ejecución recopilados](#) el de esta instancia GuardDuty, no se le Cuenta de AWS cobrará por el análisis de los registros de flujo de VPC de esta instancia de Amazon EC2. Esto ayuda a GuardDuty evitar el doble de los gastos de uso de la cuenta.

GuardDuty no administra tus registros de flujo ni los hace accesibles en tu cuenta. Para administrar el acceso y la retención de los registros de flujo, debe configurar la característica Registros de flujo de VPC.

## Registros de consultas de DNS de Route53 Resolver

Si utiliza resolutores de AWS DNS para sus instancias de Amazon EC2 (la configuración predeterminada), GuardDuty podrá acceder a los registros de consultas de DNS de Route53 Resolver de solicitudes y respuestas y procesarlos a través de los resolutores de DNS internos. AWS Si utilizas otro solucionador de DNS, como OpenDNS o GoogleDNS, o si configuras tus propios solucionadores de DNS, no podrás acceder a los datos de esta fuente de datos ni GuardDuty procesarlos.

Cuando lo habilitas GuardDuty, comienza inmediatamente a analizar los registros de consultas de DNS del Route53 Resolver a partir de un flujo de datos independiente. Este flujo de datos es independiente de los datos proporcionados a través de la característica [Registro de consultas del solucionador de Route 53](#). La configuración de esta función no afecta al GuardDuty análisis.

### Note

GuardDuty no admite la supervisión de los registros de DNS para las instancias de Amazon EC2 que se lanzan AWS Outposts porque la función de registro de Amazon Route 53 Resolver consultas no está disponible en ese entorno.

# GuardDuty Detección de amenazas extendida

GuardDuty La detección extendida de amenazas detecta automáticamente los ataques en varias etapas que abarcan fuentes de datos, varios tipos de AWS recursos y tiempo, en un Cuenta de AWS instantánea. Con esta capacidad, GuardDuty se centra en la secuencia de varios eventos que observa mediante la supervisión de diferentes tipos de fuentes de datos. La detección extendida de amenazas correlaciona estos eventos para identificar los escenarios que se presentan como una amenaza potencial para su AWS entorno y, a continuación, genera una búsqueda de la secuencia de ataque.

## Temas

- [Ejemplos de escenarios de amenazas en la secuencia de ataque](#)
- [Funcionamiento](#)
- [Habilitar planes de protección para maximizar la detección de amenazas](#)
- [Detección de amenazas ampliada en la consola GuardDuty](#)
- [Descripción y administración de resultados de secuencias de ataques](#)
- [Recursos adicionales](#)

## Ejemplos de escenarios de amenazas en la secuencia de ataque

La detección extendida de amenazas cubre los escenarios de amenazas que implican compromisos relacionados con el uso indebido de AWS credenciales, intentos de comprometer datos en buckets de Amazon S3 y comprometer recursos de contenedores y Kubernetes en clústeres de Amazon EKS. Un único resultado puede abarcar una secuencia de ataque completa. Por ejemplo, en la siguiente lista se describen los escenarios que pueden detectarse: GuardDuty

Ejemplo 1: AWS las credenciales y los datos del bucket de Amazon S3 están comprometidos

- Un actor de amenazas que obtiene acceso no autorizado a una carga de trabajo informática.
- Luego, el actor realiza una serie de acciones, como aumentar los privilegios y establecer la persistencia.
- Por último, el actor que extrae datos de un recurso de Amazon S3.

Ejemplo 2: Compromiso con el clúster de Amazon EKS

- Un actor de amenazas intenta explotar una aplicación contenedora dentro de un clúster de Amazon EKS.

- El actor usa ese contenedor comprometido para obtener tokens de cuentas de servicio privilegiadas.
- Luego, el actor aprovecha estos privilegios elevados para acceder a secretos de Kubernetes o recursos de AWS confidenciales a través de las identidades de los pods.

Debido a la naturaleza de los escenarios de amenaza asociados, GuardDuty considera que todos ellos [Tipos de resultados de secuencias de ataque](#) son críticos.

En el siguiente vídeo se muestra cómo utilizar la Detección Extendida de Amenazas.

## [Demostración de Amazon GuardDuty Extended Threat Detection](#)

## Funcionamiento

Cuando habilitas Amazon GuardDuty en tu cuenta en una cuenta específica Región de AWS, la detección extendida de amenazas también está habilitada de forma predeterminada. El uso de Detección Extendida de Amenazas no conlleva ningún costo adicional. De forma predeterminada, correlaciona los eventos en todos los [Orígenes de datos fundamentales](#). Sin embargo, si habilita más planes de GuardDuty protección, como S3 Protection, EKS Protection y Runtime Monitoring, se abrirán nuevos tipos de detecciones de secuencias de ataques al ampliar la gama de fuentes de

eventos. Esto podría ayudar a realizar un análisis de amenazas más exhaustivo y a detectar mejor las secuencias de ataque. Para obtener más información, consulte [Habilitar planes de protección para maximizar la detección de amenazas](#).

GuardDuty correlaciona varios eventos, incluidas las actividades y los hallazgos de la API. GuardDuty Estos eventos se denominan señales. A veces, es posible que se produzcan eventos en su entorno que, por sí solos, no se presenten como una amenaza potencial clara. GuardDuty los califica de señales débiles. Con la detección ampliada de amenazas, GuardDuty identifica cuándo una secuencia de varias acciones se corresponde con una actividad potencialmente sospechosa y genera una secuencia de ataque detectada en tu cuenta. Estas múltiples acciones pueden incluir señales débiles y GuardDuty hallazgos ya identificados en tu cuenta.

#### Note

Al correlacionar los eventos con las secuencias de ataque, la Detección Extendida de Amenazas no tiene en cuenta las conclusiones archivadas, incluidas las que se archivan automáticamente debido a [Reglas de supresión](#). Este comportamiento garantiza que solo las señales activas y relevantes contribuyan a la detección de la secuencia de ataque. Para asegurarse de que esto no lo afecte, consulte las normas de supresión vigentes en su cuenta. Para obtener más información, consulte [Uso de reglas de supresión con Detección Extendida de Amenazas](#).

GuardDuty también está diseñado para identificar posibles comportamientos de ataque recientes o en curso (en un plazo de 24 horas) en tu cuenta. Por ejemplo, un ataque podría comenzar cuando un actor accede involuntariamente a una carga de trabajo de cómputo. Luego, el actor realizaría una serie de pasos, que incluían la enumeración, la escalada de privilegios y la exfiltración de credenciales. AWS Estas credenciales podrían utilizarse para comprometer aún más los datos o acceder de forma malintencionada a ellos.

## Habilitar planes de protección para maximizar la detección de amenazas

La detección ampliada de amenazas se activa automáticamente en todas las GuardDuty cuentas y evalúa de forma predeterminada las señales de todos los planes de protección habilitados en la cuenta. GuardDuty [Las fuentes de datos fundamentales](#) proporcionan señales importantes para detectar varias secuencias de ataques. Por ejemplo, con la detección de amenazas básica,



GuardDuty puede identificar una secuencia de ataque potencial a partir de la actividad de descubrimiento de privilegios de IAM en las API de Amazon S3 y detectar alteraciones posteriores en el plano de control de S3, como los cambios que hacen que la política de recursos de bucket sea más permisiva. Sin embargo, otras secuencias de ataque requieren señales avanzadas que solo están disponibles en planes de protección avanzados, como la supervisión del tiempo de ejecución, la protección de S3 y la supervisión de registros de auditoría de EKS.

## Temas

- [Detección de secuencias de ataque en clústeres de Amazon EKS](#)
- [Detección de secuencias de ataques en los buckets de Amazon S3](#)
- [Detección de secuencias de ataques en clústeres de Amazon ECS](#)
- [Detección de secuencias de ataques en grupos de instancias de Amazon EC2](#)

## Detección de secuencias de ataque en clústeres de Amazon EKS

GuardDuty correlacionó varias señales de seguridad en los registros de auditoría de EKS, el comportamiento de los procesos en tiempo de ejecución y la actividad de las AWS API para detectar patrones de ataque sofisticados. Para beneficiarse de la Detección Extendida de Amenazas para EKS, debe habilitar al menos una de estas funciones: EKS Protection o el monitoreo del tiempo de ejecución (con el complemento EKS). EKS Protection supervisa las actividades del plano de control mediante registros de auditoría, mientras que Runtime Monitoring observa los comportamientos dentro de los contenedores.

Para obtener la máxima cobertura y una detección integral de amenazas, GuardDuty recomienda habilitar ambos planes de protección. Juntos, crean una vista completa de sus clústeres de EKS, lo que GuardDuty permite detectar patrones de ataque complejos. Por ejemplo, puede identificar un despliegue anómalo de un contenedor privilegiado (detectado con EKS Protection), seguido de intentos de persistencia, minería de criptomonedas y creación de shell inversos dentro de ese contenedor (detectados con Runtime Monitoring). GuardDuty representa estos eventos relacionados como un único hallazgo de gravedad crítica, denominado [AttackSequence:EKS/CompromisedCluster](#). Al activar ambos planes de protección, los resultados de la secuencia de ataque abarca los siguientes escenarios de amenaza:

- Compromiso de los contenedores que ejecutan aplicaciones web vulnerables
- Acceso no autorizado mediante credenciales mal configuradas
- Intentos de escalar los privilegios

- Solicitudes de la API sospechosas
- Intentos para acceder a los datos de forma malintencionada

La siguiente lista proporciona detalles sobre cuándo se activan estos planes de protección dedicados de forma individual:

## EKS Protection

La activación de EKS Protection permite GuardDuty detectar secuencias de ataques que involucren actividades en el plano de control del clúster de Amazon EKS. Esto permite correlacionar GuardDuty los registros de auditoría de EKS y la actividad de la AWS API. Por ejemplo, GuardDuty puede detectar una secuencia de ataque en la que un actor intenta acceder sin autorización a los secretos del clúster, modifica los permisos del control de acceso basado en roles (RBAC) de Kubernetes y crea grupos privilegiados. Para obtener información sobre cómo habilitar este plan de protección, consulte [EKS Protection](#).

## Runtime Monitoring de Amazon EKS

Al habilitar Runtime Monitoring para los clústeres de Amazon EKS, se puede mejorar la detección de la secuencia de ataques de EKS con visibilidad a nivel de contenedor. GuardDuty Esto ayuda a GuardDuty detectar posibles procesos maliciosos, comportamientos sospechosos en tiempo de ejecución y posibles ejecuciones de malware. Por ejemplo, GuardDuty puede detectar una secuencia de ataque en la que un contenedor comienza a mostrar un comportamiento sospechoso, como procesos de minería criptográfica o establecimiento de conexiones con puntos finales maliciosos conocidos. Para obtener información sobre cómo habilitar este plan de protección, consulte [Supervisión en tiempo de ejecución](#).

Si no habilitas la protección de EKS o la supervisión del tiempo de ejecución, no GuardDuty podrás generar anuncios individuales. [Tipos de resultados de la protección de EKS](#) [Tipos de resultados de la supervisión en tiempo de ejecución](#) Por lo tanto, no GuardDuty podrá detectar secuencias de ataques en varias etapas que impliquen hallazgos asociados.

## Detección de secuencias de ataques en los buckets de Amazon S3

Al habilitar S3 Protection GuardDuty , podrá detectar secuencias de ataques que impliquen intentos de comprometer datos en sus buckets de Amazon S3. Sin S3 Protection, GuardDuty puede detectar cuándo su política de recursos de bucket de S3 se vuelve demasiado permisiva. Al activar S3

Protection, GuardDuty obtiene la capacidad de detectar posibles actividades de exfiltración de datos que puedan producirse después de que su depósito de S3 se vuelva demasiado permisivo.

Si S3 Protection no está habilitada, no GuardDuty podrá generar datos individuales. [Tipos de resultados de la S3 Protection](#) Por lo tanto, no GuardDuty podrá detectar secuencias de ataques en varias etapas que impliquen hallazgos asociados. Para obtener información sobre cómo habilitar este plan de protección, consulte [S3 Protection](#).

## Detección de secuencias de ataques en clústeres de Amazon ECS

GuardDuty puede identificar secuencias de ataque, como procesos maliciosos, conexiones a puntos finales maliciosos o comportamientos de minería de criptomonedas dentro de los contenedores de ECS. Al correlacionar diversas señales entre la actividad de la red, el comportamiento de los procesos en tiempo de ejecución y la actividad de las AWS API, GuardDuty puede identificar patrones de ataque complejos que podrían pasar desapercibidos en las detecciones individuales y mapear el vector de ataque completo.

GuardDuty representa estos eventos relacionados como un único hallazgo de gravedad crítica, denominado. `AttackSequence:ECS/CompromisedCluster` La búsqueda de la secuencia de ataque abarca los siguientes escenarios de amenaza:

- Compromiso de los contenedores que ejecutan servicios vulnerables
- Ejecución no autorizada de herramientas, malware o procesos de minería de criptomonedas sospechosos
- Intentos de escalar los privilegios
- Comunicación con puntos finales sospechosos

### Important

La detección extendida de amenazas para ECS requiere la supervisión del tiempo de ejecución para Fargate o EC2, según el tipo de infraestructura de ECS. La supervisión del tiempo de ejecución observa los comportamientos de los contenedores de ECS que se ejecutan en las instancias de Fargate y EC2. No se admite el ECS en las instancias EC2 gestionadas.

## Detección de secuencias de ataques en grupos de instancias de Amazon EC2

GuardDuty puede identificar las secuencias de ataques que afectan a instancias individuales o grupos de instancias que comparten atributos comunes, como grupos de Auto Scaling, perfiles de instancias de IAM, plantillas de lanzamiento, CloudFormation pilas, AMI o ID de VPC. Estas instancias pueden mostrar comportamientos sospechosos, como procesos maliciosos, conexiones a puntos finales malintencionados, minería de criptomonedas o uso anómalo de las credenciales de las instancias de EC2.

La búsqueda de la secuencia de ataque detecta los siguientes escenarios de amenaza:

- Compromiso de las instancias que ejecutan servicios vulnerables
- Uso de credenciales de instancia Amazon EC2 obtenidas mediante IMDS desde fuera de la AWS cuenta a la que se emitieron las credenciales
- Utilícelas como infraestructura para ataques como el proxy, el escaneo o la denegación de servicio
- Ejecución no autorizada de herramientas, malware o procesos de minería de criptomonedas sospechosos
- Comunicación con puntos finales sospechosos

La detección extendida de amenazas ayuda a identificar estas amenazas. GuardDuty representa estos eventos relacionados como un único hallazgo de gravedad crítica, denominado.

`AttackSequence:EC2/CompromisedInstanceGroup`

Para mejorar las capacidades de detección de amenazas ampliadas para EC2, habilite la monitorización del tiempo de ejecución. La combinación de la monitorización básica GuardDuty, que monitorea CloudTrail la actividad de la red, y la monitorización del tiempo de ejecución, que observa los comportamientos de los procesos y las llamadas al sistema en las instancias, proporciona una detección de amenazas más completa. Esta supervisión integrada permite GuardDuty detectar secuencias de ataques sofisticadas, como el acceso no autorizado mediante credenciales mal configuradas, los intentos de escalada de privilegios y el acceso no autorizado a datos confidenciales. Al correlacionar estas diversas señales, GuardDuty puede identificar patrones de ataque complejos que podrían pasar desapercibidos en las detecciones individuales y mapear el vector de ataque completo.

# Detección de amenazas ampliada en la consola GuardDuty

De forma predeterminada, la página de detección extendida de amenazas de la GuardDuty consola muestra el estado como Activado. Con la detección de amenazas básica, el estado representa que GuardDuty puede detectar una posible secuencia de ataque que implique una actividad de descubrimiento de privilegios de IAM en las API de Amazon S3 y detectar alteraciones posteriores en el plano de control de S3.

Siga los siguientes pasos para acceder a la página de detección ampliada de amenazas de la consola: GuardDuty

1. Puede abrir la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Detección Extendida de Amenazas.

Esta página proporciona detalles sobre los escenarios de amenazas que cubre la Detección Extendida de Amenazas.

3. En la página Detección Extendida de Amenazas, consulte la sección Planes de protección relacionados. Si desea habilitar planes de protección dedicados para mejorar la cobertura de detección de amenazas en su cuenta, seleccione la opción Configurar para ese plan de protección.

## Descripción y administración de resultados de secuencias de ataques

Los hallazgos de la secuencia de ataque son iguales a GuardDuty los demás hallazgos de su cuenta. Puede verlos en la página de resultados de la GuardDuty consola. Para obtener información sobre cómo ver los resultados, consulte [Página de hallazgos en la GuardDuty consola](#).

Al igual que otros GuardDuty hallazgos, los hallazgos de la secuencia de ataque también se envían automáticamente a Amazon EventBridge. Según su configuración, los resultados de la secuencia de ataques también se exportan a un destino de publicación (bucket de Amazon S3). Para establecer un nuevo destino de publicación o actualizar uno existente, consulte [Exportar los resultados generados a Amazon S3](#)

## Recursos adicionales

Consulte las siguientes secciones para comprender mejor las secuencias de ataque:

- Tras obtener más información sobre la Detección Extendida de Amenazas y las secuencias de ataque, puede generar ejemplos de tipos de resultados de secuencias de ataque siguiendo los pasos que se indican en [Ejemplos de hallazgos](#).
- Información sobre [Tipos de resultados de secuencias de ataque](#).
- Revise los resultados y explore los detalles de los resultados asociados con [Detalles de los resultados de la secuencia de ataque](#).
- Priorice y aborde los tipos de resultados de secuencias de ataques siguiendo los pasos correspondientes a los recursos afectados asociados en [Corrección de resultados](#).

# Configuración de planes de protección

La página de planes de protección de la GuardDuty consola consolida todas las configuraciones del plan de protección en una sola página. Puede activar o desactivar los planes de protección, configurar los ajustes de activación automática de AWS Organizations las cuentas y ver las estadísticas de las cuentas de los miembros desde un solo lugar.

## Descripción general de

La página unificada de planes de protección reemplaza la necesidad de ir a las páginas de los planes de protección individuales para realizar la configuración. La navegación de la consola muestra un enlace único a los planes de protección.

La página muestra los planes de protección en el siguiente orden:

1. Fundamental GuardDuty: habilita o deshabilita GuardDuty y configura la activación automática de las AWS Organizations cuentas.
2. Protección S3: supervise los eventos de datos de Amazon S3 para detectar posibles amenazas a sus datos.
3. Supervisión del tiempo de ejecución: supervise los eventos a nivel del sistema operativo para las cargas de trabajo de EKS, ECS y EC2.
4. Registros de auditoría de EKS: supervise los registros de auditoría de Amazon EKS para detectar posibles amenazas a sus clústeres.
5. Protección de RDS: supervise la actividad de inicio de sesión de RDS para detectar posibles amenazas a sus bases de datos.
6. Protección Lambda: supervise la actividad de la red de funciones Lambda para detectar posibles amenazas.

Cada plan de protección muestra la siguiente información:

- Estado de la función (habilitada o no habilitada)
- Auto-enable estado de las AWS Organizations cuentas
- AWS Organizations estadísticas de miembros de cuentas

# Configuración de todos los planes de protección

Para configurar los planes de protección desde la página unificada, siga los siguientes pasos:

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. Todos los contenedores del plan de protección pasan al modo de edición.
4. Realice cambios en alguno de los planes de protección o en todos ellos. Para cada plan, puedes activar o desactivar la función y configurar la configuración de activación automática para las cuentas de la organización.
5. Elija Save all. Aparece un modal de confirmación que resume todos los cambios, incluidos el nombre de la función, el estado y el valor de activación automática de cada plan modificado.
6. Revise los cambios y elija Confirmar y guardar. Todos los cambios se guardan por lotes.

## Auto-enable opciones

Cada plan de protección proporciona las siguientes opciones de activación automática para las cuentas de la organización:

### Habilitar para todas las cuentas

Habilite la función para todas GuardDuty las cuentas activas de la organización. Esto incluye las cuentas nuevas que se unen a la organización.

### Habilitar para nuevas cuentas

Esto se aplicará a todas las cuentas nuevas cuando se agreguen a la organización.

### No activar automáticamente

La función no se habilita automáticamente para las cuentas de la organización.

Para el GuardDuty contenedor Foundational, las opciones de activación automática utilizan una redacción específica AWS Organizations:

- Habilitar para todas las AWS Organizations cuentas: habilite GuardDuty para todas las cuentas activas de su. AWS Organizations



- Habilitar para AWS Organizations cuentas nuevas: esto se aplicará a todas las cuentas nuevas cuando se agreguen a la suya AWS Organizations.

## Configuración de supervisión del tiempo de ejecución

El contenedor Runtime Monitoring tiene una estructura principal e secundaria con las siguientes subfunciones:

- Supervisión del tiempo de ejecución (EKS)
- Supervisión del tiempo de ejecución (ECS)
- Supervisión del tiempo de ejecución (EC2)

La configuración de la infraestructura de supervisión del tiempo de ejecución se muestra en una sección ampliable. Esta configuración es necesaria para que funcione la supervisión del tiempo de ejecución de EKS, ECS y EC2, pero no proporciona protección por sí sola.

## Restricciones bidireccionales

Las subfunciones y la infraestructura de Runtime Monitoring tienen las siguientes relaciones:

Habilite una subfunción

Activa automáticamente la infraestructura de monitoreo del tiempo de ejecución si estaba deshabilitada.

Deshabilita una subfunción

No afecta a la infraestructura de supervisión del tiempo de ejecución.

Active la infraestructura de monitoreo del tiempo de ejecución

No afecta a las subfunciones.

Deshabilite la infraestructura de monitoreo del tiempo

Desactiva todas las subfunciones.

Para la configuración de activación automática, se aplican las siguientes restricciones:

## Aumentar la activación automática de una subfunción

La infraestructura de monitoreo del tiempo de ejecución siempre es igual al máximo de todas las subfunciones.

## Reducir la activación automática de una subfunción

La infraestructura de monitorización del tiempo de ejecución vuelve a calcular el nuevo máximo de todas las subfunciones.

## Aumente la activación automática de la infraestructura de monitoreo del tiempo de ejecución

Sin efecto en las subfunciones.

La infraestructura de monitoreo de menor tiempo de ejecución se habilita automáticamente

Reduce cualquier subfunción que supere el nuevo valor principal para igualarlo.

### Note

Aparece una advertencia cuando alguna subfunción tiene un valor diferente al de Runtime Monitoring Infrastructure (ya sea al activar o desactivar automáticamente la discordancia). Al habilitar solo la infraestructura de monitoreo en tiempo de ejecución, se pasa al modo manual sin la administración automática del agente de seguridad. Active la supervisión del tiempo de ejecución para EKS, ECS o EC2 para gestionar automáticamente el agente de seguridad de sus cargas de trabajo.

## Estadísticas de la organización

Cada contenedor del plan de protección muestra las estadísticas de las cuentas de los miembros que muestran cuántas cuentas tienen habilitada la función. Si las estadísticas de la organización aún no están disponibles (por ejemplo, dentro de las primeras 24 horas después de habilitarla), la página muestra un indicador de estado pendiente con un mensaje en el que se explica que se están recopilando estadísticas.

## Integración de la página de cuentas

El botón Editar de la sección de activación automática de la página Cuentas lo redirige a la página Planes de protección en lugar de abrir el modal de configuración anterior.

# GuardDuty Protección EKS

## Note

Puede configurar EKS Protection junto con todos los demás planes de protección desde una sola página de la GuardDuty consola. Para obtener más información, consulte [Configuración de planes de protección](#).

EKS Protection le ayuda a detectar posibles riesgos de seguridad en los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) de su entorno. AWS Por ejemplo, le ayuda a detectar cuándo un actor no autenticado que intenta recopilar secretos o credenciales de su clúster está accediendo a un clúster de EKS mal configurado. AWS EKS Protection utiliza los registros de auditoría de EKS para analizar las actividades de los usuarios y las aplicaciones.

Al activar EKS Protection, comienza a supervisar GuardDuty automáticamente los clústeres de Amazon EKS para detectar posibles amenazas a la seguridad. GuardDuty utiliza su propia transmisión independiente para recopilar y analizar [Registros de auditoría de EKS en EKS Protection](#); no se requiere ninguna configuración adicional.

Cuando GuardDuty detecta una amenaza potencial basándose en la supervisión del registro de auditoría de EKS, genera una comprobación de seguridad. Para obtener información sobre los tipos de hallazgos que se GuardDuty pueden generar al activar la protección de EKS, consulte [Tipos de resultados de la protección de EKS](#).

## Note

Para ver los registros de auditoría de EKS en su cuenta (opcional), puede configurar el registro del plano de control de Amazon EKS para enviar los registros de auditoría a CloudWatch Logs. Esta configuración es independiente de la protección de EKS y no es necesaria para poder monitorizar la seguridad en ella GuardDuty.

## Prueba gratuita de 30 días

- Al GuardDuty activarla Región de AWS por primera vez Cuenta de AWS de forma automática, dispondrá de una prueba gratuita de 30 días. En este caso, también GuardDuty habilitará la protección EKS, que está incluida en la prueba gratuita de 30 días.

- Si ya está utilizando EKS Protection GuardDuty y decide activarlo por primera vez, su cuenta de esta región dispondrá de una prueba gratuita de 30 días para utilizar EKS Protection.
- Puede optar por desactivar EKS Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, GuardDuty no desactiva automáticamente la protección de EKS. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Monitorear el uso y estimar los costos](#).

Al deshabilitar EKS Protection, deja de supervisar y analizar GuardDuty inmediatamente los registros de auditoría de EKS de sus recursos de Amazon EKS.

Es posible que la protección EKS no esté disponible en todos los Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte [Region-specific disponibilidad de funciones](#).

 Note

La Supervisión en tiempo de ejecución de EKS se administra como parte de la Supervisión en tiempo de ejecución. Para obtener más información, consulte [GuardDuty Supervisión del tiempo de ejecución](#).

## Registros de auditoría de EKS en EKS Protection

Los registros de auditoría de EKS capturan las acciones secuenciales del clúster de Amazon EKS, incluidas las actividades de los usuarios, las aplicaciones que utilizan la API de Kubernetes y el plano de control. El registro de auditoría es un componente de todos los clústeres de Kubernetes.

Para obtener más información, consulte la sección de [auditorías](#) en la documentación de Kubernetes.

Amazon EKS permite que los registros de auditoría de EKS se ingieran como CloudWatch registros de Amazon mediante la función de [registro del plano de control de EKS](#). GuardDuty no gestiona el registro del plano de control de Amazon EKS ni permite que los registros de auditoría de EKS estén accesibles en su cuenta si no los ha habilitado para Amazon EKS. Para administrar el acceso a los registros de auditoría de EKS y su retención, deberá configurar la característica de registro del plano de control de Amazon EKS. Para obtener más información, consulte [Habilitar y deshabilitar registros de plano de control](#) en la Guía del usuario de Amazon EKS.

# Habilitar EKS Protection en entornos de varias cuentas

En un entorno de cuentas múltiples, solo la cuenta de GuardDuty administrador delegado tiene la opción de habilitar o deshabilitar la función EKS Protection; para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Esta cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente EKS Protection para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre los entornos de varias cuentas, consulta [Administrar varias cuentas en Amazon](#). GuardDuty

## Configuración de EKS Audit Log Monitoring para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión del registro de auditoría de EKS para la cuenta de GuardDuty administrador delegado.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. En los registros de auditoría de EKS, puede ver el estado de configuración actual de la supervisión de los registros de auditoría de EKS.
4. Realice una de las siguientes acciones:

#### Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
- Seleccione Save.

#### Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.

- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Save.

## API/CLI

Ejecute la operación de la API [updateDetector](#) con su propio ID de detector regional y pase el name del objeto features como EKS\_AUDIT\_LOGS y status como ENABLED o DISABLED.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#)API.

Puede activar o desactivar la supervisión del registro de auditoría de EKS ejecutando el siguiente AWS CLI comando. Asegúrese de utilizar una cuenta de GuardDuty administrador delegado válida *detector ID*.

### Note

El siguiente código de ejemplo habilita la supervisión de registros de auditoría de EKS. Asegúrese de *12abc34d567e8fa901bc2d34e56789f0* sustituirla por la cuenta detector-id de GuardDuty administrador delegado y por *55555555555* la cuenta Cuenta de AWS de administrador delegado GuardDuty .

Para encontrar la correspondiente detectorId a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#)API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features '[{"Name": "EKS_AUDIT_LOGS", "Status": "ENABLED"}]'
```

Para deshabilitar la supervisión de registros de auditoría de EKS, sustituya ENABLED por DISABLED.

## Auto-enable Supervisión del registro de auditoría de EKS para todas las cuentas de los miembros

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros existentes en la organización.

### Console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

#### Uso de la página de planes de protección

1. En el panel de navegación, elija Planes de protección.
2. Elija Configurar todas las habilitaciones. En los registros de auditoría de EKS, puede ver el estado actual de la supervisión de los registros de auditoría de EKS para las cuentas de los miembros activos de su organización.
3. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la supervisión de registros de auditoría de EKS para las cuentas nuevas y existentes de la organización.
4. Seleccione Guardar todo y, a continuación, seleccione Confirmar y guardar.

#### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

#### Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de registros de auditoría de EKS.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas y desea personalizar la configuración de la Supervisión de registros de auditoría de EKS para cuentas específicas de su organización, consulte [Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros](#).

## API/CLI

- Para activar o desactivar de forma selectiva la monitorización del registro de auditoría de EKS para sus cuentas de miembros, ejecute la operación de la [updateMemberDetectors](#) API con la suya propia *detector ID*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitación de la Supervisión de registros de auditoría de EKS para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en todas las cuentas de miembros activos existentes en la organización.



## Console

1. Inicia sesión en Consola de administración de AWS y abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. En Registros de auditoría de EKS, en la sección Cuentas de miembros activos, elija Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Save.

## API/CLI

- Para activar o desactivar de forma selectiva la monitorización de registros de auditoría de EKS para sus cuentas de miembros, ejecute la operación de la [updateMemberDetectors](#) API con la suya propia *detector ID*.
- El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
```

### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Auto-enable Supervisión del registro de auditoría de EKS para cuentas de nuevos miembros

Las cuentas de los miembros recién agregadas deben habilitarse GuardDuty antes de seleccionar la configuración del análisis de GuardDuty-initiated malware. Las cuentas de los miembros gestionadas mediante invitación pueden configurar manualmente la detección de GuardDuty-initiated malware para sus cuentas. Para obtener más información, consulte [Step 3 - Accept an invitation](#).

Elija su método de acceso preferido para habilitar la supervisión de registros de auditoría de EKS en las cuentas de miembros nuevos que se unen a la organización.

### Console

La cuenta de GuardDuty administrador delegado puede habilitar la supervisión del registro de auditoría de EKS para las cuentas de los nuevos miembros de una organización, mediante la página de supervisión del registro de auditoría de EKS o la página de cuentas.

Habilitación automática de la Supervisión de registros de auditoría de EKS para las cuentas de miembros nuevos

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

- Mediante la página de planes de protección:

1. En el panel de navegación, elija Planes de protección.
2. Elija Configurar todas las habilitaciones. En Registros de auditoría de EKS, configure la configuración de activación automática.
3. Elija Configurar cuentas manualmente.
4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, la supervisión de registros de auditoría de EKS se habilite automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
5. Seleccione Save.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione Auto-enable las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de registros de auditoría de EKS.
4. Seleccione Save.

## API/CLI

- Para activar o desactivar de forma selectiva la monitorización del registro de auditoría de EKS para sus nuevas cuentas, ejecute la operación de la [UpdateOrganizationConfiguration](#) API con la suya propia *detector ID*.
- El siguiente ejemplo muestra cómo puede habilitar la supervisión de registros de auditoría de EKS para los nuevos miembros que se unan a su organización. También puede pasar una lista de ID de cuentas separadas por un espacio.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
```

## Activación o desactivación de forma selectiva de la supervisión de registros de auditoría de EKS para las cuentas de miembros

Elija su método de acceso preferido para activar o desactiva la supervisión de registros de auditoría de EKS en cuentas de miembros selectivas en la organización.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna Supervisión de registros de auditoría de EKS para ver el estado de su cuenta de miembro.

### 3. Activación o desactivación de la Supervisión de registros de auditoría de EKS

Seleccione una cuenta que desee configurar para la Supervisión de registros de auditoría de EKS. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione Supervisión de registros de auditoría de EKS y, a continuación, elija la opción adecuada.

## API/CLI

Para activar o desactivar de forma selectiva la monitorización del registro de auditoría de EKS para sus cuentas de miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia. *detector ID*

El siguiente ejemplo muestra cómo se puede habilitar la supervisión de registros de auditoría de EKS para una sola cuenta de miembro. Para desactivarlo, sustituya ENABLED por DISABLED. También puede pasar una lista de ID de cuentas separadas por un espacio.

Para encontrar la correspondiente detectorId a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
"ENABLED"}]'
```

## Habilitar EKS Protection para una cuenta independiente

Las cuentas independientes son las que toman la decisión de habilitar o desactivar un plan de protección en la cuenta de AWS en una región específica.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a usted. Para obtener más información sobre la administración de varias cuentas, consulte [Habilitar EKS Protection en entornos de varias cuentas](#).

Tras activar EKS Protection, GuardDuty empezará a supervisar los registros de auditoría de EKS de los clústeres de Amazon EKS de su cuenta.

Elija el método de acceso que prefiera para habilitar la Protección EKS en la cuenta independiente.

## Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el selector de Regiones que aparece en la esquina superior derecha, seleccione una región en la que desee habilitar la protección de EKS.
3. En el panel de navegación, elija Planes de protección.
4. Elija Configurar todas las habilitaciones. En Registros de auditoría de EKS, seleccione Activar para activar la protección de EKS.
5. Selecciona Guardar todo y, a continuación, selecciona Confirmar y guardar.

## API/CLI

- Ejecute la operación de la [updateDetector](#) API utilizando el ID del detector regional de la cuenta de GuardDuty administrador delegado y pasando el nombre del features objeto como EKS\_AUDIT\_LOGS y su estado como ENABLED.

También puede habilitar EKS Protection mediante la ejecución de un comando de la AWS CLI . Ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID de detector de su cuenta y `us-east-1` por la región en la que desee activar la protección EKS.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]
```

# GuardDuty Protección S3

## Note

Puede configurar S3 Protection junto con todos los demás planes de protección desde una sola página de la GuardDuty consola. Para obtener más información, consulte [Configuración de planes de protección](#).

S3 Protection le ayuda a detectar posibles riesgos de seguridad para los datos, como la exfiltración y la destrucción de datos, en sus depósitos de Amazon Simple Storage Service (Amazon S3). GuardDuty monitorea AWS CloudTrail los eventos de datos de Amazon S3, lo que incluye operaciones de API a nivel de objeto para identificar estos riesgos en todos los buckets de Amazon S3 de su cuenta.

Cuando GuardDuty detecta una amenaza potencial en función del monitoreo de eventos de datos de S3, genera una comprobación de seguridad. Para obtener información sobre los tipos de hallazgos que se GuardDuty pueden generar al activar S3 Protection, consulte [GuardDuty Tipos de búsqueda de protección S3](#).

De forma predeterminada, la detección de amenazas fundamental incluye la supervisión de [AWS CloudTrail eventos de gestión](#) para identificar posibles amenazas en los recursos de Amazon S3. Este origen de datos es diferente de los eventos de datos de AWS CloudTrail para S3, ya que ambos supervisan diferentes tipos de actividades en el entorno.

Puede habilitar S3 Protection en una cuenta de cualquier región en la que se GuardDuty [admita esta función](#). Esto le ayudará a monitorear CloudTrail los eventos de datos de S3 en esa cuenta y región. Tras activar S3 Protection, GuardDuty podrá monitorizar completamente sus depósitos de Amazon S3 y detectar posibles accesos sospechosos a los datos almacenados en sus depósitos de S3.

Para utilizar la protección de S3, no es necesario habilitar ni configurar explícitamente el registro de eventos de datos de S3 en AWS CloudTrail.

## Prueba gratuita de 30 días

En la siguiente lista se explica cómo funciona la prueba gratuita de 30 días para la cuenta:

- Cuando lo GuardDuty habilitas Cuenta de AWS en una nueva región por primera vez, obtienes una prueba gratuita de 30 días. En este caso, también GuardDuty habilitará S3 Protection, que se incluye en la prueba gratuita.
- Si ya está utilizando S3 Protection GuardDuty y decide activarlo por primera vez, su cuenta de esta región dispondrá de una prueba gratuita de 30 días para utilizar S3 Protection.
- Puede optar por desactivar la S3 Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, la protección de S3 no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#).

## AWS CloudTrail eventos de datos para S3

En los eventos de datos, también conocidos como operaciones del plano de datos, se muestra información sobre las operaciones de recursos llevadas a cabo en un recurso determinado. Suelen ser actividades de gran volumen.

Los siguientes son ejemplos de eventos de CloudTrail datos para S3 que GuardDuty se pueden monitorear:

- Operaciones de la API de `GetObject`
- Operaciones de la API de `PutObject`
- Operaciones de la API de `ListObjects`
- Operaciones de la API de `DeleteObject`

Para obtener más información sobre estas API, consulte la [Referencia de la API de Amazon Simple Storage Service](#).

## ¿Cómo GuardDuty utiliza CloudTrail los eventos de datos para S3?

Cuando habilita S3 Protection, GuardDuty comienza a analizar CloudTrail los eventos de datos de S3 desde todos sus buckets de S3 y los monitorea para detectar actividades maliciosas o sospechosas. Para obtener más información, consulte [AWS CloudTrail eventos de gestión](#).

Si un usuario no autenticado accede a un objeto S3, significa que el objeto S3 es de acceso público. Por lo tanto, GuardDuty no procesa dichas solicitudes. GuardDuty procesa las solicitudes realizadas

a los objetos S3 mediante credenciales de IAM (AWS Identity and Access Management) o AWS STS (AWS Security Token Service) válidas.

 **Nota**

Tras activar S3 Protection, GuardDuty supervisa los eventos de datos de los buckets de Amazon S3 que residen en la misma región en la que la GuardDuty activó.

Si deshabilita la protección de S3 en su cuenta en una región específica, GuardDuty detiene la supervisión de los eventos de datos de S3 de los datos almacenados en sus depósitos de S3. GuardDuty ya no generará los tipos de búsqueda de S3 Protection para tu cuenta en esa región.

## GuardDuty usar eventos CloudTrail de datos de S3 para secuencias de ataque

[GuardDuty Detección de amenazas extendida](#) detecta las secuencias de ataque en varias etapas que abarcan los orígenes de datos fundamentales, los recursos de AWS y el cronograma de una cuenta. Cuando GuardDuty observa una secuencia de eventos que es indicativa de una actividad sospechosa reciente o en curso en su cuenta, GuardDuty genera una búsqueda de la secuencia de ataque asociada.

De forma predeterminada, cuando la activas GuardDuty, la detección extendida de amenazas también se habilita en tu cuenta. Esta capacidad cubre el escenario de amenazas asociado a los eventos de CloudTrail administración sin costo adicional. Sin embargo, para aprovechar al máximo el potencial de la detección extendida de amenazas, GuardDuty recomienda habilitar S3 Protection para cubrir los escenarios de amenazas asociados a CloudTrail los eventos de datos en S3.

Después de activar S3 Protection, GuardDuty cubrirá automáticamente los escenarios de amenaza de la secuencia de ataque, como el compromiso o la destrucción de datos, en los que puedan estar involucrados sus recursos de Amazon S3.

## Habilitar la protección de S3 en entornos de varias cuentas

En un entorno con varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de configurar (activar o desactivar) S3 Protection para las cuentas de los miembros de su AWS organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de



miembros mediante AWS Organizations. La cuenta de GuardDuty administrador delegado puede elegir que S3 Protection se active automáticamente en todas las cuentas, solo en las cuentas nuevas o en ninguna cuenta de la organización. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

## Habilitar S3 Protection para la cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para habilitar S3 Protection en la cuenta de GuardDuty administrador delegado.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija S3 Protection.
3. En la página Protección de S3, seleccione Editar.
4. Realice una de las siguientes acciones:

#### Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
- Seleccione Save.

#### Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar las cuentas manualmente.
- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Save.

### API/CLI

[updateDetector](#) Para ello, utilice el identificador de detector de la cuenta de GuardDuty administrador delegado para la región actual y pase el features objeto name tal S3\_DATA\_EVENTS y status como. ENABLED

Como alternativa, puede configurar S3 Protection mediante AWS Command Line Interface. Ejecute el siguiente comando y asegúrese de **12abc34d567e8fa901bc2d34e56789f0** reemplazarlo por el ID de detector de la cuenta de GuardDuty administrador delegado para la región actual.

Para encontrar el correspondiente `detectorId` a tu cuenta y a tu región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name": "S3_DATA_EVENTS", "Status": "ENABLED"}]'
```

## Auto-enable Protección S3 para todas las cuentas de los miembros de la organización

Elija el método de acceso que prefiera para habilitar S3 Protection para la cuenta de GuardDuty administrador delegado.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Inicie sesión con la cuenta de administrador.

2. Realice una de las siguientes acciones:

Uso de la página Protección de S3

1. En el panel de navegación, elija Protección de S3.
2. Elija Habilitar para todas las cuentas. Esta acción habilita automáticamente la protección de S3 para las cuentas nuevas y existentes de la organización.
3. Seleccione Save.

#### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

## Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Protección de S3.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitar de forma selectiva la S3 Protection en las cuentas de miembro](#).

## API/CLI

- Para habilitar S3 Protection de forma selectiva para sus cuentas de miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia. *detector ID*
- En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Asegúrese de sustituirla por *12abc34d567e8fa901bc2d34e56789f0* la `detector-id` de la cuenta de GuardDuty administrador delegado y. *111122223333*

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitación de la S3 Protection para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la S3 Protection en todas las cuentas de miembros activas existentes de la organización.

### Console

1. Inicia sesión en Consola de administración de AWS y abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija S3 Protection.
3. En la página S3 Protection, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Elija Confirmar.

### API/CLI

- Para habilitar S3 Protection de forma selectiva para sus cuentas de miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia. *detector ID*
- En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Asegúrese de sustituirla por *12abc34d567e8fa901bc2d34e56789f0* la detector-id de la cuenta de GuardDuty administrador delegado y. *111122223333*

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features ' [{"name": "S3_DATA_EVENTS", "status": "ENABLED"} ] '
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Auto-enable Protección S3 para cuentas de nuevos miembros

Elija su método de acceso preferido para habilitar la S3 Protection para las cuentas nuevas que se unan a la organización.

### Console

La cuenta de GuardDuty administrador delegado puede habilitar nuevas cuentas de miembros en una organización a través de la consola, desde la página de Protección de S3 o desde la página de Cuentas.

Habilitación automática de la S3 Protection para las cuentas de nuevos miembros

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

- Uso de la página S3 Protection:

1. En el panel de navegación, elija S3 Protection.
2. En la página S3 Protection, seleccione Editar.
3. Elija Configurar cuentas manualmente.
4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la S3 Protection se habilitará automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
5. Seleccione Save.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione Auto-enable las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en S3 Protection.

#### 4. Seleccione Save.

### API/CLI

- Para habilitar S3 Protection de forma selectiva para sus cuentas de miembros, invoque la operación de la [UpdateOrganizationConfiguration](#) API con la suya propia. *detector ID*
- En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Establezca las preferencias para habilitar o deshabilitar automáticamente el plan de protección en esa región para las nuevas cuentas (NEW) que se unan a la organización, todas las cuentas (ALL) o ninguna de las cuentas (NONE) de la organización. Para obtener más información, consulte [auto EnableOrganizationMembers](#). Según sus preferencias, es posible que deba sustituir NEW por ALL o NONE.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name": "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

### Habilitar de forma selectiva la S3 Protection en las cuentas de miembro

Elija el método de acceso que prefiera para habilitar o desactivar de forma selectiva la S3 Protection en las cuentas de miembro.

#### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna S3 Protection para ver el estado de su cuenta de miembro.

### 3. Para habilitar de forma selectiva la S3 Protection

Seleccione la cuenta para la que desee habilitar la S3 Protection. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione S3Pro y, a continuación, elija la opción adecuada.

## API/CLI

Para habilitar la S3 Protection de forma selectiva para las cuentas de miembro, ejecute la operación de la API [updateMemberDetectors](#) con el ID de detector propio. En el siguiente ejemplo se muestra cómo se puede habilitar la S3 Protection para una sola cuenta de miembro. Para desactivarlo, sustituya `true` por `false`.

Para encontrar las `detectorId` de tu cuenta y región actuales, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

#### Note

Si utiliza scripts para incorporar nuevas cuentas y desea deshabilitar la S3 Protection en sus nuevas cuentas, puede modificar la operación de la API [createDetector](#) con el objeto `dataSources` opcional, tal y como se describe en este tema.

# Habilitar la S3 Protection para una cuenta independiente

Una cuenta independiente es la que decide activar o desactivar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la protección de S3 en entornos de varias cuentas](#).

Tras activar S3 Protection, GuardDuty empezará a supervisar AWS CloudTrail los eventos de datos de los buckets de S3 de su cuenta.

Elija el método de acceso que prefiera para configurar la S3 Protection para una cuenta independiente.

## Console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el selector de Regiones que aparece en la esquina superior derecha, seleccione una región en la que desee habilitar la S3 Protection.
3. En el panel de navegación, elija S3 Protection.
4. En la página S3 Protection se indica el estado actual de la S3 Protection de su cuenta. Seleccione Habilitar o Deshabilitar para habilitar o deshabilitar la S3 Protection en cualquier momento.
5. Elija Confirmar para confirmar su selección.

## API/CLI

Ejecute [updateDetector](#) con el ID de detector válido para la región actual y transfiera el name del objeto de features como S3\_DATA\_EVENTS establecido en ENABLED para habilitar la S3 Protection, respectivamente.

### Note

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.



Como alternativa, puedes usar AWS Command Line Interface. Para activar la protección de S3, ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID del detector de su cuenta y `us-east-1` por la región en la que desee activar la protección de S3.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

# GuardDuty Supervisión del tiempo de ejecución

## Note

Puede configurar Runtime Monitoring junto con todos los demás planes de protección desde una sola página de la GuardDuty consola. Para obtener más información, consulte [Configuración de planes de protección](#).

Runtime Monitoring observa y analiza los eventos a nivel del sistema operativo, las redes y los archivos para ayudarlo a detectar posibles amenazas en AWS cargas de trabajo específicas de su entorno.

AWS Recursos compatibles en Runtime Monitoring: GuardDuty inicialmente se lanzó Runtime Monitoring para admitir únicamente los recursos de Amazon Elastic Kubernetes Service (Amazon EKS). Ahora, puede utilizar la función Runtime Monitoring para detectar amenazas también para sus recursos de AWS Fargate Amazon Elastic Container Service (Amazon ECS) y Amazon Elastic Compute Cloud (Amazon EC2).

GuardDuty no admite la ejecución de clústeres de Amazon EKS AWS Fargate.

En este documento y en otras secciones relacionadas con la supervisión del tiempo de ejecución, se GuardDuty utiliza la terminología de tipo de recurso para referirse a los recursos de Amazon EKS, Fargate, Amazon ECS y Amazon EC2.

Runtime Monitoring utiliza un agente GuardDuty de seguridad que añade visibilidad al comportamiento en tiempo de ejecución, como el acceso a los archivos, la ejecución de procesos, los argumentos de la línea de comandos y las conexiones de red. Para cada tipo de recurso que desee supervisar en busca de posibles amenazas, puede administrar el agente de seguridad correspondiente a ese tipo de recurso específico de forma automática o manual (a excepción de Fargate, solo Amazon ECS). Administrar el agente de seguridad automáticamente significa que usted GuardDuty permite instalar y actualizar el agente de seguridad en su nombre. Por otra parte, al administrar manualmente el agente de seguridad para los recursos, usted será responsable de instalar y actualizar el agente de seguridad, según sea necesario.

Con esta capacidad ampliada, GuardDuty puede ayudarlo a identificar y responder a las posibles amenazas que puedan afectar a las aplicaciones y los datos que se ejecutan en sus cargas de

trabajo e instancias individuales. Por ejemplo, una amenaza puede empezar por comprometer un único contenedor que ejecuta una aplicación web vulnerable. Es posible que esta aplicación web tenga permisos de acceso a los contenedores y las cargas de trabajo subyacentes. En este escenario, las credenciales mal configuradas podrían dar lugar a un acceso más amplio a la cuenta y a los datos almacenados en ella.

Al analizar los eventos de tiempo de ejecución de los contenedores y las cargas de trabajo individuales, es GuardDuty posible identificar si un contenedor y AWS las credenciales asociadas están en peligro en una fase inicial, y detectar los intentos de escalar los privilegios, las solicitudes de API sospechosas y el acceso malintencionado a los datos de su entorno.

## Contenido

- [Funcionamiento](#)
- [¿Cómo funciona la prueba gratuita de 30 días en la supervisión en tiempo de ejecución?](#)
- [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#)
- [¿Habilitar la GuardDuty supervisión del tiempo](#)
- [Administrar agentes GuardDuty de seguridad](#)
- [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#)
- [Configuración de la supervisión de la CPU y la memoria](#)
- [Uso de VPC compartida con Runtime Monitoring](#)
- [Uso de la infraestructura como código \(IaC\) con GuardDuty agentes de seguridad automatizados](#)
- [Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty](#)
- [Agente de alojamiento GuardDuty de repositorios Amazon ECR](#)
- [Dos agentes de seguridad en el mismo host subyacente](#)
- [Supervisión del tiempo de ejecución de EKS en GuardDuty](#)
- [GuardDuty versiones de lanzamiento del agente de seguridad](#)
- [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#)

## Funcionamiento

Para utilizar Runtime Monitoring, debe habilitar Runtime Monitoring y, a continuación, administrar el agente de GuardDuty seguridad. La siguiente lista explica este proceso en dos pasos:

1. Habilite Runtime Monitoring en su cuenta para que GuardDuty pueda aceptar los eventos de tiempo de ejecución que reciba de sus instancias de Amazon EC2, clústeres de Amazon ECS y cargas de trabajo de Amazon EKS.
2. Administre el GuardDuty agente para los recursos individuales cuyo comportamiento en tiempo de ejecución desee supervisar. Según el tipo de recurso, puede:
  - Utilice una configuración de agentes automatizada, en la que se GuardDuty gestiona el despliegue del agente y automáticamente un punto final de Amazon Virtual Private Cloud (Amazon VPC).
  - Instalar el agente de manera manual, lo que requiere crear un punto de conexión de VPC como requisito previo.

El agente de seguridad utiliza el punto final de la VPC para enviar los eventos y garantizar que los datos permanezcan dentro de la AWS red. GuardDuty Este enfoque mejora la seguridad y permite GuardDuty supervisar y analizar el comportamiento del tiempo de ejecución en todos sus recursos (Amazon EKS, Amazon EC2 y AWS Fargate-Amazon ECS). GuardDuty utiliza [funciones de identidad de instancia](#) que autentican el agente de seguridad de cada tipo de recurso para enviar los eventos de tiempo de ejecución asociados al punto final de la VPC.

#### Note

GuardDuty analiza los eventos de tiempo de ejecución en su AWS entorno, los utiliza internamente para detectar amenazas y presenta los resultados mediante las conclusiones.

Si administra el agente de seguridad (de forma manual o a través de él GuardDuty) en EKS Runtime Monitoring o Runtime Monitoring for EC2, y si actualmente GuardDuty está desplegado en una instancia de Amazon EC2 y recibe [Tipos de eventos de tiempo de ejecución recopilados](#) el de esta instancia GuardDuty , no se le Cuenta de AWS cobrará por el análisis de los registros de flujo de VPC de esta instancia de Amazon EC2. Esto ayuda a GuardDuty evitar el doble de los gastos de uso de la cuenta.

En los siguientes temas se explica cómo la activación de Runtime Monitoring y la administración del agente de GuardDuty seguridad funcionan de forma diferente para cada tipo de recurso.

#### Contenido

- [Cómo funciona la supervisión en tiempo de ejecución con los clústeres de Amazon EKS](#)

- [Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2](#)
- [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#)
- [Después de habilitar la supervisión en tiempo de ejecución](#)

## Cómo funciona la supervisión en tiempo de ejecución con los clústeres de Amazon EKS

Runtime Monitoring utiliza un [complemento EKS aws-guardduty-agent](#), también denominado agente GuardDuty de seguridad. Una vez desplegado el agente de GuardDuty seguridad en los clústeres de EKS, GuardDuty puede recibir los eventos de tiempo de ejecución de dichos clústeres de EKS.

### Notas

Runtime Monitoring admite los clústeres de Amazon EKS que se ejecutan en instancias de Amazon EC2 y en Amazon EKS Auto Mode.

Runtime Monitoring no admite los clústeres de Amazon EKS con los nodos híbridos de Amazon EKS ni los que se ejecutan en AWS Fargate.

Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

Puede supervisar los eventos en tiempo de ejecución de los clústeres de Amazon EKS a nivel de cuenta o de clúster. Puede administrar el agente GuardDuty de seguridad solo para los clústeres de Amazon EKS que desee supervisar para detectar amenazas. Puede administrar el agente GuardDuty de seguridad manualmente o GuardDuty permitir que lo administre en su nombre mediante la configuración automática del agente.

Cuando utilice el enfoque de configuración de agentes automatizado GuardDuty para poder gestionar el despliegue del agente de seguridad en su nombre, este creará automáticamente un punto final de Amazon Virtual Private Cloud (Amazon VPC). El agente de seguridad envía los eventos de tiempo de ejecución GuardDuty mediante este punto de conexión de Amazon VPC.

Junto con el punto final de la VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada (entrada) controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC del

recurso y también se adapta a él cuando cambia el rango CIDR. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.

#### Notas

- El uso del punto de conexión de VPC no conlleva ningún costo adicional.
- Trabajar con una VPC centralizada con un agente automatizado: cuando utilice la configuración de agentes GuardDuty automatizada para un tipo de recurso, GuardDuty se creará un punto de enlace de VPC en su nombre para todas las VPC. Esto incluye la VPC centralizada y las VPC radiales. GuardDuty no admite la creación de un punto final de VPC solo para la VPC centralizada. Para obtener más información sobre el funcionamiento de la VPC centralizada, consulte los [puntos finales de la VPC](#) de interfaz en el AWS documento técnico: Creación de una infraestructura de red escalable y segura. Multi-VPC AWS

## Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS

Antes del 13 de septiembre de 2023, podía configurarlo GuardDuty para administrar el agente de seguridad a nivel de cuenta. Este comportamiento indicaba que, de forma predeterminada, GuardDuty administrará el agente de seguridad en todos los clústeres de EKS que pertenezcan a un Cuenta de AWS. Ahora, GuardDuty proporciona una capacidad granular que le ayuda a elegir los clústeres de EKS en los que GuardDuty desea administrar el agente de seguridad.

Si decide [Administre el agente GuardDuty de seguridad manualmente](#), puede seguir seleccionando los clústeres de EKS que desee supervisar. Sin embargo, para gestionar el agente manualmente, Cuenta de AWS es imprescindible crear un punto de enlace de Amazon VPC para usted.

#### Note

Independientemente del enfoque que utilice para administrar el agente de GuardDuty seguridad, EKS Runtime Monitoring siempre está activado a nivel de cuenta.

## Temas

- [Administre el agente de seguridad mediante GuardDuty](#)
- [Administre el agente GuardDuty de seguridad manualmente](#)

## Administre el agente de seguridad mediante GuardDuty

GuardDuty despliega y administra el agente de seguridad en su nombre. En cualquier momento, puede supervisar los clústeres de EKS de su cuenta con uno de los siguientes enfoques.

### Temas

- [Supervisar todos los clústeres de EKS](#)
- [Excluir determinados clústeres de EKS](#)
- [Incluir determinados clústeres de EKS](#)

### Supervisar todos los clústeres de EKS

Utilice este enfoque cuando desee GuardDuty implementar y administrar el agente de seguridad para todos los clústeres de EKS de su cuenta. De forma predeterminada, también GuardDuty implementará el agente de seguridad en un clúster de EKS potencialmente nuevo creado en su cuenta.

#### Impacto de optar por este enfoque

- GuardDuty crea un punto final de Amazon Virtual Private Cloud (Amazon VPC) a través del cual el agente de GuardDuty seguridad envía los eventos de tiempo de ejecución. GuardDuty La creación del punto de conexión de Amazon VPC no conlleva ningún coste adicional si se gestiona el agente de seguridad a través de él. GuardDuty
- Es necesario que el nodo de trabajo tenga una ruta de red válida a un punto final de guardduty-data VPC activo. GuardDuty despliega el agente de seguridad en sus clústeres de EKS. Amazon Elastic Kubernetes Service (Amazon EKS) coordinará la implementación del agente de seguridad en los nodos de los clústeres de EKS.
- En función de la disponibilidad de IP, GuardDuty selecciona la subred para crear un punto final de VPC. Si utiliza topologías de red avanzadas, debe validar que la conectividad sea posible.

### Excluir determinados clústeres de EKS

Utilice este enfoque cuando desee administrar el agente de seguridad GuardDuty para todos los clústeres de EKS de su cuenta, pero excluya algunos clústeres de EKS. Este método utiliza un enfoque basado en etiquetas<sup>1</sup> en el que puede etiquetar los clústeres de EKS para los que no desea recibir los eventos de tiempo de ejecución. La etiqueta predefinida debe tener GuardDutyManaged-false como par de clave-valor.

## Impacto de optar por este enfoque

Este enfoque requiere que habilite la administración automática de los GuardDuty agentes solo después de agregar etiquetas a los clústeres de EKS que desee excluir de la supervisión.

Por lo tanto, el impacto que se produce al [Administre el agente de seguridad mediante GuardDuty](#) también se aplica este enfoque. Cuando añada etiquetas antes de habilitar la administración automática del GuardDuty agente, no GuardDuty implementará ni administrará el agente de seguridad para los clústeres de EKS que están excluidos de la supervisión.

## Consideraciones

- Debe añadir el par clave-valor de la siguiente manera `GuardDutyManaged: false` para los clústeres de EKS selectivos antes de activar la configuración automática de agentes; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS hasta que utilice la etiqueta.
- Debe impedir que se modifiquen las etiquetas, excepto por parte de identidades de confianza.

### Important

Administre los permisos para modificar el valor de la etiqueta `GuardDutyManaged` de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations o [Control de acceso a los recursos de AWS mediante etiquetas](#) en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor `GuardDutyManaged=false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para [Supervisar todos los clústeres de EKS](#).

## Incluir determinados clústeres de EKS

Utilice este enfoque cuando desee GuardDuty implementar y administrar las actualizaciones del agente de seguridad solo para algunos clústeres de EKS de su cuenta. Este método utiliza un enfoque basado en etiquetas<sup>1</sup> en el que puede etiquetar el clúster de EKS para el que desea recibir los eventos de tiempo de ejecución.



## Impacto de optar por este enfoque

- Al usar etiquetas de inclusión, GuardDuty implementará y administrará automáticamente el agente de seguridad solo para los clústeres de EKS selectivos que estén etiquetados con GuardDutyManaged el par clave-valor. `true`
- El uso de este enfoque también tendrá el mismo impacto que el especificado para [Supervisar todos los clústeres de EKS](#).

## Consideraciones

- Si el valor de la etiqueta GuardDutyManaged no está establecido en `true`, la etiqueta de inclusión no funcionará como se esperaba y esto podría afectar a la supervisión del clúster de EKS.
- Para asegurarse de que se estén supervisando determinados clústeres de EKS, debe evitar que las etiquetas se modifiquen, salvo por parte de identidades de confianza.

### Important

Administre los permisos para modificar el valor de la etiqueta GuardDutyManaged de su clúster de EKS mediante políticas de control de servicios o políticas de IAM. Para obtener más información, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations o [Control de acceso a los recursos de AWS mediante etiquetas](#) en la Guía del usuario de IAM.

- En el caso de un clúster de EKS potencialmente nuevo que no desee supervisar, asegúrese de agregar el par de clave-valor GuardDutyManaged-`false` al crear este clúster de EKS.
- Este enfoque también tendrá las mismas consideraciones que las especificadas para [Supervisar todos los clústeres de EKS](#).

<sup>1</sup> Para obtener más información sobre el etiquetado de determinados clústeres de EKS, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

## Administre el agente GuardDuty de seguridad manualmente

Utilice este enfoque cuando desee implementar y administrar el agente de GuardDuty seguridad en todos los clústeres de EKS de forma manual. Asegúrese de que la supervisión en tiempo de ejecución de EKS esté habilitada en sus cuentas. Es posible que el agente de GuardDuty seguridad no funcione según lo esperado si no habilita EKS Runtime Monitoring.

## Impacto de optar por este enfoque

Deberá coordinar el despliegue del agente de GuardDuty seguridad en sus clústeres de EKS en todas las cuentas y en los Regiones de AWS lugares en los que esté disponible esta función. También tendrás que actualizar la versión del agente cuando la GuardDuty publique. Para obtener más información sobre las versiones de los agentes para EKS, consulte [GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS](#).

## Consideraciones

Debe admitir un flujo de datos seguro a la vez que supervisa y soluciona las deficiencias de cobertura a medida que se implementan continuamente nuevos clústeres y cargas de trabajo.

## Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2

Las instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo en el entorno de AWS . Cuando habilita Runtime Monitoring y administra el agente de GuardDuty seguridad, le GuardDuty ayuda a detectar amenazas en sus instancias Amazon EC2 existentes y en posibles instancias nuevas. Además, esta característica es compatible con las instancias de Amazon EC2 administradas por Amazon ECS. Para obtener más información, consulte el [soporte de instancias administradas en Guardduty](#).

### Note

Runtime Monitoring no admite aplicaciones que se ejecuten en [instancias administradas por Amazon ECS](#).

La activación de Runtime GuardDuty Monitoring permite consumir eventos de tiempo de ejecución de procesos nuevos y en ejecución en instancias de Amazon EC2. GuardDuty requiere un agente de seguridad al que enviar los eventos de tiempo de ejecución desde su instancia EC2 a. GuardDuty

En el caso de las instancias Amazon EC2, el agente GuardDuty de seguridad funciona a nivel de instancia. Puede decidir si desea supervisar todas las instancias de Amazon EC2 en la cuenta o solo algunas. Si desea administrar instancias determinadas, el agente de seguridad solo será necesario para estas instancias.

GuardDuty también puede consumir eventos de tiempo de ejecución de tareas nuevas y tareas existentes que se ejecutan en instancias de Amazon EC2 dentro de los clústeres de Amazon ECS.

Para instalar el agente GuardDuty de seguridad, Runtime Monitoring ofrece las dos opciones siguientes:

- [Utilice la configuración automatizada de agentes \(opción recomendada\)](#), or
- [Administrar el agente de seguridad manualmente](#)

## Utilice la configuración automática del agente mediante GuardDuty (recomendado)

Utilice una configuración de agente automatizada que permita GuardDuty instalar el agente de seguridad en sus instancias de Amazon EC2 en su nombre. GuardDuty también administra las actualizaciones del agente de seguridad.

De forma predeterminada, GuardDuty instala el agente de seguridad en todas las instancias de su cuenta. Si desea GuardDuty instalar y administrar el agente de seguridad solo para determinadas instancias de EC2, añada etiquetas de inclusión o exclusión a las instancias de EC2, según sea necesario.

En algunos casos, es posible que no desee supervisar los eventos en tiempo de ejecución de todas las instancias de Amazon EC2 pertenecientes a la cuenta. Para los casos en los que desee supervisar los eventos en tiempo de ejecución de una cantidad limitada de instancias, agregue una etiqueta de inclusión como `GuardDutyManaged:true` a estas instancias determinadas. Empezando por la disponibilidad de la configuración de agentes automatizada para Amazon EC2, si su instancia de EC2 tiene una etiqueta de inclusión (`GuardDutyManaged:true`), GuardDuty respetará la etiqueta y gestionará el agente de seguridad para las instancias seleccionadas, incluso si no habilita explícitamente la configuración automática del agente.

Por otro lado, si hay un número limitado de instancias de EC2 para las que no desea supervisar los eventos de tiempo de ejecución, añada una etiqueta de exclusión (`GuardDutyManaged:false`) a las instancias seleccionadas. GuardDuty respetará la etiqueta de exclusión al no instalar ni administrar el agente de seguridad para estos recursos de EC2.

## Impact

Cuando utiliza la configuración de agentes automatizada en una Cuenta de AWS u otra organización, permite GuardDuty realizar los siguientes pasos en su nombre:

- GuardDuty crea una asociación de SSM para todas las instancias de Amazon EC2 gestionadas por SSM y que aparecen en Fleet Manager en la consola. <https://console.aws.amazon.com/systems-manager/>
- Uso de etiquetas de inclusión con la configuración automática del agente deshabilitada: después de habilitar Runtime Monitoring, si no habilita la configuración automática del agente pero agrega una etiqueta de inclusión a su instancia de Amazon EC2, significa que está permitiendo GuardDuty administrar el agente de seguridad en su nombre. La asociación de SSM instalará entonces el agente de seguridad en cada instancia que tenga la etiqueta de inclusión (`GuardDutyManaged:true`).
- Si habilita la configuración automatizada del agente: la asociación de SSM instalará entonces el agente de seguridad en todas las instancias de EC2 pertenecientes a la cuenta.
- Uso de etiquetas de exclusión con configuración de agente automatizada: antes de habilitar la configuración automática de agentes, al añadir una etiqueta de exclusión a la instancia de Amazon EC2, significa que está permitiendo GuardDuty impedir la instalación y la administración del agente de seguridad para la instancia seleccionada.

Ahora, al habilitar la configuración automatizada del agente, la asociación de SSM instalará y administrará el agente de seguridad en todas las instancias de EC2 excepto en aquellas etiquetadas con la etiqueta de exclusión.

- GuardDuty crea puntos de enlace de VPC en todas las VPC, incluidas las VPC compartidas, siempre que haya al menos una instancia EC2 de Linux en esa VPC que no se encuentre en los estados de instancia terminada o de cierre. Esto incluye la VPC centralizada y las VPC radiales. GuardDuty no admite la creación de un punto final de VPC solo para la VPC centralizada. Para obtener más información sobre el funcionamiento de la VPC centralizada, consulte los [puntos finales de la VPC](#) de interfaz en el AWS documento técnico: Creación de una infraestructura de red escalable y segura. Multi-VPC AWS

Para obtener información sobre los diferentes estados de las instancias, consulte [Ciclo de vida de las instancias](#) en la Guía del usuario de Amazon EC2.

GuardDuty también es compatible. [Uso de VPC compartida con Runtime Monitoring](#) Cuando se tengan en cuenta todos los requisitos previos para su organización Cuenta de AWS, GuardDuty utilizará la VPC compartida para recibir los eventos de tiempo de ejecución.

 Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

- Junto con el punto final de la VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada (entrada) controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC del recurso y también se adapta a él cuando cambia el rango CIDR. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.

## Administrar el agente de seguridad manualmente

Existen dos formas de administrar manualmente el agente de seguridad para Amazon EC2:

- Utilice los documentos GuardDuty gestionados AWS Systems Manager para instalar el agente de seguridad en las instancias de Amazon EC2 que ya están gestionadas por SSM.

Siempre que lance una nueva instancia de Amazon EC2, asegúrese de que esté habilitada para SSM.

- Utilice scripts del administrador de paquetes RPM (RPM) para instalar el agente de seguridad en las instancias de Amazon EC2, independientemente de si son administradas por SSM o no.

## Siguiente paso

Para comenzar a utilizar la configuración de supervisión en tiempo de ejecución para supervisar las instancias de Amazon EC2, consulte [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#).

## Cómo funciona la supervisión en tiempo de ejecución con Fargate (solo Amazon ECS)

Cuando habilita la monitorización del tiempo de ejecución, GuardDuty estará preparado para consumir los eventos de tiempo de ejecución de una tarea. Estas tareas se ejecutan dentro de los clústeres de Amazon ECS, que a su vez se ejecutan en las AWS Fargate instancias. GuardDuty Para recibir estos eventos de tiempo de ejecución, debe usar el agente de seguridad dedicado y totalmente administrado.

 Note

Runtime Monitoring no admite aplicaciones que se ejecuten en [instancias administradas por Amazon ECS](#).

Puede GuardDuty permitir la administración del agente GuardDuty de seguridad en su nombre mediante la configuración automática del agente para una AWS cuenta o una organización. GuardDuty empezará a implementar el agente de seguridad en las nuevas tareas de Fargate que se lanzan en sus clústeres de Amazon ECS. La siguiente lista especifica qué esperar al habilitar el agente de GuardDuty seguridad.

### Impacto de habilitar el agente GuardDuty de seguridad

GuardDuty crea un grupo de seguridad y punto final de nube privada virtual (VPC)

- Al implementar el agente de GuardDuty seguridad, GuardDuty creará un punto final de VPC a través del cual el agente de seguridad envía los eventos de tiempo de ejecución. GuardDuty  
  
Junto con el punto final de la VPC, GuardDuty también crea un nuevo grupo de seguridad. Las reglas de entrada (entrada) controlan el tráfico que puede llegar a los recursos asociados al grupo de seguridad. GuardDuty agrega reglas de entrada que coinciden con el rango CIDR de la VPC del recurso y también se adapta a él cuando cambia el rango CIDR. Para obtener más información, consulte [Rango de CIDR de la VPC](#) en la Guía del usuario de Amazon VPC.
- Trabajar con una VPC centralizada con un agente automatizado: cuando utilice la configuración de agentes GuardDuty automatizada para un tipo de recurso, GuardDuty se creará un punto de enlace de VPC en su nombre para todas las VPC. Esto incluye la VPC centralizada y las VPC radiales. GuardDuty no admite la creación de un punto final de VPC solo para la VPC centralizada. Para obtener más información sobre el funcionamiento de la VPC centralizada, consulte los [puntos finales de la VPC](#) de interfaz en el AWS documento técnico: Creación de una infraestructura de red escalable y segura. Multi-VPC AWS
- El uso del punto de conexión de VPC no conlleva ningún costo adicional.

### GuardDuty añade un contenedor con sidecar

Para una nueva tarea o servicio de Fargate que comience a ejecutarse, se adjunta un GuardDuty contenedor (sidecar) a cada contenedor de la tarea Fargate de Amazon ECS. El agente de GuardDuty seguridad se encuentra dentro del contenedor adjunto. GuardDuty Esto ayuda

GuardDuty a recopilar los eventos de tiempo de ejecución de cada contenedor que se ejecuta dentro de estas tareas.

La imagen del contenedor GuardDuty sidecar se almacena en Amazon Elastic Container Registry (Amazon ECR) y sus capas de imágenes se almacenan en Amazon S3. Cuando comience la tarea, necesitará extraer esta imagen del ECR. Según la configuración de la red, esto puede requerir ajustes específicos para garantizar el acceso tanto al ECR como al S3. Por ejemplo, si se utilizan grupos de seguridad con acceso restringido, se tendrá que permitir el acceso a la lista de prefijos administrados de S3. Para obtener más información acerca de cómo hacerlo, consulte [Requisitos previos para el acceso a imágenes de contenedores](#).

Cuando inicias una tarea de Fargate, si el GuardDuty contenedor (sidecar) no puede iniciarse en buen estado, Runtime Monitoring está diseñado para no impedir que las tareas se ejecuten.

De forma predeterminada, las tareas de Fargate son inmutables. GuardDuty no desplegará el sidecar cuando una tarea ya esté en ejecución. Si desea supervisar un contenedor en una tarea que ya está en ejecución, puede detener la tarea e iniciarla de nuevo.

## Enfoques para gestionar los agentes GuardDuty de seguridad en ECS-Fargate los recursos de Amazon

La supervisión en tiempo de ejecución brinda la opción de detectar posibles amenazas a la seguridad en todos los clústeres de Amazon ECS (nivel de cuenta) o en clústeres concretos (nivel de clúster) en la cuenta. Al habilitar la configuración automática de agentes para cada tarea de Amazon ECS Fargate que se vaya a ejecutar, GuardDuty añadirá un contenedor sidecar para cada carga de trabajo de contenedores incluida en esa tarea. El agente GuardDuty de seguridad se despliega en este contenedor de sidecar. Así es como GuardDuty obtiene visibilidad del comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS.

Runtime Monitoring permite administrar el agente de seguridad para sus clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Antes de configurar las cuentas, valore si desea supervisar el comportamiento en tiempo de ejecución de todos los contenedores que pertenecen a las tareas de Amazon ECS, o incluir o excluir recursos específicos. Tenga en cuenta los siguientes enfoques.

## Supervisión de todos los clústeres de Amazon ECS

Este enfoque ayudará a detectar posibles amenazas a la seguridad a nivel de cuenta. Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para todos los clústeres de Amazon ECS que pertenecen a su cuenta.

## Exclusión de clústeres de Amazon ECS específicos

Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para la mayoría de los clústeres de Amazon ECS de su AWS entorno, pero excluya algunos de ellos. Este enfoque ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS a nivel de clúster. Por ejemplo, la cantidad de clústeres de Amazon ECS que pertenecen a la cuenta es 1000. Sin embargo, solo desea supervisar 930 clústeres de Amazon ECS.

Este enfoque requiere que añada una GuardDuty etiqueta predefinida a los clústeres de Amazon ECS que no desee supervisar. Para obtener más información, consulte [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#).

## Incluir clústeres de Amazon ECS específicos

Utilice este enfoque cuando desee GuardDuty detectar posibles amenazas de seguridad para algunos de los clústeres de Amazon ECS. Este enfoque ayuda a supervisar el comportamiento en tiempo de ejecución de los contenedores dentro de las tareas de Amazon ECS a nivel de clúster. Por ejemplo, la cantidad de clústeres de Amazon ECS que pertenecen a la cuenta es 1000. Sin embargo, solo desea supervisar 230 clústeres.

Este enfoque requiere que añada una GuardDuty etiqueta predefinida a los clústeres de Amazon ECS que desee supervisar. Para obtener más información, consulte [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#).

## Después de habilitar la supervisión en tiempo de ejecución

Después de activar Runtime Monitoring e instalar el agente de GuardDuty seguridad en su cuenta independiente o en las cuentas de varios miembros, puede seguir los siguientes pasos para asegurarse de que la configuración del plan de protección funcione según lo esperado y controlar la cantidad de memoria y CPU que utiliza el agente de GuardDuty seguridad.



## Evaluar la cobertura en tiempo de ejecución

GuardDuty le recomienda que evalúe continuamente el estado de cobertura del recurso en el que ha desplegado el agente de seguridad. La cobertura puede estar en buen estado o en mal estado. Un estado de cobertura en buen estado indica que GuardDuty está recibiendo los eventos de tiempo de ejecución del recurso correspondiente cuando hay una actividad a nivel del sistema operativo.

Cuando el estado de cobertura pasa a ser Correcto para el recurso, GuardDuty puede recibir los eventos de tiempo de ejecución y analizarlos para detectar amenazas. Cuando GuardDuty detecta una posible amenaza a la seguridad en las tareas o aplicaciones que se ejecutan en su contenedor, GuardDuty genera [GuardDuty Tipos de búsqueda de Runtime Monitoring](#) cargas de trabajo e instancias.

También puedes configurar Amazon EventBridge (EventBridge) para recibir una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o de otra manera. Para obtener más información, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

## Configure el monitoreo de la CPU y la memoria para el agente GuardDuty de seguridad

Una vez que haya comprobado que la cobertura esté en buen estado, podrá evaluar el rendimiento del agente de seguridad para el tipo de recurso. Para los clústeres de Amazon EKS que tienen la versión 1.5 o superior del agente de seguridad, GuardDuty admite la configuración de los parámetros del agente de seguridad (complementario). Para obtener más información, consulte [Configuración de la supervisión de la CPU y la memoria](#).

## GuardDuty detecta posibles amenazas

A medida que GuardDuty comienza a recibir los eventos de tiempo de ejecución de su recurso, comienza a analizarlos. Cuando GuardDuty detecta una posible amenaza de seguridad en cualquiera de sus instancias de Amazon EC2, clústeres de Amazon ECS o clústeres de Amazon EKS, genera una o más. [GuardDuty Tipos de búsqueda de Runtime Monitoring](#) Puede acceder a los detalles del resultado para ver los detalles del recurso impactado.

## ¿Cómo funciona la prueba gratuita de 30 días en la supervisión en tiempo de ejecución?

El período de prueba gratuito de 30 días funciona de forma diferente para las GuardDuty cuentas nuevas y las cuentas existentes que ya tenían habilitado EKS Runtime Monitoring antes de que la

capacidad de Runtime Monitoring se extendiera a las instancias de Amazon EC2 y AWS Fargate (solo Amazon ECS).

## Estoy utilizando el período de GuardDuty prueba o nunca he activado EKS Runtime Monitoring

La siguiente lista explica cómo funciona el período de prueba gratuito de 30 días si está utilizando el período de prueba de GuardDuty 30 días o si nunca ha activado EKS Runtime Monitoring:

- Cuando lo active GuardDuty por primera vez, Runtime Monitoring y EKS Runtime Monitoring no estarán habilitados de forma predeterminada.

Al habilitar Runtime Monitoring para su cuenta u organización, asegúrese de configurar también el agente de GuardDuty seguridad del recurso que quiere monitorear para detectar amenazas. Por ejemplo, si desea utilizar la supervisión en tiempo de ejecución para las instancias de Amazon EC2, después de habilitar la supervisión en tiempo de ejecución, también deberá configurar el agente de seguridad para Amazon EC2. Puede elegir hacerlo de forma manual o automática a través de GuardDuty.

- El plan de protección de supervisión en tiempo de ejecución se habilita a nivel de cuenta. El periodo de prueba gratuito de 30 días funciona a nivel del recurso. Una vez que el agente de GuardDuty seguridad se haya desplegado en un tipo de recurso específico, la prueba gratuita de 30 días comenzará cuando GuardDuty reciba el primer evento de tiempo de ejecución asociado a este tipo de recurso. Por ejemplo, ha implementado el GuardDuty agente a nivel de recursos (para la instancia de Amazon EC2, el clúster de Amazon ECS y el clúster de Amazon EKS). Cuando GuardDuty reciba el primer evento de tiempo de ejecución de una instancia de Amazon EC2, la prueba gratuita de 30 días solo comenzará para Amazon EC2.
- Cuando desee habilitar únicamente la monitorización de tiempo de ejecución de EKS: cuando la active GuardDuty por primera vez, la supervisión de tiempo de ejecución de EKS no estará habilitada de forma predeterminada (después del lanzamiento de la supervisión de tiempo de ejecución). Deberá habilitar la supervisión en tiempo de ejecución de EKS. Para utilizarla de forma óptima, asegúrese de gestionar el agente de GuardDuty seguridad manualmente o de habilitar la configuración automática del agente para que GuardDuty gestione el agente en su nombre. El período de prueba gratuito de 30 días de EKS Runtime Monitoring comienza cuando GuardDuty recibe su primer evento de tiempo de ejecución para el recurso Amazon EKS.

## Habilite la supervisión en tiempo de ejecución de EKS antes del lanzamiento de la supervisión en tiempo de ejecución

Utilice esta sección únicamente cuando EKS Runtime Monitoring esté activado y ahora desee migrar a Runtime Monitoring. Cuenta de AWS

En la siguiente lista se incluyen escenarios que se podrían aplicar a su caso de uso de la habilitación de la supervisión en tiempo de ejecución:

- En el caso de una GuardDuty cuenta existente que tenga activado el plan de protección de EKS Runtime Monitoring y utilice la experiencia de la GuardDuty consola para utilizar este plan de protección, con el anuncio de Runtime Monitoring, la experiencia de la consola de EKS Runtime Monitoring se ha consolidado en Runtime Monitoring. La configuración existente para la Supervisión en tiempo de ejecución de EKS se mantiene sin cambios. Puede seguir utilizando el API/CLI soporte para realizar las operaciones asociadas a EKS Runtime Monitoring.
- Para utilizar la Supervisión en tiempo de ejecución de EKS como parte de la Supervisión en tiempo de ejecución, deberá configurar la Supervisión en tiempo de ejecución para la cuenta u organización. Para mantener la misma configuración para la Supervisión en tiempo de ejecución, consulte [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#). Sin embargo, esto no repercutirá en la prueba gratuita de 30 días del recurso de Amazon EKS.
- El plan de protección de Supervisión en tiempo de ejecución se habilita a nivel de cuenta por región. Después de implementar el agente de GuardDuty seguridad en uno de los tipos de recursos especificados (instancia de Amazon EC2 y clúster de Amazon ECS), la prueba gratuita de 30 días comienza cuando se GuardDuty recibe el primer evento de tiempo de ejecución asociado al recurso. Hay una prueba gratuita de 30 días relacionada con cada tipo de recurso.

Por ejemplo, después de habilitar Runtime Monitoring, si decide implementar el GuardDuty agente solo en una instancia de Amazon EC2, la prueba gratuita de 30 días de este recurso solo se iniciará cuando GuardDuty reciba su primer evento de tiempo de ejecución para una instancia de Amazon EC2. Más adelante, cuando implemente el GuardDuty agente para Fargate (solo Amazon ECS), la prueba gratuita de 30 días de este recurso solo comenzará cuando GuardDuty reciba su primer evento de tiempo de ejecución para el clúster de Amazon ECS. Teniendo en cuenta que ya tiene activado EKS Runtime Monitoring en su cuenta, GuardDuty no restablece la prueba gratuita de 30 días de un recurso de Amazon EKS.

# Requisitos previos para habilitar la Supervisión en tiempo de ejecución

Para habilitar la supervisión en tiempo de ejecución y administrar el agente de GuardDuty seguridad, debe cumplir los requisitos previos de cada tipo de recurso que desee supervisar para detectar amenazas. Cada tipo de recurso tiene diferentes requisitos previos. Por ejemplo, GuardDuty admite diferentes distribuciones de sistema operativo según el tipo de recurso.

Si solo desea supervisar los recursos de Amazon EC2, deberá seguir los requisitos previos para las instancias de Amazon EC2. Si posteriormente decide supervisar los recursos de Amazon EKS, deberá seguir los requisitos previos específicos de los clústeres de Amazon EKS.

En las siguientes secciones se indican los requisitos previos en función del tipo de recurso.

## Contenido

- [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#)
- [Requisitos previos para AWS Fargate Soporte \(solo Amazon ECS\)](#)
- [Requisitos previos para la compatibilidad con clústeres de Amazon EKS](#)

## Requisitos previos para la compatibilidad con instancias de Amazon EC2

En esta sección se incluyen los requisitos previos para supervisar el comportamiento en tiempo de ejecución de las instancias de Amazon EC2. Una vez cumplidos estos requisitos previos, consulte [¿Habilitar la GuardDuty supervisión del tiempo.](#)

## Temas

- [Haga que SSM administre las instancias de EC2 \(solo para la configuración automatizada de agentes\)](#)
- [Validar los requisitos de arquitectura](#)
- [Validación de la política de control de servicios de la organización en un entorno de varias cuentas](#)
- [Al utilizar la configuración automatizada de agentes](#)
- [Límite de CPU y memoria para el agente GuardDuty](#)
- [Siguiendo el siguiente paso](#)

## Haga que SSM administre las instancias de EC2 (solo para la configuración automatizada de agentes)

GuardDuty usa AWS Systems Manager (SSM) para implementar, instalar y administrar automáticamente el agente de seguridad en sus instancias. Si planea instalar y administrar el GuardDuty agente manualmente, el SSM no es necesario.

Para administrar las instancias de Amazon EC2 con Systems Manager, consulte [Configurar Systems Manager para instancias de Amazon EC2](#) en la Guía del usuario de AWS Systems Manager .

## Validar los requisitos de arquitectura

La arquitectura de la distribución del sistema operativo puede afectar al comportamiento del agente de GuardDuty seguridad. Debe cumplir los siguientes requisitos antes de utilizar la Supervisión en tiempo de ejecución para instancias de Amazon EC2:

- La compatibilidad del kernel incluye eBPF, Tracepoints y Kprobe. Para las arquitecturas de CPU, Runtime Monitoring admite AMD64 (x64) y ARM64 (Graviton2 y versiones posteriores)<sup>1</sup>.

En la siguiente tabla se muestra la distribución del sistema operativo que se ha verificado para admitir el agente GuardDuty de seguridad para las instancias de Amazon EC2.

| Distribución del sistema operativo <sup>2</sup> | Versión de kernel <sup>3</sup>                                   |
|-------------------------------------------------|------------------------------------------------------------------|
| Amazon Linux 2                                  | 5.4 <sup>4</sup> , 5.10 <sup>4</sup> , 5.15                      |
| Amazon Linux 2023                               | 5.4 <sup>4</sup> , 5.10 <sup>4</sup> , 5.15, 6.1, 6.5, 6.8, 6.12 |
| Ubuntu 20.04 y Ubuntu 22.04                     | 5.4 <sup>4</sup> , 5.10 <sup>4</sup> , 5.15, 6.1, 6.5, 6.8       |
| Debian 11 y Debian 12                           | 5.4 <sup>4</sup> , 5.10, 5.15 <sup>4</sup> , 6.1, 6.5, 6.8       |
| Ubuntu 24.04                                    | 6.8<br>6.13 <sup>5</sup> , 6.14 <sup>5</sup>                     |
| RedHat 9.4                                      | 5.14                                                             |

| Distribución del sistema operativo <sup>2</sup> | Versión de kernel <sup>3</sup> |
|-------------------------------------------------|--------------------------------|
| Fedora 34.0                                     | 5.11, 5.17                     |
| Fedora 40                                       | 6.8                            |
| Fedora 41                                       | 6.12                           |
| CentOS Stream 9                                 | 5.14                           |
| Oracle Linux 8.9                                | 5.15                           |
| Oracle Linux 9.3                                | 5.15                           |
| Rocky Linux 9.5                                 | 5.14                           |
| Alma Linux 9                                    | 5.14                           |
| Alma Linux 10                                   | 6.12                           |
| Servidor SUSE Linux Enterprise 16               | 6.12                           |

1. Runtime Monitoring para recursos de Amazon EC2 no es compatible con la primera generación de instancias de Graviton, como los tipos de instancia A1.
2. Soporte para varios sistemas operativos: GuardDuty ha verificado el soporte de Runtime Monitoring para la distribución operativa indicada en la tabla anterior. Si bien el agente de GuardDuty seguridad puede funcionar en sistemas operativos que no figuran en la tabla anterior, el GuardDuty equipo no puede garantizar el valor de seguridad esperado.
3. Para cualquier versión del kernel, debe establecer el marcador `CONFIG_DEBUG_INFO_BTF` en y (que significa verdadero). Esto es necesario para que el agente GuardDuty de seguridad pueda funcionar según lo esperado.
4. En las versiones 5.10 y anteriores del núcleo, el agente GuardDuty de seguridad utiliza la memoria bloqueada en la RAM (`RLIMIT_MEMLOCK`) para funcionar según lo previsto.

Si el `RLIMIT_MEMLOCK` valor del sistema es demasiado bajo, se GuardDuty recomienda establecer los límites fijos y flexibles en al menos 32 MB. Para obtener información sobre cómo comprobar y modificar el valor `RLIMIT_MEMLOCK` predeterminado, consulte [Visualización y actualización de los valores de `RLIMIT\_MEMLOCK`](#).

5. Para Ubuntu 24.04, las versiones 6.13 y 6.14 del núcleo solo admiten las versiones 1.15.0 y superiores del agente de EC2.

- Requisitos adicionales: solo si tiene Amazon ECS/Amazon EC2

Para Amazon ECS/Amazon EC2, le recomendamos que utilice las ECS-optimized AMI de Amazon más recientes (con fecha del 29 de septiembre de 2023 o posterior) o que utilice la versión 1.77.0 del agente Amazon ECS.

## Visualización y actualización de los valores de `RLIMIT_MEMLOCK`

Si el `RLIMIT_MEMLOCK` límite del sistema es demasiado bajo, es posible que el agente de GuardDuty seguridad no funcione según lo diseñado. GuardDuty recomienda que tanto el límite estricto como el límite flexible sean de 32 MB como mínimo. Si no actualiza los límites, no GuardDuty podrá supervisar los eventos de tiempo de ejecución de su recurso. Cuando `RLIMIT_MEMLOCK` supere los límites mínimos establecidos, la actualización de estos límites pasa a ser opcional.

Puede modificar el `RLIMIT_MEMLOCK` valor predeterminado antes o después de instalar el agente GuardDuty de seguridad.

Para ver los valores de **`RLIMIT_MEMLOCK`**

1. Ejecute `ps aux | grep guardduty`. Esto generará el ID del proceso (pid).
2. Copie el ID del proceso (pid) del resultado del comando anterior.
3. Ejecute `grep "Max locked memory" /proc/pid/limits` después de reemplazar el pid con el ID de proceso copiado del paso anterior.

Esto mostrará la memoria máxima bloqueada para ejecutar el agente de seguridad. GuardDuty

Para actualizar los valores de **`RLIMIT_MEMLOCK`**

1. Si el archivo `/etc/systemd/system.conf.d/NUMBER-limits.conf` existe, comente la línea `DefaultLimitMEMLOCK` de este archivo. Este archivo establece un valor predeterminado

- RLIMIT\_MEMLOCK con alta prioridad, que sobrescribe la configuración del archivo `/etc/systemd/systemd.conf`.
2. Abre el archivo `/etc/systemd/systemd.conf` y quita el comentario de la línea que contiene `#DefaultLimitMEMLOCK=`.
  3. Actualice el valor predeterminado proporcionando límites RLIMIT\_MEMLOCK fijos y flexibles de al menos 32 MB. La política actualizada debería ser así: `DefaultLimitMEMLOCK=32M:32M`. El formato es `soft-limit:hard-limit`.
  4. Ejecute `sudo reboot`.

## Validación de la política de control de servicios de la organización en un entorno de varias cuentas

Si ha configurado una política de control de servicio (SCP) para administrar los permisos en la organización, valide que el límite de permisos permita la acción `guardduty:SendSecurityTelemetry`. Es necesario para admitir la supervisión del tiempo GuardDuty de ejecución en diferentes tipos de recursos.

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#).

## Al utilizar la configuración automatizada de agentes

Para [Utilice la configuración automatizada de agentes \(opción recomendada\)](#) ello, Cuenta de AWS debe cumplir los siguientes requisitos previos:

- Cuando utilices etiquetas de inclusión con una configuración de agente automatizada, GuardDuty para crear una asociación de SSM para una nueva instancia, asegúrate de que la nueva instancia esté gestionada por SSM y aparezca en Fleet Manager en la consola. <https://console.aws.amazon.com/systems-manager/>
- Al utilizar etiquetas de exclusión con configuración automatizada del agente
  - Añada la `false` etiqueta `GuardDutyManaged`: antes de configurar el agente GuardDuty automatizado para su cuenta.

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para Amazon



EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

- Activa la opción Permitir etiquetas en los metadatos de las instancias. Esta configuración es obligatoria porque GuardDuty necesita leer la etiqueta de exclusión del servicio de metadatos de la instancia (IMDS) para determinar si debe excluir la instancia de la instalación del agente. Para obtener más información, consulte [Habilitar el acceso a etiquetas de instancia en los metadatos de la instancia](#) en la Guía del usuario de Amazon EC2.

## Límite de CPU y memoria para el agente GuardDuty

### Límite de CPU

El límite máximo de CPU para el agente de GuardDuty seguridad asociado a las instancias de Amazon EC2 es del 10 por ciento del total de núcleos de vCPU. Por ejemplo, si la instancia de EC2 tiene 4 núcleos vCPU, el agente de seguridad puede utilizar un máximo del 40 por ciento del 400 por ciento total disponible.

### Memory limit (Límite de memoria)

De la memoria asociada a la instancia de Amazon EC2, hay una memoria limitada que el agente de GuardDuty seguridad puede utilizar.

En la siguiente tabla aparece el límite de memoria.

| Memoria de la instancia de Amazon EC2 | Memoria máxima para el agente GuardDuty |
|---------------------------------------|-----------------------------------------|
| Menos de 8 GB                         | 128 MB                                  |
| Menos de 32 GB                        | 256 MB                                  |
| Mayor o igual que 32 GB               | 1 GB                                    |

## Siguiente paso

El siguiente paso consiste en configurar la Supervisión en tiempo de ejecución y también administrar el agente de seguridad (automática o manualmente).

## Requisitos previos para AWS Fargate Soporte (solo Amazon ECS)

Esta sección incluye los requisitos previos para monitorear el comportamiento en tiempo de ejecución de sus recursos de Fargate-Amazon ECS. Una vez cumplidos estos requisitos previos, consulte [¿Habilitar la GuardDuty supervisión del tiempo.](#)

### Temas

- [Validación de los requisitos de arquitectura](#)
- [Requisitos previos para el acceso a imágenes de contenedores](#)
- [Validación de la política de control de servicios de la organización en un entorno de varias cuentas](#)
- [Validación de permisos de roles y límites de permisos de políticas](#)
- [Límites de CPU y memoria](#)

### Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma GuardDuty en que el agente GuardDuty de seguridad admite la recepción de los eventos de tiempo de ejecución de sus clústeres de Amazon ECS. Debe validar que esté utilizando una de las plataformas verificadas.

#### Consideraciones iniciales:

La AWS Fargate plataforma de los clústeres de Amazon ECS debe ser Linux. La versión de plataforma correspondiente debe ser como mínimo 1.4.0, o LATEST. Para obtener más información sobre las versiones de plataforma, consulte [Versiones de plataforma Linux](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

Aún no se admiten las versiones de la plataforma Windows.

### Plataformas verificadas

La distribución del sistema operativo y la arquitectura de la CPU afectan al soporte que proporciona el agente GuardDuty de seguridad. La siguiente tabla muestra la configuración verificada para implementar el agente GuardDuty de seguridad y configurar Runtime Monitoring.

| Distribución del sistema operativo <sup>1</sup> | Compatibilidad del kernel | Arquitectura de CPU x64 (AMD64) | Arquitectura de CPU Graviton (ARM64) |
|-------------------------------------------------|---------------------------|---------------------------------|--------------------------------------|
| Linux                                           | eBPF, Tracepoints, Kprobe | Soportado                       | compatible                           |

<sup>1</sup> Support para varios sistemas operativos: GuardDuty ha verificado el soporte de Runtime Monitoring para la distribución operativa indicada en la tabla anterior. Si bien el agente de GuardDuty seguridad puede funcionar en sistemas operativos que no figuran en la tabla anterior, el GuardDuty equipo no puede garantizar el valor de seguridad esperado.

## Requisitos previos para el acceso a imágenes de contenedores

Los siguientes requisitos previos le ayudan a acceder a la imagen del contenedor GuardDuty sidecar desde el repositorio de Amazon ECR.

### Requisitos de los permisos

La función de ejecución de tareas requiere determinados permisos de Amazon Elastic Container Registry (Amazon ECR) para descargar GuardDuty la imagen del contenedor del agente de seguridad:

```
...
    "ecr:GetAuthorizationToken",
    "ecr:BatchCheckLayerAvailability",
    "ecr:GetDownloadUrlForLayer",
    "ecr:BatchGetImage",
    ...
```

Para restringir aún más los permisos de Amazon ECR, puede añadir el URI del repositorio de Amazon ECR que aloja el agente de GuardDuty seguridad para (solo AWS Fargate Amazon ECS). Para obtener más información, consulte [Agente de alojamiento GuardDuty de repositorios Amazon ECR](#).

Puede utilizar la política [AmazonECSTaskExecutionRolePolicy](#) gestionada o añadir los permisos anteriores a su TaskExecutionRole política.

## Configuración de definición de tareas

Al crear o actualizar los servicios de Amazon ECS, debe proporcionar información de subred en la definición de la tarea:

Para ejecutar las [UpdateService](#) API [CreateService](#) en la referencia de API de Amazon Elastic Container Service, es necesario pasar la información de la subred. Para obtener más información, consulte las [definiciones de tareas de Amazon ECS](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

## Requisitos de conectividad de red

Debe garantizar la conectividad de red para descargar la imagen del GuardDuty contenedor de Amazon ECR. Este requisito es específico GuardDuty porque utiliza Amazon ECR para alojar su agente de seguridad. En función de la configuración de red, tendrá que implementar una de las siguientes opciones:

### Opción 1: usar el acceso a la red pública (si está disponible)

Si sus tareas de Fargate se ejecutan en subredes con acceso a Internet saliente, no es necesaria ninguna configuración de red adicional.

### Opción 2: Uso de puntos de conexión de Amazon VPC (para subredes privadas)

Si sus tareas de Fargate se ejecutan en subredes privadas sin acceso a Internet, debe configurar los puntos finales de VPC para ECR a fin de garantizar que el URI del repositorio de ECR que aloja el agente de seguridad sea accesible desde la red. GuardDuty Sin estos puntos de conexión, las tareas de las subredes privadas no pueden descargar la imagen del contenedor. GuardDuty

Para obtener instrucciones sobre la configuración del punto de conexión de VPC, consulte [Crear los puntos de conexión de VPC para Amazon ECR](#) en la Guía del usuario de Amazon Elastic Container Registry.

Para obtener información sobre cómo permitir que Fargate descargue el GuardDuty contenedor, consulte Uso de imágenes de [Amazon ECR con Amazon ECS en la Guía del usuario](#) de Amazon Elastic Container Registry.

## Configuración del grupo de seguridad

Las imágenes del GuardDuty contenedor están en Amazon ECR y requieren acceso a Amazon S3. Este requisito es específico para descargar imágenes de contenedores de Amazon ECR. En el caso de las tareas con acceso restringido a la red, debe configurar sus grupos de seguridad para permitir el acceso a S3.

Agregue una regla de salida a su grupo de seguridad que permita el tráfico a la [lista de prefijos administrados de S3 \(p1-xxxxxxx\) en el puerto 443](#). Para agregar una regla de salida, consulte [Configurar las reglas de un grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

Para ver sus listas de AWS prefijos administradas en la consola o describirlas mediante AWS Command Line Interface (AWS CLI), consulte las listas de [prefijos AWS administradas en](#) la Guía del usuario de Amazon VPC.

## Validación de la política de control de servicios de la organización en un entorno de varias cuentas

En esta sección, se explica cómo validar la configuración de la política de control de servicio (SCP) para garantizar que Runtime Monitoring funcione según lo esperado en toda la organización.

Si ha configurado una o más políticas de control de servicio para administrar los permisos en la organización, debe validar que no niegue la acción `guardduty:SendSecurityTelemetry`. Para obtener información sobre cómo funcionan las SCP, consulte la [evaluación de los SCP](#) en la Guía del usuario de AWS Organizations .

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar las SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#) en la Guía del usuario de AWS Organizations .

Realice los siguientes pasos para todas las SCP que haya configurado en su entorno de cuentas múltiples:

### Para validar **guardduty: no se deniega en SCP SendSecurityTelemetry**

1. Inicie sesión en la consola de Organizations en <https://console.aws.amazon.com/organizations/>. Debe iniciar sesión como rol de IAM o iniciar sesión como usuario raíz ([no se recomienda](#)) en la cuenta de administración de la organización.
2. En el panel de navegación izquierdo, seleccione Políticas (Políticas). A continuación, en Tipos de políticas compatibles, seleccione Políticas de control de servicios.

3. En la página Políticas de control de servicios, elija el nombre de la política que desea adjuntar.
4. En la página de detalles de la política, consulte el contenido de esta política. Asegúrese de que no deniegue la acción `guardduty:SendSecurityTelemetry`.

La siguiente política de SCP es un ejemplo para no denegar la acción `guardduty:SendSecurityTelemetry`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:SendSecurityTelemetry"
      ],
      "Resource": "*"
    }
  ]
}
```

Si su política deniega esta acción, debe actualizarla. Para obtener más información, consulte [Actualización de una política de control de servicio \(SCP\)](#) en la Guía del usuario de AWS Organizations .

## Validación de permisos de roles y límites de permisos de políticas

Siga los siguientes pasos para validar que los límites de permisos asociados al rol y a su política no impliquen la acción `guardduty:SendSecurityTelemetry` de restricción.

Para ver los límites de permisos de los roles y su política

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, en Administración del acceso, elija Roles.
3. En la página Roles, seleccione el rol *TaskExecutionRole* que acaba de crear.

4. En la página del rol seleccionado, en la pestaña Permisos, amplía el nombre de la política asociada a este rol. A continuación, verifique que esta política no restrinja `guardduty:SendSecurityTelemetry`.
5. Si el límite de permisos está establecido, amplíe esta sección. A continuación, amplíe cada política para comprobar que no restrinja la acción `guardduty:SendSecurityTelemetry`. El aspecto de la respuesta debe ser parecido a [Example SCP policy](#).

Si es necesario, lleve a cabo una de las siguientes acciones:

- Para modificar la política, seleccione Editar. En la página Modificar los permisos de esta política, actualice la política en el editor de políticas. Asegúrese de que el esquema JSON siga siendo válido. A continuación, elija Siguiente. A continuación, puede revisar y guardar los cambios.
- Para cambiar este límite de permisos y elegir otro límite, elija Cambiar límite.
- Para eliminar este límite de permisos, seleccione Eliminar límite.

Para obtener más información sobre las políticas de IAM, consulte [Políticas y permisos en AWS Identity and Access Management](#) en la Guía del usuario de IAM.

## Límites de CPU y memoria

En la definición de la tarea de Fargate, debe especificar el valor de CPU y memoria a nivel de tarea. La siguiente tabla muestra las combinaciones válidas de valores de CPU y memoria a nivel de tarea y el límite máximo de memoria del agente de GuardDuty seguridad correspondiente para el contenedor. GuardDuty

| Valor de CPU    | Valor de memoria       | GuardDuty límite máximo de memoria del agente |
|-----------------|------------------------|-----------------------------------------------|
| 256 (0,25 vCPU) | 512 MiB, 1 GB, 2 GB    | 128 MB                                        |
| 512 (0,5 vCPU)  | 1 GB, 2 GB, 3 GB, 4 GB |                                               |
| 1024 (1 vCPU)   | 2 GB, 3 GB, 4 GB       |                                               |
|                 | 5 GB, 6 GB, 7 GB, 8 GB |                                               |

| Valor de CPU    | Valor de memoria                            | GuardDuty límite máximo de memoria del agente |
|-----------------|---------------------------------------------|-----------------------------------------------|
| 2048 (2 vCPU)   | Entre 4 GB y 16 GB en incrementos de 1 GB   |                                               |
| 4096 (4 vCPU)   | Entre 8 GB y 20 GB en incrementos de 1 GB   |                                               |
| 8192 (8 vCPU)   | Entre 16 GB y 28 GB en incrementos de 4 GB  | 256 MB                                        |
|                 | Entre 32 GB y 60 GB en incrementos de 4 GB  | 512 MB                                        |
| 16384 (16 vCPU) | Entre 32 GB y 120 GB en incrementos de 8 GB | 1 GB                                          |

Después de habilitar la Supervisión en tiempo de ejecución y evaluar que la cobertura del clúster esté en buen estado, podrá configurar y ver las métricas de Información de contenedores. Para obtener más información, [Configurar la supervisión en el clúster de Amazon ECS](#).

El siguiente paso consiste en configurar la Supervisión en tiempo de ejecución, así como el agente de seguridad.

## Requisitos previos para la compatibilidad con clústeres de Amazon EKS

Esta sección incluye los requisitos previos para supervisar el comportamiento en tiempo de ejecución de los recursos de Amazon EKS. Estos requisitos previos son cruciales para que el GuardDuty agente funcione según lo esperado. Una vez cumplidos estos requisitos previos, consulte [¿Habilitar la GuardDuty supervisión del tiempo](#) para empezar a monitorear los recursos.

### Compatibilidad con características de Amazon EKS

Runtime Monitoring admite los clústeres de Amazon EKS que se ejecutan en instancias de Amazon EC2 y en Amazon EKS Auto Mode.

Runtime Monitoring no admite los clústeres de Amazon EKS con los nodos híbridos de Amazon EKS ni los que se ejecutan en AWS Fargate.



Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

## Validación de los requisitos de arquitectura

La plataforma que utilice puede afectar a la forma GuardDuty en que el agente GuardDuty de seguridad admite la recepción de los eventos de tiempo de ejecución de sus clústeres de EKS. Debe validar que esté utilizando una de las plataformas verificadas. Si administra el GuardDuty agente manualmente, asegúrese de que la versión de Kubernetes sea compatible con la versión del GuardDuty agente que está en uso actualmente.

### Plataformas verificadas

La distribución del sistema operativo, la versión del núcleo y la arquitectura de la CPU afectan al soporte que proporciona el agente de seguridad. GuardDuty La compatibilidad del kernel incluye eBPF, Tracepoints y Kprobe. Para las arquitecturas de CPU, Runtime Monitoring es compatible con AMD64 (x64) y ARM64 (Graviton2 y versiones posteriores)<sup>1</sup>.

La siguiente tabla muestra la configuración verificada para implementar el agente de GuardDuty seguridad y configurar EKS Runtime Monitoring.

| Distribución del sistema operativo <sup>2</sup> | Versión de kernel <sup>3</sup>                            | Versión de Kubernetes compatible |
|-------------------------------------------------|-----------------------------------------------------------|----------------------------------|
| Bottlerocket                                    | 5.4, 5.10, 5.15, 6.1 <sup>4</sup>                         | v1.23 - v1.36                    |
| Ubuntu                                          | 5.4, 5.10, 5.15, 6.1, 6.15, 6.16, 6.17, 6.18 <sup>4</sup> | v1.21 - v1.36                    |
| Amazon Linux 2                                  | 5.4, 5.10, 5.15, 6.1 <sup>4</sup>                         | v1.21 - v1.36                    |
| Amazon Linux 2023 <sup>5</sup>                  | 5.4, 5.10, 5.15, 6.1, 6.8, 6.12 <sup>4</sup>              | v1.21 - v1.36                    |
| RedHat 9.4                                      | 5.14 <sup>4</sup>                                         | v1.21 - v1.36                    |
| Fedora 34                                       | 5.11, 5.17                                                | v1.21 - v1.36                    |
| Fedora 40                                       | 6.8                                                       | v1.28 - v1.36                    |

| Distribución del sistema operativo <sup>2</sup> | Versión de kernel <sup>3</sup> | Versión de Kubernetes compatible |
|-------------------------------------------------|--------------------------------|----------------------------------|
| Fedora 41                                       | 6.12                           | v1.28 - v1.36                    |
| CentOS Stream 9                                 | 5.14                           | v1.21 - v1.36                    |

1. La Supervisión en tiempo de ejecución para clústeres de Amazon EKS no es compatible con la primera generación de instancias de Graviton, como los tipos de instancia A1.
2. Soporte para varios sistemas operativos: GuardDuty ha verificado el soporte de Runtime Monitoring para la distribución operativa indicada en la tabla anterior. Si bien el agente de GuardDuty seguridad puede funcionar en sistemas operativos que no figuran en la tabla anterior, el GuardDuty equipo no puede garantizar el valor de seguridad esperado.
3. Para cualquier versión del kernel, debe establecer el marcador CONFIG\_DEBUG\_INFO\_BTTF en y (que significa verdadero). Esto es necesario para que el agente GuardDuty de seguridad pueda funcionar según lo esperado.
4. Actualmente, con la versión Kernel6.1, no [GuardDuty Tipos de búsqueda de Runtime Monitoring](#) se GuardDuty puede generar nada relacionado con [Eventos del sistema de nombres de dominio \(DNS\)](#).
5. Runtime Monitoring es compatible con AL2023 con el lanzamiento del agente de GuardDuty seguridad v1.6.0 y versiones posteriores. Para obtener más información, consulte [GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS](#).

## Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty

En la siguiente tabla se muestran las versiones de Kubernetes para los clústeres de EKS compatibles con el agente de seguridad. GuardDuty

| Versión del agente de GuardDuty seguridad complementario Amazon EKS | Versión de Kubernetes |
|---------------------------------------------------------------------|-----------------------|
| v1.15.0 (última versión: v1.15.0-eksbuild.2)                        | 1.28 - 1.36           |

| Versión del agente de GuardDuty seguridad complementario Amazon EKS | Versión de Kubernetes |
|---------------------------------------------------------------------|-----------------------|
| v1.12.2 (última versión: v1.12.2-eksbuild.2)                        | 1.28 - 1.36           |
| v1.12.1 (última versión: v1.12.1-eksbuild.4)                        | 1.28 - 1.35           |
| v1.11.0 (más reciente: v1.11.0-eksbuild.4)                          | 1.28 - 1.34           |
| v1.10.0 (más reciente: v1.10.0-eksbuild.2)                          | 1,21 - 1,33           |
| v1.9.0 (más reciente: v1.9.0-eksbuild.2)                            | 1,21 - 1,32           |
| v1.8.1 (más reciente: v1.8.1-eksbuild.2)                            |                       |
| v1.7.1                                                              | 1,21 - 1,31           |
| v1.7.0                                                              |                       |
| v1.6.1                                                              |                       |
| Versión 1.6.0                                                       | 1,21 - 1,29           |
| v1.5.0                                                              |                       |
| v1.4.1                                                              |                       |
| v1.4.0                                                              |                       |
| v1.3.1                                                              |                       |
| v1.3.0                                                              | 1,21 - 1,28           |
| v1.2.0                                                              |                       |
| v1.1.0                                                              | 1,21 - 1,26           |
| v1.0.0                                                              | 1.21 - 1.25           |

Algunas de las versiones del agente GuardDuty de seguridad llegarán al final del soporte estándar.

Para obtener información sobre las versiones de lanzamiento del agente, consulte [GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS](#).

## Límites de CPU y memoria

En la siguiente tabla se muestran los límites de CPU y memoria del complemento Amazon EKS para GuardDuty (aws-guardduty-agent).

| Parámetro | Límite mínimo | Límite máximo |
|-----------|---------------|---------------|
| CPU       | 200m          | 1000m         |
| Memoria   | 256 Mi        | 1024 Mi       |

Cuando utiliza la versión 1.5.0 o superior del complemento Amazon EKS, GuardDuty ofrece la posibilidad de configurar el esquema del complemento para los valores de CPU y memoria. Para obtener información sobre el rango configurable, consulte [Parámetros y valores que se pueden configurar](#).

Después de habilitar la supervisión en tiempo de ejecución de EKS y evaluar el estado de la cobertura de sus clústeres de EKS, podrá configurar y ver las métricas de información de los contenedores. Para obtener más información, consulte [Configuración de la supervisión de la CPU y la memoria](#).

## Validar la política de control de servicios de la organización

Si ha configurado una política de control de servicio (SCP) para administrar los permisos en la organización, valide que el límite de permisos no restrinja `guardduty:SendSecurityTelemetry`. Es necesario GuardDuty para admitir la monitorización del tiempo de ejecución en diferentes tipos de recursos.

Si es una cuenta de miembro, contacte al administrador delegado asociado. Para obtener información sobre cómo administrar SCP para la organización, consulte [Políticas de control de servicios \(SCP\)](#).

## ¿Habilitar la GuardDuty supervisión del tiempo

Antes de habilitar la Supervisión en tiempo de ejecución en la cuenta, asegúrese de que el tipo de recurso para el que desea supervisar los eventos en tiempo de ejecución sea compatible con los requisitos de la plataforma. Para obtener más información, consulte [Requisitos previos](#).

Si ha utilizado la Supervisión en tiempo de ejecución de EKS antes del lanzamiento de la Supervisión en tiempo de ejecución, puede utilizar las API para comprobar y actualizar la configuración existente para la Supervisión en tiempo de ejecución de EKS. También puede migrar la configuración existente de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución. Para obtener más información, consulte [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#).

### Note

Actualmente, en esta documentación se indican los pasos necesarios para habilitar la Supervisión en tiempo real para las cuentas y la organización únicamente mediante la consola. También puede habilitar la supervisión del tiempo de ejecución mediante [las acciones de la API](#) o [AWS CLI para GuardDuty](#).

Puede configurar la Supervisión en tiempo de ejecución si sigue los pasos que se indican en los siguientes temas.

### Contenido

- [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#)
- [Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente](#)

## Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar Runtime Monitoring para las cuentas de los miembros y administrar la configuración automática de los agentes para los tipos de recursos que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de

miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Para la cuenta de administrador delegado GuardDuty

Para habilitar Runtime Monitoring para la cuenta de administrador delegado GuardDuty

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.
4. Uso de Habilitar para todas las cuentas

Si desea activar Runtime Monitoring para todas las cuentas que pertenecen a la organización, incluida la cuenta de GuardDuty administrador delegado, seleccione Activar para todas las cuentas.

5. Uso de Configurar cuentas manualmente

Si desea habilitar la Supervisión en tiempo de ejecución para cada cuenta de miembro individualmente, elija Configurar cuentas manualmente.

- Seleccione Habilitar en la sección Administrador delegado (esta cuenta).
6. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para todas las cuentas de miembro

Para habilitar la Supervisión en tiempo de ejecución para todas las cuentas de miembro en la organización

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.  
  
Inicie sesión con la cuenta de GuardDuty administrador delegado.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la página Supervisión en tiempo de ejecución, en la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.
4. Elija Habilitar para todas las cuentas.
5. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para todas las cuentas de miembro activas existentes

Para habilitar la Supervisión en tiempo de ejecución para las cuentas de miembro existentes en la organización

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.  
  
Inicie sesión con la cuenta de GuardDuty administrador delegado de la organización.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la página Supervisión en tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración de la Supervisión en tiempo de ejecución.

4. En el panel Supervisión en tiempo de ejecución, en la sección Cuentas de miembro activas, seleccione Acciones.
5. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
6. Elija Confirmar.
7. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

 Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Auto-enable Supervisión del tiempo de ejecución solo para las cuentas de los nuevos miembros

Para habilitar la Supervisión en tiempo de ejecución para las nuevas cuentas de miembro en la organización

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con la cuenta de GuardDuty administrador delegado designada de la organización.

2. En el panel de navegación, elija Supervisión en tiempo de ejecución
3. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.
4. Elija Configurar cuentas manualmente.



5. Elija Habilitar automáticamente las cuentas de miembros nuevas.
6. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

Para determinadas cuentas de miembro activas únicamente

Para habilitar la Supervisión en tiempo de ejecución para cuentas de miembro activas individuales

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, revise los valores de las columnas Supervisión en tiempo de ejecución y Administrar agente automáticamente. Estos valores indican si la supervisión del tiempo de ejecución y la administración de GuardDuty agentes están habilitadas o no para la cuenta correspondiente.
4. En la tabla Cuentas, seleccione la cuenta para la que desea habilitar la Supervisión en tiempo de ejecución. Puede elegir varias cuentas a la vez.
5. Elija Confirmar.
6. Seleccione Editar planes de protección. Elija la acción apropiada.
7. Elija Confirmar.
8. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

## Habilitar la Supervisión en tiempo de ejecución para una cuenta independiente

Una cuenta independiente es la propietaria de la decisión de habilitar o deshabilitar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de activar Runtime Monitoring, asegúrese de instalar el agente GuardDuty de seguridad mediante una configuración automática o un despliegue manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Para habilitar la Supervisión en tiempo de ejecución en una cuenta independiente

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, seleccione Habilitar para habilitar la Supervisión en tiempo de ejecución para la cuenta.
4. GuardDuty Para recibir los eventos de tiempo de ejecución de uno o más tipos de recursos (una instancia de Amazon EC2, un clúster de Amazon ECS o un clúster de Amazon EKS), utilice las siguientes opciones para administrar el agente de seguridad de estos recursos:

Para habilitar el agente GuardDuty de seguridad

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)

## Administrar agentes GuardDuty de seguridad

Puede administrar el agente de GuardDuty seguridad del recurso que desee supervisar. Si desea supervisar más de un tipo de recurso, asegúrese de administrar el GuardDuty agente de ese recurso.

Los siguientes temas resultan útiles para los pasos a seguir para administrar el agente de seguridad.

### Contenido

- [Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2](#)
- [Administrar manualmente el agente de seguridad para el recurso de Amazon EC2](#)
- [Administrar el agente de seguridad automatizado para Fargate \(solo Amazon ECS\)](#)
- [Administración automática del agente de seguridad para los recursos de Amazon EKS](#)
- [Administrar manualmente el agente de seguridad para el clúster de Amazon EKS](#)
- [Configurar los parámetros del agente de GuardDuty seguridad \(complemento\) para Amazon EKS](#)
- [Validar la configuración del punto de conexión de VPC](#)

## Habilitar el agente de seguridad automatizado para la instancia de Amazon EC2

En esta sección se incluyen los pasos para habilitar un agente GuardDuty automatizado para sus recursos de Amazon EC2 en su cuenta independiente o en un entorno de cuentas múltiples.

Antes de continuar, asegúrese de cumplir todos los [Requisitos previos para la compatibilidad con instancias de Amazon EC2](#).

### Temas

- [GuardDuty Agente habilitador para los recursos de Amazon EC2 en un entorno de cuentas múltiples](#)
- [Habilitación de un agente GuardDuty automatizado para los recursos de Amazon EC2 en una cuenta independiente](#)
- [Pasar del agente manual de Amazon EC2 al agente automatizado](#)

Si va a pasar de administrar el GuardDuty agente manualmente a habilitar el agente GuardDuty automatizado, antes de seguir los pasos para habilitar GuardDuty el agente automatizado, consulte.

[Pasar del agente manual de Amazon EC2 al agente automatizado](#)

## GuardDuty Agente habilitador para los recursos de Amazon EC2 en un entorno de cuentas múltiples

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar la configuración automática de los agentes para los tipos de recursos que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

Para la cuenta de administrador delegado GuardDuty

Configure for all instances

Si eligió Activar Runtime Monitoring para todas las cuentas, elija una de las siguientes opciones para la cuenta de GuardDuty administrador delegado:

- Opción 1

En Configuración automatizada del agente, en la sección EC2, seleccione Habilitar para todas las cuentas.

- Opción 2
  - En Configuración automatizada del agente, en la sección EC2, seleccione Configurar cuentas manualmente.
  - En Administrador delegado (esta cuenta), elija Habilitar.
- Seleccione Save.

Si elige Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente:

- En Configuración automatizada del agente, en la sección EC2, seleccione Configurar cuentas manualmente.
- En Administrador delegado (esta cuenta), elija Habilitar.
- Seleccione Save.

Independientemente de la opción que elija para habilitar la configuración automática del agente para la cuenta de GuardDuty administrador delegado, puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a esta cuenta.

1. Abra la consola en AWS Systems Manager . <https://console.aws.amazon.com/systems-manager/>
2. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la tecla de etiqueta aparece como Instancelds.

### Using inclusion tag in selected instances

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la true etiquetaGuardDutyManaged: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Si agrega esta etiqueta, podrá GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>

- Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete) que se crea. La tecla Tag aparece como etiqueta: GuardDutyManaged.

### Using exclusion tag in selected instances

#### Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la false etiquetaGuardDutyManaged: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para el registro [las etiquetas de exclusión estarán disponibles](#) en los metadatos de la instancia, lleve a cabo los siguientes pasos:
  - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.  
  
Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
  - b. En el menú Acciones, elija Configuración de la instancia.
  - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Auto-enable para todas las cuentas de los miembros

 Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

### Configure for all instances

En los siguientes pasos, se supone que seleccionó Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución:

1. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente para Amazon EC2.
2. Puede comprobar que la asociación SSM que GuardDuty crea (GuardDutyRuntimeMonitoring-do-not-delete) instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a esta cuenta.
  - a. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
  - b. Abra la pestaña Destinos correspondiente a la asociación de SSM. Observe que la tecla de etiqueta aparece como Instancelds.

### Using inclusion tag in selected instances

Para configurar el GuardDuty agente para las instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la true etiquetaGuardDutyManaged: a las instancias de EC2 que desee GuardDuty supervisar y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Si agrega esta etiqueta, podrá GuardDuty instalar y administrar el agente de seguridad para estas instancias de EC2 seleccionadas. No es necesario habilitar la configuración automática del agente de forma explícita.

3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad en todos los recursos de EC2 que pertenezcan a su cuenta.
  - a. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
  - b. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la tecla de etiqueta aparece como InstanceIds.

#### Using exclusion tag in selected instances

##### Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la false etiquetaGuardDutyManaged: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para el registro [las etiquetas de exclusión estarán disponibles](#) en los metadatos de la instancia, lleve a cabo los siguientes pasos:
  - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.



Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.

- b. En el menú Acciones, elija Configuración de la instancia.
  - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Auto-enable solo para cuentas de miembros nuevos

La cuenta de GuardDuty administrador delegado puede establecer la configuración del agente automatizado para el recurso Amazon EC2 para que se habilite automáticamente para las cuentas de los nuevos miembros a medida que se unan a la organización.

Configure for all instances

En los siguientes pasos se presupone que ha seleccionado Habilitar automáticamente para nuevas cuentas de miembro en la sección Supervisión en tiempo de ejecución:

1. En el panel de navegación, elija Supervisión en tiempo de ejecución.
2. En la página Supervisión en tiempo de ejecución, elija Editar.
3. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que siempre que una nueva cuenta se una a la organización, la configuración automatizada del agente para Amazon EC2 se habilitará automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta selección.
4. Seleccione Save.

Cuando una nueva cuenta de miembro se une a la organización, esta configuración se habilitará para esta automáticamente. GuardDuty Para gestionar el agente de seguridad de las instancias de Amazon EC2 que pertenecen a esta nueva cuenta de miembro, asegúrese de que se cumplen todos los requisitos previos [Para la instancia de EC2](#).

Cuando se crea una asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete), puede comprobar que la asociación de SSM instalará y administrará el agente de seguridad en todas las instancias de EC2 pertenecientes a la nueva cuenta de miembro.

- Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
- Abra la pestaña Destinos correspondiente a la asociación de SSM. Observe que la tecla de etiqueta aparece como Instancelds.

### Using inclusion tag in selected instances

Para configurar el agente de GuardDuty seguridad para instancias seleccionadas de su cuenta

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la true etiquetaGuardDutyManaged: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Si agrega esta etiqueta, podrá GuardDuty instalar y administrar el agente de seguridad para estas instancias seleccionadas. No es necesario habilitar explícitamente la configuración automática del agente.

3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.
  - a. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
  - b. Abra la pestaña Destinos correspondiente a la asociación de SSM que se crea. La tecla Tag aparece como etiqueta: GuardDutyManaged.

### Using exclusion tag in selected instances

#### Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para

Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

Para configurar el agente GuardDuty de seguridad para instancias específicas de su cuenta independiente

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Añada la `false` etiqueta `GuardDutyManaged`: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para el registro [las etiquetas de exclusión estarán disponibles](#) en los metadatos de la instancia, lleve a cabo los siguientes pasos:
  - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.  
  
Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
  - b. En el menú Acciones, elija Configuración de la instancia.
  - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

Solo determinadas cuentas de miembro seleccionadas

Configure for all instances

1. En la página Cuentas, seleccione una o más cuentas para las que desee habilitar la configuración del Monitoring-Automated agente Runtime (Amazon EC2). Asegúrese de que las cuentas que seleccione en este paso ya tienen habilitada la Supervisión en tiempo de ejecución.

2. En Editar planes de protección, elija la opción adecuada para habilitar la configuración del Monitoring-Automated agente Runtime (Amazon EC2).
3. Elija Confirmar.

### Using inclusion tag in selected instances

Para configurar el agente GuardDuty de seguridad para las instancias seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/ec2/>
2. Añada la `true` etiqueta `GuardDutyManaged`: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

Añadir esta etiqueta permitirá GuardDuty gestionar el agente de seguridad de las instancias etiquetadas de Amazon EC2. No necesita habilitar explícitamente la configuración automatizada del agente (Supervisión en tiempo de ejecución: configuración automatizada del agente (EC2)).

### Using exclusion tag in selected instances

#### Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

Para configurar el agente GuardDuty de seguridad para las instancias seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/ec2/>
2. Añada la `false` etiqueta `GuardDutyManaged`: a las instancias de EC2 que no desee GuardDuty supervisar o detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).

3. Para el registro [las etiquetas de exclusión estarán disponibles](#) en los metadatos de la instancia, lleve a cabo los siguientes pasos:
  - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.  
  
Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
  - b. En el menú Acciones, elija Configuración de la instancia.
  - c. Elija Permitir etiquetas en los metadatos de la instancia.
4. Tras agregar la etiqueta de exclusión, siga los mismos pasos tal como se indica en la pestaña Configurar para todas las instancias.

Ahora puede evaluar [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

## Habilitación de un agente GuardDuty automatizado para los recursos de Amazon EC2 en una cuenta independiente

Una cuenta independiente es la propietaria de la decisión de habilitar o deshabilitar un plan de protección Cuenta de AWS en un plan específico. Región de AWS

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de activar Runtime Monitoring, asegúrese de instalar el agente GuardDuty de seguridad mediante una configuración automática o un despliegue manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según su preferencia de supervisar todos o algunos recursos de Amazon EC2, elija el método que prefiera y siga los pasos que se indican en la tabla siguiente.

## Configure for all instances

Para configurar la Supervisión en tiempo de ejecución para todas las instancias en la cuenta independiente

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Editar.
4. En la sección EC2, elija Habilitar.
5. Seleccione Save.
6. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y gestionará el agente de seguridad en todos los recursos de EC2 que pertenezcan a su cuenta.
  - a. Abra la AWS Systems Manager consola en <https://console.aws.amazon.com/systems-manager/>
  - b. Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete). Observe que la tecla de etiqueta aparece como InstanceIds.

## Using inclusion tag in selected instances

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/ec2/>
2. Añada la true etiquetaGuardDutyManaged: a las instancias que desee GuardDuty monitorear y detectar posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Puede comprobar que la asociación SSM que se GuardDuty cree instalará y administrará el agente de seguridad únicamente en los recursos de EC2 que estén etiquetados con las etiquetas de inclusión.

Abra la AWS Systems Manager consola en <https://console.aws.amazon.com/systems-manager/>

- Abra la pestaña Destinos correspondiente a la asociación de SSM (GuardDutyRuntimeMonitoring-do-not-delete) que se crea. La tecla Tag aparece como etiqueta: GuardDutyManaged.

## Using exclusion tag in selected instances

### Note

Asegúrese de agregar la etiqueta de exclusión a las instancias de Amazon EC2 antes de lanzarlas. Una vez que haya activado la configuración automática de agentes para Amazon EC2, cualquier instancia de EC2 que se lance sin una etiqueta de exclusión se incluirá en la configuración GuardDuty automática de agentes.

Para configurar el agente GuardDuty de seguridad para instancias de Amazon EC2 seleccionadas

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/ec2/>
2. Añada la false etiquetaGuardDutyManaged: a las instancias que no desee GuardDuty monitorear y detecte posibles amenazas. Para obtener información sobre cómo agregar esta etiqueta, consulte [Para agregar una etiqueta a un recurso individual](#).
3. Para el registro [las etiquetas de exclusión estarán disponibles](#) en los metadatos de la instancia, lleve a cabo los siguientes pasos:
  - a. En la pestaña Detalles de la instancia, consulte el estado de Permitir etiquetas en los metadatos de la instancia.

Si actualmente está Desactivado, siga estos pasos para cambiar el estado a Habilitado. De lo contrario, omita este paso.
  - b. Seleccione la instancia para la que desea permitir etiquetas.
  - c. En el menú Acciones, elija Configuración de la instancia.
  - d. Elija Permitir etiquetas en los metadatos de la instancia.
  - e. En Acceso a etiquetas en metadatos de instancia, seleccione Permitir.
  - f. Seleccione Save.

4. Después de agregar la etiqueta de exclusión, siga los mismos pasos que se indican en la pestaña Configurar para todas las instancias.

Ahora puede evaluar el tiempo de ejecución [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#).

## Pasar del agente manual de Amazon EC2 al agente automatizado

Esta sección se aplica a su Cuenta de AWS caso si anteriormente administraba el agente de seguridad de forma manual y ahora desea utilizar la configuración GuardDuty automática del agente. Si esto no se aplica a su caso, continúe con la configuración del agente de seguridad para la cuenta.

Cuando habilita el agente GuardDuty automatizado, GuardDuty administra el agente de seguridad en su nombre. Para obtener información sobre las medidas que se GuardDuty deben tomar, consulte [Utilice la configuración automatizada de agentes \(opción recomendada\)](#).

### Eliminar recursos

#### Eliminar asociación de SSM

- Elimine cualquier asociación de SSM que pueda haber creado al administrar manualmente el agente de seguridad para Amazon EC2. Para obtener más información, consulte [Eliminar una asociación](#).
- Esto se hace para poder hacerse cargo de la gestión de las acciones de SSM, ya sea que utilice agentes automatizados a nivel de cuenta o de instancia (mediante etiquetas de inclusión o exclusión). GuardDuty Para obtener más información sobre las acciones que puede GuardDuty realizar el SSM, consulte. [Service-linked permisos de rol para GuardDuty](#)
- Al eliminar una asociación de SSM que se creó anteriormente para administrar el agente de seguridad de forma manual, es posible que se produzca un breve período de superposición cuando se GuardDuty cree una asociación de SSM para administrar el agente de seguridad automáticamente. Es posible que durante este periodo se produzcan conflictos relacionados con la programación de SSM. Para obtener más información, consulte [Programación de SSM en Amazon EC2](#).

#### Administre las etiquetas de inclusión y exclusión para las instancias de Amazon EC2

- Etiquetas de inclusión: cuando no habilita la configuración GuardDuty automática del agente, pero etiqueta alguna de sus instancias de Amazon EC2 con una etiqueta de inclusión (GuardDutyManaged:true), se GuardDuty crea una asociación SSM que instalará y administrará el agente de seguridad en las instancias de EC2 seleccionadas. Este es un



comportamiento esperado que ayuda a administrar el agente de seguridad únicamente en instancias de EC2 seleccionadas. Para obtener más información, consulte [Cómo funciona la supervisión en tiempo de ejecución con las instancias de Amazon EC2](#).

Para GuardDuty evitar la instalación y la administración del agente de seguridad, elimine la etiqueta de inclusión de estas instancias de EC2. Para obtener más información, consulte [Agregar y eliminar etiquetas](#) en la Guía del usuario de Amazon EC2.

- Etiquetas de exclusión: si desea habilitar la configuración GuardDuty automática de los agentes para todas las instancias de EC2 de su cuenta, asegúrese de que ninguna instancia de EC2 esté etiquetada con una etiqueta de exclusión (`:GuardDutyManaged`). `false`

## Administrar manualmente el agente de seguridad para el recurso de Amazon EC2

En esta sección se indican los pasos a seguir para instalar y actualizar manualmente el agente de seguridad para los recursos de Amazon EC2.

Tras activar Runtime Monitoring, tendrá que instalar el agente de GuardDuty seguridad manualmente. Para gestionar el agente GuardDuty de seguridad de forma manual, primero debe crear un punto de conexión de Amazon VPC de forma manual. Después de esto, puede instalar el agente de seguridad para que GuardDuty comience a recibir los eventos de tiempo de ejecución de las instancias de Amazon EC2. Cuando GuardDuty publique una nueva versión del agente para este recurso, podrá actualizar la versión del agente en su cuenta.

En los siguientes temas se incluyen los pasos a seguir para administrar de forma continua el agente de seguridad para los recursos de Amazon EC2.

### Temas

- [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#)
- [Instalación manual del agente de seguridad](#)
- [Actualización manual del agente GuardDuty de seguridad para la instancia de Amazon EC2](#)

### Requisito previo: crear manualmente el punto de conexión de Amazon VPC

Antes de poder instalar el agente GuardDuty de seguridad, debe crear un punto final de Amazon Virtual Private Cloud (Amazon VPC). Esto ayudará a GuardDuty recibir los eventos de tiempo de ejecución de sus instancias de Amazon EC2.

 Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

Para crear un punto de conexión de Amazon VPC

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/vpc/>
2. En el panel de navegación, en Nube privada VPC, seleccione Puntos de conexión.
3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.
5. En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de reemplazarla por **us-east-1** su. Región de AWS Debe ser la misma región que la instancia de Amazon EC2 que pertenece a su ID de AWS cuenta.

6. Elija Verificar el servicio.
7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside la instancia. Agregue la siguiente política para restringir el uso de puntos de conexión de Amazon VPC únicamente a la cuenta especificada. Con el valor de Condition de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar compatibilidad con el punto de conexión de Amazon VPC a ID de cuenta específicos de la organización, consulte [Organization condition to restrict access to your endpoint](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
  ],
}
```

```
{
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  },
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Principal": "*"
}
```

El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se muestra cómo compartir el punto final de la VPC con otros ID de AWS cuenta:

- Para especificar varias cuentas para acceder al punto de conexión de VPC, sustituya `"aws:PrincipalAccount: "111122223333"` por el siguiente bloque:

```
"aws:PrincipalAccount": [
    "666666666666",
    "555555555555"
]
```

Asegúrese de reemplazar los ID de AWS cuenta por los ID de cuenta de las cuentas que necesitan acceder al punto final de la VPC.

- Para permitir que todos los miembros de una organización accedan al punto de conexión de VPC, sustituya `"aws:PrincipalAccount: "111122223333"` por la siguiente línea:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Asegúrese de reemplazar la organización ***o-abcdef0123*** por su ID de organización.

- Para restringir el acceso a un recurso mediante un ID de organización, agregue el `ResourceOrgID` a la política. Para obtener más información, consulte [aws:ResourceOrgID](#) en la Guía del usuario de IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elija las subredes en las que reside la instancia.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga habilitado el puerto de entrada 443 desde la VPC (o la instancia de Amazon EC2). Si aún no dispone de un grupo de seguridad que tenga habilitado un puerto de entrada 443, consulte [Crear un grupo de seguridad para la VPC](#) en la Guía del usuario de Amazon VPC.

Si se produce un problema al restringir los permisos de entrada a la VPC (o instancia), puede utilizar el puerto de entrada 443 desde cualquier dirección IP (0.0.0.0/0). Sin embargo, GuardDuty recomienda utilizar direcciones IP que coincidan con el bloque CIDR de la VPC. Para obtener más información, consulte [Bloques de CIDR de VPC](#) en la Guía del usuario de Amazon VPC.

Una vez que haya seguido los pasos, consulte [Validar la configuración del punto de conexión de VPC](#) para asegurarse de que el punto de conexión de VPC se configuró correctamente.

## Instalación manual del agente de seguridad

GuardDuty proporciona los dos métodos siguientes para instalar el agente GuardDuty de seguridad en las instancias de Amazon EC2. Antes de continuar, asegúrese de seguir los pasos que se indican en [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#).

Elija el método de acceso que prefiera para instalar el agente de seguridad en los recursos de Amazon EC2.

- [Método 1: usar AWS Systems Manager](#)— Este método requiere que la instancia de Amazon EC2 esté AWS Systems Manager gestionada.
- [Método 2: utilizar administradores de paquetes de Linux](#)— Puede utilizar este método independientemente de que sus instancias de Amazon EC2 estén AWS Systems Manager gestionadas o no. Según las [distribuciones de sistema operativo](#), puede elegir un método adecuado para instalar scripts RPM o Debian. Si usa la plataforma Fedora, debe usar este método para instalar el agente.

## Método 1: usar AWS Systems Manager

Para usar este método, asegúrese de que las instancias de Amazon EC2 estén administradas por AWS Systems Manager y, a continuación, instale el agente.

### AWS Systems Manager instancia Amazon EC2 gestionada

Siga los pasos que se indican a continuación para que AWS Systems Manager administre las instancias de Amazon EC2.

- [AWS Systems Manager](#) le ayuda a gestionar sus AWS aplicaciones y recursos de principio a fin y a posibilitar operaciones seguras a escala.

Para gestionar sus instancias de Amazon EC2 con AWS Systems Manager, consulte [Configuración de Systems Manager para instancias de Amazon EC2](#) en la Guía del usuario de AWS Systems Manager.

- En la siguiente tabla se muestran los nuevos documentos GuardDuty gestionados por AWS Systems Manager :

| Nombre del documento                                | Tipo de documento | Finalidad                                                                                           |
|-----------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------|
| AmazonGuardDuty-RunTimeMonitoringSsmPlugin          | Distributor       | Para empaquetar el agente GuardDuty de seguridad.                                                   |
| AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin | Comando           | Ejecutar el script de instalación/un de instalación para instalar el agente GuardDuty de seguridad. |

Para obtener más información sobre AWS Systems Manager, consulte los documentos de [Amazon EC2 Systems Manager](#) en la Guía del usuario de AWS Systems Manager.

#### Para servidores de Debian

Las Amazon Machine Images (AMI) para el servidor Debian proporcionadas por AWS requieren que instale el agente de AWS Systems Manager (agente SSM). Deberá seguir un paso adicional para instalar el agente de SSM y hacer que SSM administre las instancias de servidor de Debian de Amazon EC2. Para obtener información sobre los pasos que

debe seguir, consulte [Instalación manual del agente de SSM en instancias de servidor Debian](#) en la Guía del usuario de AWS Systems Manager .

Para instalar el GuardDuty agente para la instancia de Amazon EC2 mediante AWS Systems Manager

1. Abra la AWS Systems Manager consola en. <https://console.aws.amazon.com/systems-manager/>
2. En el panel de navegación, elija Documentos
3. En Propiedad de Amazon, elija AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin.
4. Elija Run Command (Ejecutar comando).
5. Ingrese los siguientes parámetros del Comando de ejecución
  - Acción: elija Instalar.
  - Tipo de instalación: elija Instalar o desinstalar.
  - Nombre: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
  - Versión: si permanece vacío, obtendrá la última versión del agente de GuardDuty seguridad. Para obtener más información acerca de las versiones de lanzamiento, [GuardDuty versiones de agentes de seguridad para instancias de Amazon EC2](#).
6. Seleccione la instancia de Amazon EC2 de destino. Puede seleccionar una o más instancias de Amazon EC2. Para obtener más información, consulte [Ejecución de comandos de AWS Systems Manager desde la consola](#) en la Guía de usuario de AWS Systems Manager
7. Compruebe si la instalación del GuardDuty agente está en buen estado. Para obtener más información, consulte [Validación del estado de instalación GuardDuty del agente de seguridad](#).

Método 2: utilizar administradores de paquetes de Linux

Con este método, puede instalar el agente GuardDuty de seguridad ejecutando scripts RPM o Debian. En función de los sistemas operativos, puede elegir el método que prefiera:

- Utilice scripts RPM para instalar el agente de seguridad en las distribuciones de sistemas operativos AL2, AL2023, RedHat CentOS o Fedora.
- Utilice los scripts de Debian para instalar el agente de seguridad en las distribuciones de sistema operativo Ubuntu o Debian. Para obtener información sobre las distribuciones de Ubuntu y Debian compatibles, consulte [Validar los requisitos de arquitectura](#).

## RPM installation

### Important

Recomendamos comprobar la firma RPM del agente de GuardDuty seguridad antes de instalarlo en su máquina.

#### 1. Compruebe la firma RPM del agente de GuardDuty seguridad

##### a. Prepare la plantilla

Prepare los comandos con la clave pública adecuada, la firma del RPM x86\_64, la firma del RPM arm64 y el enlace de acceso correspondiente a los scripts RPM alojados en buckets de Amazon S3. Sustituya el valor del Región de AWS identificador de AWS cuenta y la versión del GuardDuty agente para acceder a los scripts del RPM.

- Clave pública

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/  
publickey.pem
```

- GuardDuty firma RPM del agente de seguridad:

Firma de x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/  
x86_64/amazon-guardduty-agent-1.15.0.x86_64.sig
```

Firma de arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/arm64/  
amazon-guardduty-agent-1.15.0.arm64.sig
```

- Enlaces de acceso a los scripts RPM en el bucket de Amazon S3:

Enlace de acceso para x86\_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/  
x86_64/amazon-guardduty-agent-1.15.0.x86_64.rpm
```

## Enlace de acceso para arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/arm64/
amazon-guardduty-agent-1.15.0.arm64.rpm
```

| Región de AWS  | Nombre de la región                 | AWS ID de cuenta |
|----------------|-------------------------------------|------------------|
| eu-west-1      | Europa (Irlanda)                    | 694911143906     |
| us-east-1      | Este de EE. UU. (Norte de Virginia) | 593207742271     |
| us-west-2      | Oeste de EE. UU. (Oregón)           | 733349766148     |
| eu-west-3      | Europa (París)                      | 665651866788     |
| us-east-2      | Este de EE. UU. (Ohio)              | 307168627858     |
| eu-central-1   | Europa (Fráncfort)                  | 323658145986     |
| ap-northeast-2 | Asia-Pacífico (Seúl)                | 914738172881     |
| eu-north-1     | Europa (Estocolmo)                  | 591436053604     |
| ap-east-1      | Asia-Pacífico (Hong Kong)           | 258348409381     |
| me-south-1     | Middle East (Bahrain)               | 536382113932     |
| eu-west-2      | Europa (Londres)                    | 892757235363     |
| ap-northeast-1 | Asia-Pacífico (Tokio)               | 533107202818     |
| ap-southeast-1 | Asia-Pacífico (Singapur)            | 174946120834     |
| ap-south-1     | Asia-Pacífico (Mumbai)              | 251508486986     |
| ap-southeast-3 | Asia-Pacífico (Yakarta)             | 510637619217     |



|                |                                        |              |
|----------------|----------------------------------------|--------------|
| sa-east-1      | América del Sur (São Paulo)            | 758426053663 |
| ap-northeast-3 | Asia-Pacífico (Osaka)                  | 273192626886 |
| eu-south-1     | Europa (Milán)                         | 266869475730 |
| af-south-1     | África (Ciudad del Cabo)               | 197869348890 |
| ap-southeast-2 | Asia-Pacífico (Sídney)                 | 005257825471 |
| me-central-1   | Medio Oriente (EAU)                    | 000014521398 |
| us-west-1      | Oeste de EE. UU. (Norte de California) | 684579721401 |
| ca-central-1   | Canadá (centro)                        | 354763396469 |
| ca-west-1      | Oeste de Canadá (Calgary)              | 339712888787 |
| ap-south-2     | Asia-Pacífico (Hyderabad)              | 950823858135 |
| eu-south-2     | Europa (España)                        | 919611009337 |
| eu-central-2   | Europa (Zúrich)                        | 529164026651 |
| ap-southeast-4 | Asia-Pacífico (Melbourne)              | 251357961535 |
| ap-southeast-7 | Asia-Pacífico (Tailandia)              | 054037130133 |
| il-central-1   | Israel (Tel Aviv)                      | 870907303882 |
| mx-central-1   | México (centro)                        | 982081086614 |
| ap-east-2      | Asia-Pacífico (Taipei)                 | 259886477082 |

b. Descargar la plantilla

En el siguiente comando para descargar la clave pública apropiada, la firma del RPM x86\_64, la firma del RPM arm64 y el enlace de acceso correspondiente a los scripts

RPM alojados en buckets de Amazon S3, asegúrese de sustituir el ID de cuenta por el ID de Cuenta de AWS apropiado y la región por la región actual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/x86_64/amazon-guardduty-agent-1.15.0.x86_64.rpm ./amazon-guardduty-agent-1.15.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/x86_64/amazon-guardduty-agent-1.15.0.x86_64.sig ./amazon-guardduty-agent-1.15.0.x86_64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.15.0/publickey.pem ./publickey.pem
```

c. Importar la clave pública

Utilice el siguiente comando para importar la clave pública a la base de datos:

```
gpg --import publickey.pem
```

gpg muestra que la importación se realizó correctamente

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:          imported: 1 (RSA: 1)
```

d. Verificación de la firma

Utilice el siguiente comando para verificar la firma

```
gpg --verify amazon-guardduty-agent-1.15.0.x86_64.sig amazon-guardduty-agent-1.15.0.x86_64.rpm
```

Si aprueba la verificación, verá un mensaje similar al resultado que se muestra a continuación. Ahora puede proceder a instalar el agente de GuardDuty seguridad mediante RPM.

Ejemplo de código de salida:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
```

```
gpg:          There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Si la verificación falla, significa que la firma en RPM ha sido potencialmente manipulada. Debe eliminar la clave pública de la base de datos e intentar de nuevo el proceso de verificación.

Ejemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilice el siguiente comando para eliminar la clave pública de la base de datos:

```
gpg --delete-keys AwsGuardDuty
```

Ahora, intente de nuevo el proceso de verificación.

2. [Conéctese con SSH desde Linux o macOS.](#)
3. Instale el agente GuardDuty de seguridad mediante el siguiente comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.15.0.x86_64.rpm
```

4. Compruebe si la instalación del GuardDuty agente está en buen estado. Para obtener más información sobre los pasos, consulte [Validación del estado de instalación GuardDuty del agente de seguridad.](#)

## Debian installation

### Important

Recomendamos comprobar la firma Debian del agente de GuardDuty seguridad antes de instalarlo en su máquina.

1. Compruebe la firma de Debian del agente GuardDuty de seguridad

- a. Prepare plantillas para la clave pública adecuada, la firma del paquete de Debian amd64, la firma del paquete de Debian arm64 y el enlace de acceso correspondiente a los scripts de Debian alojados en buckets de Amazon S3.

En las plantillas siguientes, sustituya el valor del identificador de AWS cuenta y la Región de AWS versión del GuardDuty agente para acceder a los scripts de los paquetes de Debian.

- Clave pública

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/
publickey.pem
```

- GuardDuty firma Debian del agente de seguridad:

Firma de amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/amd64/
amazon-guardduty-agent-1.15.0.amd64.sig
```

Firma de arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/arm64/
amazon-guardduty-agent-1.15.0.arm64.sig
```

- Enlaces de acceso a los scripts Debian en el bucket de Amazon S3:

Enlace de acceso para amd64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/amd64/
amazon-guardduty-agent-1.15.0.amd64.deb
```

Enlace de acceso para arm64

```
s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/arm64/
amazon-guardduty-agent-1.15.0.arm64.deb
```

Región de AWS

Nombre de la región

AWS ID de cuenta

|                |                                     |              |
|----------------|-------------------------------------|--------------|
| eu-west-1      | Europa (Irlanda)                    | 694911143906 |
| us-east-1      | Este de EE. UU. (Norte de Virginia) | 593207742271 |
| us-west-2      | Oeste de EE. UU. (Oregón)           | 733349766148 |
| eu-west-3      | Europa (París)                      | 665651866788 |
| us-east-2      | Este de EE. UU. (Ohio)              | 307168627858 |
| eu-central-1   | Europa (Fráncfort)                  | 323658145986 |
| ap-northeast-2 | Asia-Pacífico (Seúl)                | 914738172881 |
| eu-north-1     | Europa (Estocolmo)                  | 591436053604 |
| ap-east-1      | Asia-Pacífico (Hong Kong)           | 258348409381 |
| me-south-1     | Middle East (Bahrain)               | 536382113932 |
| eu-west-2      | Europa (Londres)                    | 892757235363 |
| ap-northeast-1 | Asia-Pacífico (Tokio)               | 533107202818 |
| ap-southeast-1 | Asia-Pacífico (Singapur)            | 174946120834 |
| ap-south-1     | Asia-Pacífico (Mumbai)              | 251508486986 |
| ap-southeast-3 | Asia-Pacífico (Yakarta)             | 510637619217 |
| sa-east-1      | América del Sur (São Paulo)         | 758426053663 |
| ap-northeast-3 | Asia-Pacífico (Osaka)               | 273192626886 |
| eu-south-1     | Europa (Milán)                      | 266869475730 |
| af-south-1     | África (Ciudad del Cabo)            | 197869348890 |

|                |                                        |              |
|----------------|----------------------------------------|--------------|
| ap-southeast-2 | Asia-Pacífico (Sídney)                 | 005257825471 |
| me-central-1   | Medio Oriente (EAU)                    | 000014521398 |
| us-west-1      | Oeste de EE. UU. (Norte de California) | 684579721401 |
| ca-central-1   | Canadá (centro)                        | 354763396469 |
| ca-west-1      | Oeste de Canadá (Calgary)              | 339712888787 |
| ap-south-2     | Asia-Pacífico (Hyderabad)              | 950823858135 |
| eu-south-2     | Europa (España)                        | 919611009337 |
| eu-central-2   | Europa (Zúrich)                        | 529164026651 |
| ap-southeast-4 | Asia-Pacífico (Melbourne)              | 251357961535 |
| il-central-1   | Israel (Tel Aviv)                      | 870907303882 |
| mx-central-1   | México (centro)                        | 982081086614 |
| ap-east-2      | Asia-Pacífico (Taipéi)                 | 259886477082 |

- b. Descargue la clave pública adecuada, la firma de amd64, la firma de arm64 y el enlace de acceso correspondiente a los scripts de Debian alojados en los buckets de Amazon S3

En los siguientes comandos, sustituya el identificador de cuenta por el Cuenta de AWS identificador correspondiente y la región por su región actual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/
amd64/amazon-guardduty-agent-1.15.0.amd64.deb ./amazon-guardduty-
agent-1.15.0.amd64.deb
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/
amd64/amazon-guardduty-agent-1.15.0.amd64.sig ./amazon-guardduty-
agent-1.15.0.amd64.sig
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-deb-artifacts/1.15.0/
publickey.pem ./publickey.pem
```

c. Importar la clave pública a la base de datos

```
gpg --import publickey.pem
```

gpg muestra que la importación se realizó correctamente

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:             imported: 1 (RSA: 1)
```

d. Verificación de la firma

```
gpg --verify amazon-guardduty-agent-1.15.0.amd64.sig amazon-guardduty-
agent-1.15.0.amd64.deb
```

Tras una verificación correcta, verá un mensaje similar al siguiente resultado:

Ejemplo de código de salida:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:             There is no indication that the signature belongs to the
owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456 7603 06C9 06A7 093F F49D
```

Ahora puede proceder a instalar el agente GuardDuty de seguridad mediante Debian.

Sin embargo, si se produce un error en la verificación, significa que la firma en el paquete Debian ha sido potencialmente manipulada.

Ejemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

Utilice el siguiente comando para eliminar la clave pública de la base de datos:

```
gpg --delete-keys AwsGuardDuty
```

Ahora, intente de nuevo el proceso de verificación.

2. [Conéctese con SSH desde Linux o macOS.](#)
3. Instale el agente GuardDuty de seguridad mediante el siguiente comando:

```
sudo dpkg -i amazon-guardduty-agent-1.15.0.amd64.deb
```

4. Compruebe si la instalación del GuardDuty agente está en buen estado. Para obtener más información sobre los pasos, consulte [Validación del estado de instalación GuardDuty del agente de seguridad.](#)

## Error de falta de memoria

Si se produce un out-of-memory error al instalar o actualizar manualmente el agente de GuardDuty seguridad para Amazon EC2, consulte. [Solución de problemas de memoria insuficiente](#)

## Validación del estado de instalación GuardDuty del agente de seguridad

Una vez realizados los pasos para instalar el agente GuardDuty de seguridad, utilice los siguientes pasos para validar el estado del agente:

Para validar si el agente GuardDuty de seguridad está en buen estado

1. [Conéctese con SSH desde Linux o macOS.](#)
2. Ejecute el siguiente comando para comprobar el estado del agente de GuardDuty seguridad:

```
sudo systemctl status amazon-guardduty-agent
```

Si desea ver los registros de instalación del agente de seguridad, están disponibles en `/var/log/amzn-guardduty-agent/`.

Para ver los registros, realice `sudo journalctl -u amazon-guardduty-agent`.

## Actualización manual del agente GuardDuty de seguridad para la instancia de Amazon EC2

GuardDuty publica actualizaciones de las versiones del agente de seguridad. Si administra el agente de seguridad manualmente, es responsable de actualizar el agente para las instancias de Amazon



EC2. Para obtener información sobre las nuevas versiones de los agentes, consulte [GuardDuty versiones de lanzamiento del agente de seguridad](#) para las instancias de Amazon EC2. Para recibir notificaciones sobre el lanzamiento de una nueva versión del agente, consulte [Suscripción a los anuncios de Amazon GuardDuty SNS](#).

Para actualizar manualmente el agente de seguridad para una instancia de Amazon EC2

El proceso para actualizar el agente de seguridad es el mismo que para instalarlo. Según el método que haya utilizado para instalar el agente, puede seguir los pasos que se indican en [Instalación manual del agente de seguridad](#) para las instancias de Amazon EC2.

Si utiliza el [método 1: Mediante el uso AWS Systems Manager](#), puede actualizar el agente de seguridad mediante el comando Ejecutar. Utilice la versión del agente a la que desea actualizar.

Si utiliza el [Método 2: mediante administradores de paquetes de Linux](#), puede usar los scripts tal como se indica en la sección [Instalación manual del agente de seguridad](#). Los scripts ya incluyen la versión más reciente del agente. Para obtener información sobre las versiones de agentes lanzadas recientemente, consulte [GuardDuty versiones de agentes de seguridad para instancias de Amazon EC2](#).

Después de actualizar el agente de seguridad, puede comprobar el estado de la instalación al consultar los registros. Para obtener más información, consulte [Validación del estado de instalación GuardDuty del agente de seguridad](#).

## Administrar el agente de seguridad automatizado para Fargate (solo Amazon ECS)

Runtime Monitoring permite administrar el agente de seguridad para sus clústeres de Amazon ECS (AWS Fargate) únicamente a través de GuardDuty. No se admite la administración manual del agente de seguridad en los clústeres de Amazon ECS.

Antes de continuar con los pasos de esta sección, asegúrese de cumplir con [Requisitos previos para AWS Fargate Soporte \(solo Amazon ECS\)](#).

En función de [Enfoques para gestionar los agentes GuardDuty de seguridad en ECS-Fargate los recursos de Amazon](#), elija el método que prefiera para habilitar el agente GuardDuty automatizado en sus recursos.

## Configuración del GuardDuty agente para un entorno de múltiples cuentas

En un entorno de varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar la configuración automática de agentes para las cuentas de los miembros y administrar la configuración automatizada de los agentes para los clústeres de Amazon ECS que pertenecen a las cuentas de los miembros de su organización. La cuenta de un GuardDuty miembro no puede modificar esta configuración. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para obtener más información sobre los entornos de varias cuentas, consulte [Administrar varias cuentas](#) en GuardDuty.

### Habilitar la configuración automática de agentes para la cuenta de administrador delegado GuardDuty

#### Manage for all Amazon ECS clusters (account level)

Si ha elegido Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución, tendrá las siguientes opciones:

- Seleccione Activar para todas las cuentas en la sección de configuración automatizada de agentes. GuardDuty desplegará y gestionará el agente de seguridad para todas las tareas de Amazon ECS que se inicien.
- Elija Configurar cuentas manualmente.

Si ha elegido Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente:

1. Elija Configurar cuentas manualmente en la sección Configuración automatizada del agente.
2. Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).

Seleccione Save.

Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```

```
}  
]  
}
```

3. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

4. En el panel de navegación, elija Supervisión en tiempo de ejecución.

5.

 Note

Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, elija Habilitar en la Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

6. Seleccione Save.

7. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser `GuardDutyManaged=true`.

2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
    }
  ]
}
```

```

        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:TagResource",
                "ecs:UntagResource"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}

```

 Note

Al utilizar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar el GuardDuty agente mediante la configuración automática de agentes de forma explícita.

3. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Auto-enable para todas las cuentas de los miembros

Manage for all Amazon ECS clusters (account level)

Los siguientes pasos presuponen que ha elegido Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución.

1. Seleccione Activar para todas las cuentas en la sección de configuración automática de agentes. GuardDuty desplegará y gestionará el agente de seguridad para todas las tareas de Amazon ECS que se inicien.
2. Seleccione Save.
3. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.



Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged=false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
```

```

        "ecs:ResourceTag/GuardDutyManaged": false
    }
}
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {

```

```
    "aws:PrincipalTag/GuardDutyManaged": true
  }
}
}
```

3. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, elija Editar.

6. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

7. Seleccione Save.
8. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

## Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Independientemente de cómo decida habilitar la Supervisión en tiempo de ejecución, los pasos que se indican a continuación sirven para supervisar tareas específicas de Amazon ECS Fargate para todas las cuentas de miembro de la organización.

1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que seleccionó en el paso anterior.
2. Seleccione Save.
3. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```

```
}  
]  
}
```

 Note

Al usar etiquetas de inclusión para sus clústeres de Amazon ECS, no necesita habilitar la administración automática de GuardDuty agentes de forma explícita.

4. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Habilitar la configuración automática del agente para las cuentas de miembro activas existentes

Manage for all Amazon ECS clusters (account level)

1. En la página Supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración automatizada del agente.
2. En el panel de configuración automática de agentes, en la sección Cuentas de miembros activos, seleccione Acciones.
3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
4. Elija Confirmar.
5. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la

Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como `GuardDutyManaged=false`.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",

```

```

        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
    },
    "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
    }
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {

```



```
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
]
```

3. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, en la sección Configuración automatizada del agente, en Cuentas de miembro activas, elija Acciones.

6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

7. Elija Confirmar.
8. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.

- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

### Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ],
  {
```

```

        "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "GuardDutyManaged"
                ]
            }
        }
    },
    {
        "Sid": "DenyModifyTagsIfPrinTagNotExists",
        "Effect": "Deny",
        "Action": [
            "ecs:TagResource",
            "ecs:UntagResource"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
            },
            "Null": {
                "aws:PrincipalTag/GuardDutyManaged": true
            }
        }
    }
]

```

```
}
```

**Note**

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

3. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Auto-enable Configuración automatizada de agentes para nuevos miembros

Manage for all Amazon ECS clusters (account level)

1. En la página Supervisión en tiempo de ejecución, elija Editar para actualizar la configuración existente.
2. En la sección Configuración automatizada del agente, seleccione Habilitar automáticamente para nuevas cuentas de miembro.
3. Seleccione Save.
4. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged-false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}

```

```
}  
  }  
] }  
}
```

3. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 Note

Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de activar la configuración automática de agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la pestaña Configuración, seleccione Habilitar automáticamente para nuevas cuentas de miembro en la sección Configuración automatizada del agente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

6. Seleccione Save.
7. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

## Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
2. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
```



```

        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

 Note

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

3. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Habilitar la Configuración automatizada del agente para cuentas de miembro activas de forma selectiva

Manage for all Amazon ECS (account level)

1. En la página Cuentas, seleccione las cuentas para las que quiere habilitar la configuración del Monitoring-Automated agente Runtime (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con la Supervisión en tiempo de ejecución.
2. En Editar planes de protección, elija la opción adecuada para habilitar la configuración del Monitoring-Automated agente de ejecución (ECS-Fargate).
3. Elija Confirmar.
4. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Agregue una etiqueta a este clúster de Amazon ECS con el par de clave y valor como GuardDutyManaged=false.
2. Evite la modificación de las etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
```

```

        "ecs:ResourceTag/GuardDutyManaged": false
    }
}
},
{
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {

```

```
    "aws:PrincipalTag/GuardDutyManaged": true
  }
}
}
```

3. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
4. En el panel de navegación, elija Supervisión en tiempo de ejecución.
- 5.

 **Note**

Añada siempre la etiqueta de exclusión a sus clústeres de Amazon ECS antes de habilitar la administración automática de GuardDuty agentes en su cuenta; de lo contrario, el contenedor GuardDuty sidecar se adjuntará a todos los contenedores de las tareas de Amazon ECS que se lancen.

En la página Cuentas, seleccione las cuentas para las que desee habilitar la configuración del Monitoring-Automated agente Runtime (ECS-Fargate). Puede seleccionar varias cuentas. Asegúrese de que las cuentas que seleccione en este paso ya estén habilitadas con la Supervisión en tiempo de ejecución.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

6. En Editar planes de protección, elija la opción adecuada para habilitar la configuración del Monitoring-Automated agente en tiempo de ejecución (ECS-Fargate).
7. Seleccione Save.
8. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de habilitar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.

- [update-service](#) en la Referencia del comando de la AWS CLI .

## Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Asegúrese de no habilitar la configuración automática de agentes (o la configuración de Monitoring-Automated agentes en tiempo de ejecución (ECS-Fargate)) para las cuentas seleccionadas que tienen los clústeres de Amazon ECS que desea supervisar.
2. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
3. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    }
  ]
}
```

```

    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": [
            "GuardDutyManaged"
          ]
        }
      }
    },
    {
      "Sid": "DenyModifyTagsIfPrinTagNotExists",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
        },
        "Null": {
          "aws:PrincipalTag/GuardDutyManaged": true
        }
      }
    }
  }

```

```
}  
]  
}
```

 Note

Al utilizar etiquetas de inclusión para los clústeres de Amazon ECS, no necesita habilitar la Configuración automatizada del agente de forma explícita.

4. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

Configurar el GuardDuty agente para una cuenta independiente

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración:
  - a. Para administrar la Configuración automatizada del agente para todos los clústeres de Amazon ECS (nivel de cuenta)

Elija Habilitar en la sección Configuración automatizada del agente para AWS Fargate (sólo ECS). Cuando se lance una nueva tarea de Fargate Amazon ECS, GuardDuty gestionará el despliegue del agente de seguridad.

- Seleccione Save.



- b. Para administrar la Configuración automatizada del agente mediante la exclusión de algunos de los clústeres de Amazon ECS (nivel de clúster)
  - i. Agregue una etiqueta al clúster de Amazon ECS para el que desea excluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged-false.
  - ii. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ecs:ResourceTag/GuardDutyManaged":
            "${aws:PrincipalTag/GuardDutyManaged}",
          "aws:PrincipalArn":
            "arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
          "ecs:ResourceTag/GuardDutyManaged": false
        }
      }
    },
    {
      "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
```

```

        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
            "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": [
                "GuardDutyManaged"
            ]
        }
    }
},
{
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
        },
        "Null": {
            "aws:PrincipalTag/GuardDutyManaged": true
        }
    }
}
]
}

```

- iii. En la pestaña Configuración, elija Habilitar en la sección Configuración automatizada del agente.

 Note

Añada siempre la etiqueta de exclusión a su clúster de Amazon ECS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el agente de seguridad se desplegará en todas las tareas que se lancen dentro del clúster de Amazon ECS correspondiente.

En el caso de los clústeres de Amazon ECS que no se hayan excluido, GuardDuty gestionará el despliegue del agente de seguridad en el contenedor sidecar.

- iv. Seleccione Save.
- c. Para administrar la Configuración automatizada del agente mediante la inclusión de algunos de los clústeres de Amazon ECS (nivel de clúster).
  - i. Agregue una etiqueta a un clúster de Amazon ECS para el que desee incluir todas las tareas. El par de clave y valor debe ser GuardDutyManaged=true.
  - ii. Evite la modificación de estas etiquetas, excepto por las entidades de confianza. La política proporcionada en [Evitar la modificación de etiquetas excepto por entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations ha sido modificada para ser aplicable en esta situación.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
      "Effect": "Deny",
      "Action": [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringNotEquals": {
        "ecs:ResourceTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "Null": {
        "ecs:ResourceTag/GuardDutyManaged": false
      }
    }
  },
  {
    "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:RequestTag/GuardDutyManaged":
"${aws:PrincipalTag/GuardDutyManaged}",
        "aws:PrincipalArn":
"arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "ForAnyValue:StringEquals": {
        "aws:TagKeys": [
          "GuardDutyManaged"
        ]
      }
    }
  },
  {
    "Sid": "DenyModifyTagsIfPrinTagNotExists",
    "Effect": "Deny",
    "Action": [
      "ecs:TagResource",
      "ecs:UntagResource"
    ],

```

```
    "Resource": [
      "*"
    ],
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalArn":
          "arn:aws:iam::123456789012:role/org-admins/iam-admin"
      },
      "Null": {
        "aws:PrincipalTag/GuardDutyManaged": true
      }
    }
  }
}
```

4. Si GuardDuty desea supervisar las tareas que forman parte de un servicio, es necesario implementar un nuevo servicio después de activar Runtime Monitoring. Si la última implementación de un servicio ECS específico se inició antes de habilitar la Supervisión en tiempo de ejecución, puede reiniciar el servicio o actualizarlo mediante `forceNewDeployment`.

Para conocer los pasos a seguir para actualizar el servicio, consulte los siguientes recursos:

- [Actualizar un servicio de Amazon ECS mediante la consola](#) en la Guía para desarrolladores de Amazon Elastic Container Service.
- [UpdateService](#) en la referencia de la API de Amazon Elastic Container Service.
- [update-service](#) en la Referencia del comando de la AWS CLI .

## Administración automática del agente de seguridad para los recursos de Amazon EKS

La monitorización del tiempo de ejecución permite activar el agente de seguridad mediante una configuración GuardDuty automática y manual. En esta sección se indican los pasos necesarios para habilitar la configuración automatizada del agente para los clústeres de Amazon EKS.

Antes de continuar, asegúrese de haber cumplido con los [Requisitos previos para la compatibilidad con clústeres de Amazon EKS](#).

Según el enfoque que prefiera para [Administre el agente de seguridad mediante GuardDuty](#), elija los pasos a seguir en las próximas secciones en consecuencia.

## Configuración automatizada del agente para entornos de varias cuentas

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar la configuración automática de agentes para las cuentas de los miembros y administrar el agente automatizado para los clústeres de EKS que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

### Configuración de la configuración automática del agente para la cuenta de administrador delegado GuardDuty

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                            | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Administre el agente de seguridad mediante GuardDuty</p> <p>(Supervisión de todos los clústeres de EKS)</p> | <p>Si eligió Habilitar para todas las cuentas en la sección Supervisión en tiempo de ejecución, dispondrá de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• Seleccione Activar para todas las cuentas en la sección de configuración automática del agente. GuardDuty desplegará y gestionará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de GuardDuty administrador delegado y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembros existentes y potencialmente nuevas de la organización.</li> <li>• Elija Configurar cuentas manualmente.</li> </ul> <p>Si ha elegido Configurar cuentas manualmente en la sección Supervisión en tiempo de ejecución, haga lo siguiente:</p> <ol style="list-style-type: none"> <li>1. Elija Configurar cuentas manualmente en la sección Configuración automatizada del agente.</li> <li>2. Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).</li> </ol> |

|                                                                            |                  |
|----------------------------------------------------------------------------|------------------|
| <b>Enfoque preferido para administrar el agente GuardDuty de seguridad</b> | <b>Pasos</b>     |
|                                                                            | Seleccione Save. |

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                           | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión) | <p>De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación.</p> <p>Para excluir un clúster de EKS de la supervisión cuando el agente GuardDuty de seguridad no se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> </li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li> </ol> |



| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>4. En el panel de navegación, elija Supervisión en tiempo de ejecución.</p> <div data-bbox="586 432 1507 793" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <p>5. En la pestaña Configuración, seleccione Activar en la sección de administración de GuardDuty agentes.</p> <p>En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.</p> <p>6. Seleccione Save.</p> <p>Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster</p> <p>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</p> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:</p> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> .</li> <li>• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <i>access-project</i> por <code>GuardDutyManaged</code></li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"> <li>3. Si tenía un agente automatizado habilitado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</li> </ol> <p>Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> <ol style="list-style-type: none"> <li>4. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad          | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión | <p>Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultarán útiles a la hora de supervisar determinados clústeres de EKS en la cuenta:</p> <ol style="list-style-type: none"> <li>1. Asegúrese de seleccionar Inhabilitar la cuenta de GuardDuty administrador delegado (esta cuenta) en la sección de configuración automática del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione Save.</li> <li>3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</p> <ol style="list-style-type: none"> <li>4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> |

|                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                                                     | <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Administre el agente GuardDuty de seguridad manualmente             | <p>Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS.</p> <ol style="list-style-type: none"> <li>1. Asegúrese de seleccionar Inhabilitar la cuenta de GuardDuty administrador delegado (esta cuenta) en la sección de configuración automática del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione Save.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Auto-enable Agente automatizado para todas las cuentas de los miembros

### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                                  | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Administre el agente de seguridad mediante GuardDuty</p> <p>(Supervisión de todos los clústeres de EKS)</p>       | <p>Este tema es para habilitar la Supervisión en tiempo de ejecución para todas las cuentas de miembro y, por lo tanto, los siguientes pasos suponen que la opción Habilitar para todas las cuentas se ha elegido en la sección Supervisión en tiempo de ejecución.</p> <ol style="list-style-type: none"> <li>1. Seleccione Activar para todas las cuentas en la sección de configuración automática del agente. GuardDuty desplegará y gestionará el agente de seguridad para todos los clústeres de EKS que pertenezcan a la cuenta de GuardDuty administrador delegado y también para todos los clústeres de EKS que pertenezcan a todas las cuentas de miembros existentes y potencialmente nuevas de la organización.</li> <li>2. Seleccione Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)</p> | <p>De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación.</p> <p>Excluir un clúster de EKS de la supervisión cuando el agente GuardDuty de seguridad no se haya desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <ol style="list-style-type: none"> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> </ul> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <ul style="list-style-type: none"> <li>• Reemplace <i>access-project</i> por GuardDutyManaged</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"> <li>3. Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li> <li>4. En el panel de navegación, elija Supervisión en tiempo de ejecución.</li> </ol> <div data-bbox="586 1056 1508 1417"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar el agente automatizado en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <ol style="list-style-type: none"> <li>5. En la pestaña Configuración, elija Editar en la sección Configuración de la supervisión en tiempo de ejecución.</li> <li>6. Elija Habilitar para todas las cuentas en la sección Configuración automatizada del agente. En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.</li> <li>7. Seleccione Save.</li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li> <p>Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</p> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> </li> <li> <p>Si tenía habilitada la configuración automática del agente para este clúster de EKS, después de este paso, no GuardDuty se actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</p> <p>Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> </li> <li> <p>Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:</p> <ul style="list-style-type: none"> <li>Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li><code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <div data-bbox="620 428 1507 625"><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></div> <ol style="list-style-type: none"><li>4. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</li></ol> |



| Enfoque preferido para administrar el agente GuardDuty de seguridad           | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determina dos clústeres de EKS mediante etiquetas de inclusión | <p>Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS para todas las cuentas de miembros en la organización:</p> <ol style="list-style-type: none"> <li>1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione Save.</li> <li>3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</p> <ol style="list-style-type: none"> <li>4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Administre el agente GuardDuty de seguridad manualmente             | <p>Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS.</p> <ol style="list-style-type: none"> <li>1. No habilite ninguna configuración en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione Save.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Habilitar el agente automatizado para todas las cuentas de miembro activas existentes

### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

Para administrar el agente GuardDuty de seguridad para las cuentas de miembros activos existentes en su organización

- GuardDuty Para recibir los eventos en tiempo de ejecución de los clústeres de EKS que pertenecen a las cuentas de los miembros activos existentes en la organización, debe elegir el enfoque que prefiera para administrar el agente de GuardDuty seguridad de estos clústeres de

EKS. Para obtener más información acerca de cada uno de estos métodos, consulte [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#).

| Método preferido para administrar los agentes GuardDuty de seguridad                                    | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administre el agente de seguridad mediante GuardDuty<br><br>(Supervisión de todos los clústeres de EKS) | Supervisión de todos los clústeres de EKS para todas las cuentas de miembros activas existentes<br><br><ol style="list-style-type: none"><li>1. En la página Supervisión del tiempo de ejecución, en la pestaña Configuración, puede ver el estado actual de la configuración automatizada del agente.</li><li>2. En el panel Configuración automatizada del agente, en la sección Cuentas de miembro activas, seleccione Acciones.</li><li>3. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.</li><li>4. Elija Confirmar.</li></ol> |

| Método preferido para administrar los agentes GuardDuty de seguridad                                             | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <p>De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación.</p> <p>Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> </li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> |

| Método preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li>3. Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li>4. En el panel de navegación, elija Supervisión en tiempo de ejecución.</li></ol> <div><p> <b>Note</b></p><p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automática del agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p></div> <ol style="list-style-type: none"><li>5. En la pestaña Configuración, en la sección Configuración automatizada del agente, en Cuentas de miembro activas, elija Acciones.</li><li>6. En Acciones, seleccione Habilitar para todas las cuentas de miembros activas.</li><li>7. Elija Confirmar.</li></ol> |

| Método preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <p>Para excluir un clúster de EKS de la supervisión una vez que el agente de GuardDuty seguridad ya se haya implementado en este clúster</p> <ol style="list-style-type: none"><li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.<br/><br/>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.<br/><br/>Tras este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</li><li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:<ul style="list-style-type: none"><li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li><li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li><li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li></ul></li></ol> |

| Método preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <ul style="list-style-type: none"><li>• <b>123456789012</b> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li></ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li>3. Independientemente de cómo administre el agente de seguridad (a través GuardDuty o manualmente), para dejar de recibir los eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad desplegado de este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</li></ol> |

| Método preferido para administrar los agentes GuardDuty de seguridad         | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión | <ol style="list-style-type: none"> <li>1. En la página Cuentas, después de habilitar la Supervisión en tiempo de ejecución, no habilite Supervisión en tiempo de ejecución: configuración automatizada del agente.</li> <li>2. Agregue una etiqueta al clúster de EKS que pertenezca a la cuenta seleccionada que desee supervisar. El par de clave-valor de la etiqueta debe ser <code>GuardDutyManaged -true</code>.<br/><br/>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.<br/><br/>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</li> <li>3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> |



| Método preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                                                               |
| Administre el agente GuardDuty de seguridad manualmente              | <ol style="list-style-type: none"> <li>1. Asegúrese de no elegir <b>Habilitar</b> en la sección <b>Configuración automatizada del agente</b>. Mantenga habilitada la <b>Supervisión en tiempo de ejecución</b>.</li> <li>2. Seleccione <b>Save</b>.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

### Auto-enable configuración automatizada de agentes para nuevos miembros

| Enfoque preferido para administrar los agentes GuardDuty de seguridad                                   | Pasos                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administre el agente de seguridad mediante GuardDuty<br><br>(Supervisión de todos los clústeres de EKS) | <ol style="list-style-type: none"> <li>1. En la página <b>Supervisión en tiempo de ejecución</b>, elija <b>Editar</b> para actualizar la configuración existente.</li> <li>2. En la sección <b>Configuración automatizada del agente</b>, seleccione <b>Habilitar automáticamente para nuevas cuentas de miembro</b>.</li> <li>3. Seleccione <b>Save</b>.</li> </ol> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad                                         | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión) | <p>De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación.</p> <p>Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> </li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el ID de la entidad de confianza.</li> </ul> </li> </ol> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                       | <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"><li>3. Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li><li>4. En el panel de navegación, elija Supervisión en tiempo de ejecución.</li></ol> <div> <b>Note</b><p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automática del agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p></div> <ol style="list-style-type: none"><li>5. En la pestaña Configuración, selecciona Activar automáticamente las cuentas de nuevos miembros en la sección de administración de GuardDuty agentes.<p>En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.</p></li><li>6. Seleccione Save.</li></ol> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                       | <p>Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>Independientemente de si administra el agente de GuardDuty seguridad de forma automática GuardDuty o manual, añada una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>. <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>Si tenía el agente automatizado habilitado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</p> <p>Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> </li> <li>Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la</li> </ol> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                       | <p>Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:</p> <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> .</li> <li>• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <i>access-project</i> por GuardDuty Managed</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad        | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión | <p>Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS para las nuevas cuentas de miembro en la organización.</p> <ol style="list-style-type: none"> <li>1. Asegúrese de desmarcar <b>Habilitar automáticamente</b> para nuevas cuentas de miembro en la sección <b>Configuración automatizada del agente</b>. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione <b>Save</b>.</li> <li>3. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>.<br/><br/>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.<br/><br/>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</li> <li>4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> </ul> </li> </ol> |

| Enfoque preferido para administrar los agentes GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                       | <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <i>access-project</i> por GuardDuty Managed</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                                      |
| Administre el agente GuardDuty de seguridad manualmente               | <p>Independientemente de cómo haya decidido habilitar la supervisión en tiempo de ejecución, puede administrar el agente de seguridad manualmente para los clústeres de EKS.</p> <ol style="list-style-type: none"> <li>1. Asegúrese de desmarcar la casilla Habilitar automáticamente para nuevas cuentas de miembro en la sección Configuración automatizada del agente. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior.</li> <li>2. Seleccione Save.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Configurar el agente automatizado para cuentas de miembro activas de forma selectiva

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                                  | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Administre el agente de seguridad mediante GuardDuty</p> <p>(Supervisión de todos los clústeres de EKS)</p>       | <ol style="list-style-type: none"> <li>1. En la página Cuentas, seleccione las cuentas para las que desea activar la Configuración automatizada del agente. Puede seleccionar más de una cuenta a la vez. Asegúrese de que las cuentas que seleccione en este paso ya tengan habilitada la supervisión en tiempo de ejecución de EKS.</li> <li>2. En Editar planes de protección, elija la opción adecuada para habilitar la Supervisión en tiempo de ejecución: configuración automatizada del agente.</li> <li>3. Elija Confirmar.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante etiquetas de exclusión)</p> | <p>De los siguientes procedimientos, elija uno de los escenarios que se aplique a su situación.</p> <p>Para excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <ol style="list-style-type: none"> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> </ul> </li> </ol> |



| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <ul style="list-style-type: none"> <li>• <b>123456789012</b> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"> <li>Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li> </ol> <div data-bbox="584 892 1510 1249"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de activar la configuración automática a del agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <ol style="list-style-type: none"> <li>En la página Cuentas, seleccione la cuenta para la que desee habilitar Administrar agente automáticamente. Puede seleccionar más de una cuenta a la vez.</li> <li>En Editar planes de protección, elija la opción adecuada para habilitar la configuración del Monitoring-Automated agente Runtime para la cuenta seleccionada.</li> </ol> <p>En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.</p> <ol style="list-style-type: none"> <li>Seleccione Save.</li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad se ha desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>Si anteriormente tenía habilitada la configuración del agente automatizado para este clúster de EKS, después de este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</p> <p>Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información sobre la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> <ol style="list-style-type: none"> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> </ul> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <ul style="list-style-type: none"><li>• <b>123456789012</b> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li></ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <div data-bbox="618 554 1507 751"><pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre></div> <ol style="list-style-type: none"><li>3. Si administraba el agente de GuardDuty seguridad de este clúster de EKS de forma manual, debe eliminarlo. Para obtener más información, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</li></ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad           | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determina dos clústeres de EKS mediante etiquetas de inclusión | <p>Independientemente de cómo haya decidido habilitar la Supervisión en tiempo de ejecución, los siguientes pasos resultan útiles a la hora de supervisar determinados clústeres de EKS que pertenecen a las cuentas seleccionadas:</p> <ol style="list-style-type: none"> <li>1. Asegúrese de no habilitar la configuración del Monitoring-Automated agente Runtime para las cuentas seleccionadas que tienen los clústeres de EKS que desea supervisar.</li> <li>2. Agregue una etiqueta a su clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>.</li> </ol> <p>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p>Tras añadir la etiqueta, GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</p> <ol style="list-style-type: none"> <li>3. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyala por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                                                                                                                                                                                                                                                                         |
| Administre el agente GuardDuty de seguridad manualmente             | <ol style="list-style-type: none"> <li>1. Mantenga la misma configuración de Supervisión en tiempo de ejecución que en el paso anterior. Asegúrese de no habilitar Supervisión en tiempo de ejecución: configuración automatizada del agente para ninguna de las cuentas seleccionadas.</li> <li>2. Elija Confirmar.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Configurar el agente automatizado para una cuenta independiente

Una cuenta independiente es la propietaria de la decisión de habilitar o deshabilitar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la Supervisión en tiempo de ejecución para entornos de múltiples cuentas](#).

Después de activar Runtime Monitoring, asegúrese de instalar el agente GuardDuty de seguridad mediante una configuración automática o un despliegue manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según su preferencia de supervisar todos o algunos recursos de Amazon EKS, elija el método que prefiera y siga los pasos que se indican en la tabla siguiente.

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

2. En el panel de navegación, elija Supervisión en tiempo de ejecución.
3. En la pestaña Configuración, elija Habilitar para habilitar la configuración automatizada del agente para la cuenta.

| Método preferido para implementar un agente GuardDuty de seguridad                                               | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administre el agente de seguridad mediante GuardDuty<br><br>(Supervisión de todos los clústeres de EKS)          | <ol style="list-style-type: none"> <li>1. Seleccione Activar en la sección de configuración automática del agente. GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de EKS existentes y potencialmente nuevos de su cuenta.</li> <li>2. Seleccione Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <p>De los siguientes procedimientos, elija uno de los escenarios que le corresponda.</p> <p>Excluir un clúster de EKS de la supervisión cuando el agente de GuardDuty seguridad no se haya desplegado en este clúster</p> <ol style="list-style-type: none"> <li>1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.<br/><br/>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:</li> </ol> |

| Método preferido para implementar un agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> .</li> <li>• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <i>access-project</i> por GuardDuty Managed</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <ol style="list-style-type: none"> <li>3. Abra la GuardDuty consola en <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a>.</li> <li>4. En el panel de navegación, elija Supervisión en tiempo de ejecución.</li> </ol> <div> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a sus clústeres de EKS antes de habilitar la administración automática del GuardDuty agente en su cuenta; de lo contrario, el agente de GuardDuty seguridad se</p> </div> |

| Método preferido para implementar un agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <div data-bbox="756 296 1520 432">desplegará en todos los clústeres de EKS de su cuenta.</div> <p data-bbox="691 443 1495 527">5. En la pestaña Configuración, seleccione Activar en la sección de administración de GuardDuty agentes.</p> <p data-bbox="756 569 1495 747">En el caso de los clústeres de EKS que no se hayan excluido de la supervisión, GuardDuty gestionará el despliegue y las actualizaciones del agente GuardDuty de seguridad.</p> <p data-bbox="691 768 1000 810">6. Seleccione Save.</p> <p data-bbox="691 884 1446 1010">Excluir un clúster de EKS de la supervisión después de que el agente de GuardDuty seguridad ya se haya desplegado en este clúster</p> <p data-bbox="691 1062 1487 1188">1. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>false</code>.</p> <p data-bbox="756 1230 1487 1409">Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.</p> <p data-bbox="756 1451 1495 1734">Tras este paso, no GuardDuty actualizará el agente de seguridad de este clúster. Sin embargo, el agente de seguridad permanecerá desplegado y GuardDuty seguirá recibiendo los eventos de tiempo de ejecución de este clúster de EKS. Esto puede afectar a sus estadísticas de uso.</p> <p data-bbox="691 1755 1503 1829">2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política</p> |



| Método preferido para implementar un agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <p>que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes:</p> <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por <code>eks:TagResource</code> .</li> <li>• Sustituya <i>ec2:DeleteTags</i> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <i>access-project</i> por GuardDuty Managed</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> <p>3. Para dejar de recibir eventos de tiempo de ejecución de este clúster, debe eliminar el agente de seguridad implementado de este clúster de EKS. Para obtener más información acerca de la eliminación del agente de seguridad implementado, consulte <a href="#">Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución</a>.</p> |

| Método preferido para implementar un agente GuardDuty de seguridad           | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS mediante etiquetas de inclusión | <ol style="list-style-type: none"> <li>1. Asegúrese de no elegir Desactivar en la sección Configuración automatizada del agente. Mantenga habilitada la Supervisión en tiempo de ejecución.</li> <li>2. Seleccione Guardar.</li> <li>3. Agregue una etiqueta a este clúster de EKS con la clave como <code>GuardDutyManaged</code> y su valor como <code>true</code>.<br/><br/>Para obtener más información sobre el etiquetado del clúster de Amazon EKS, consulte <a href="#">Etiquetado de los recursos para facturación</a> en la Guía del usuario de Amazon EKS.<br/><br/>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para los clústeres de EKS selectivos que desee supervisar.</li> <li>4. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> </li> </ol> |

| Método preferido para implementar un agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre data-bbox="805 495 1396 726">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre>                                    |
| Administración manual del agente                                   | <ol style="list-style-type: none"> <li>1. Asegúrese de no elegir Desactivar en la sección Configuración automatizada del agente. Mantenga habilitada la Supervisión en tiempo de ejecución.</li> <li>2. Seleccione Save.</li> <li>3. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Administrar manualmente el agente de seguridad para el clúster de Amazon EKS

En esta sección se describe cómo puede gestionar su agente complementario (GuardDuty agente) de Amazon EKS después de activar Runtime Monitoring (o EKS Runtime Monitoring). Para utilizar la Supervisión en tiempo de ejecución, debe habilitarla y configurar el complemento de Amazon EKS, `aws-guardduty-agent`. Debe realizar los dos pasos GuardDuty para detectar posibles amenazas y generarlas [GuardDuty Tipos de búsqueda de Runtime Monitoring](#).

Para administrar el agente manualmente, es necesario crear un punto de conexión de VPC como requisito previo. Esto ayuda a GuardDuty recibir los eventos en tiempo de ejecución. Después de esto, puede instalar el agente de seguridad para que GuardDuty comience a recibir los eventos

de tiempo de ejecución de los recursos de Amazon EKS. Cuando GuardDuty publique una nueva versión del agente para este recurso, podrá actualizar la versión del agente en su cuenta.

## Temas

- [Requisito previo: crear un punto de conexión de Amazon VPC](#)
- [Instalación manual GuardDuty del agente de seguridad en los recursos de Amazon EKS](#)
- [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#)

## Requisito previo: crear un punto de conexión de Amazon VPC

Antes de poder instalar el agente GuardDuty de seguridad, debe crear un punto final de Amazon Virtual Private Cloud (Amazon VPC). Esto le ayudará a GuardDuty recibir los eventos de tiempo de ejecución de sus recursos de Amazon EKS.

### Note

El uso del punto de conexión de VPC no conlleva ningún costo adicional.

Elija el método de acceso que prefiera para crear un punto de conexión de Amazon VPC.

## Console

Para crear un punto de conexión de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, en Nube virtual privada, seleccione Puntos de conexión.
3. Seleccione Crear punto de conexión.
4. En la página Crear punto de conexión, en Categoría de servicio, elija Otros servicios de punto de conexión.
5. En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de **us-east-1** reemplazarla por la región correcta. Debe ser la misma región que el clúster de EKS que pertenece a su Cuenta de AWS ID.

6. Elija Verificar el servicio.
7. Una vez que el nombre del servicio se haya verificado correctamente, elija la VPC en la que reside el clúster. Agregue la siguiente política para restringir el uso de los puntos de conexión

de VPC únicamente a la cuenta especificada. Con el valor de `Condition` de la organización que se indica debajo de esta política, puede actualizar la siguiente política para restringir el acceso a su punto de conexión. Para proporcionar compatibilidad con puntos de conexión de VPC a ID de cuentas específicos de su organización, consulte [Organization condition to restrict access to your endpoint](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Allow",
      "Principal": "*"
    },
    {
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      },
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Principal": "*"
    }
  ]
}
```

El ID de cuenta de `aws:PrincipalAccount` debe coincidir con la cuenta que contiene la VPC y el punto de conexión de VPC. En la siguiente lista se muestra cómo compartir el punto de conexión de VPC con otros ID de Cuenta de AWS :

Condición de la organización para restringir el acceso a su punto de conexión

- Si quiere especificar varias cuentas para acceder al punto de conexión de VPC, sustituya `"aws:PrincipalAccount": "111122223333"` por lo siguiente:

```
"aws:PrincipalAccount": [  
    "666666666666",  
    "555555555555"  
]
```

- Para permitir que todos los miembros de una organización accedan al punto de conexión de VPC, sustituya "aws:PrincipalAccount": "**111122223333**" por lo siguiente:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Para restringir el acceso a un recurso a un ID de organización, agregue su ResourceOrgID a la política.

Para obtener más información, consulte [ResourceOrgID](#).

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. En Configuración adicional, seleccione Habilitar nombre de DNS.
9. En Subredes, elija las subredes en las que reside el clúster.
10. En Grupos de seguridad, elija un grupo de seguridad que tenga el puerto de entrada 443 habilitado desde su VPC (o su clúster de EKS). Si aún no tiene ningún grupo de seguridad que tenga habilitado el puerto de entrada 443, [cree un grupo de seguridad](#).

Si se produce un problema al restringir los permisos de entrada a la VPC (o instancia), puede utilizar el puerto de entrada 443 desde cualquier dirección IP (0.0.0.0/0). Sin embargo, GuardDuty recomienda utilizar direcciones IP que coincidan con el bloque CIDR de la VPC. Para obtener más información, consulte [Bloques de CIDR de VPC](#) en la Guía del usuario de Amazon VPC.

## API/CLI

Para crear un punto de conexión de VPC

- Invoca. [CreateVpcEndpoint](#)
- Utilice los siguientes valores para los parámetros:
  - En Nombre del servicio, escriba **com.amazonaws.us-east-1.guardduty-data**.

Asegúrese de reemplazarla por *us-east-1* la región correcta. Debe ser la misma región que el clúster de EKS que pertenece a su Cuenta de AWS ID.

- Para [DNSOptions](#), establezca la opción de DNS privado en `true` para habilitarla.
- Para ello AWS Command Line Interface, consulte [create-vpc-endpoint](#).

Una vez que haya seguido los pasos, consulte [Validar la configuración del punto de conexión de VPC](#) para asegurarse de que el punto de conexión de VPC se configuró correctamente.

## Instalación manual GuardDuty del agente de seguridad en los recursos de Amazon EKS

En esta sección se describe cómo puede implementar el agente GuardDuty de seguridad por primera vez en clústeres de EKS específicos. Antes de continuar con esta sección, asegúrese de que ya ha configurado los requisitos previos y habilitado la Supervisión en tiempo de ejecución para las cuentas. El agente GuardDuty de seguridad (complemento EKS) no funcionará si no habilita Runtime Monitoring.

Elija el método de acceso que prefiera para implementar el agente de GuardDuty seguridad por primera vez.

### Console

1. Abra la consola Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. Elija un nombre para el clúster.
3. Elija la pestaña Add-ons.
4. Escoja Obtener más complementos.
5. En la página Seleccionar complementos, elija Amazon GuardDuty EKS Runtime Monitoring.
6. GuardDuty recomienda elegir la versión del agente más reciente y la predeterminada.
7. En la página Definir configuración del complemento seleccionado, utilice la configuración predeterminada. Si el estado de su complemento de EKS es Requiere activación, seleccione Activar GuardDuty. Esta acción abrirá la GuardDuty consola para configurar Runtime Monitoring para sus cuentas.
8. Una vez que haya configurado la Supervisión en tiempo de ejecución para las cuentas, vuelva a la consola de Amazon EKS. El estado de su complemento de EKS debería haber cambiado a Listo para instalar.

## 9. (Opcional) Proporcionar esquema de configuración del complemento de EKS

Para la versión complementaria, si elige la versión 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener información sobre los rangos de parámetros, consulte [Configurar los parámetros del complemento de EKS](#).

- a. Amplíe Ajustes de configuración opcionales para ver los parámetros que se pueden configurar y su valor y formato previstos.
- b. Establezca los parámetros. Los valores deben estar en el rango proporcionado en [Configurar los parámetros del complemento de EKS](#).
- c. Elija Guardar cambios para crear el complemento según la configuración avanzada.
- d. En Método de resolución de conflictos, la opción que elija se utilizará para resolver conflictos en caso de que actualice el valor de un parámetro a un valor que no sea el predeterminado. Para obtener más información sobre las opciones enumeradas, consulte [resolveConflicts](#) en la Referencia de la API de Amazon EKS.

10. Elija Siguiente.

11. En la página Revisar y crear, compruebe todos los detalles y elija Crear.

12. Vuelva a los detalles del clúster y elija la pestaña Recursos.

13. Puede ver los nuevos pods con el prefijo aws-guardduty-agent.

## API/CLI

Puede configurar el agente del complemento de Amazon EKS (aws-guardduty-agent) mediante una de las siguientes opciones:

- Ejecute [CreateAddon](#) para su cuenta.

- 



### Note

En el caso del complemento `version`, si elige la versión 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener más información, consulte [Configurar los parámetros del complemento de EKS](#).

Utilice los siguientes valores para los parámetros de la solicitud:

- En `addonName`, introduzca `aws-guardduty-agent`.



Puede utilizar el siguiente AWS CLI ejemplo cuando utilice valores configurables compatibles con las versiones complementarias v1.5.0 o superiores. Asegúrese de sustituir los valores del marcador de posición resaltados en rojo y el `Example.json` asociado por los valores configurados.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.15.0-eksbuild.2 --configuration-values 'file://example.json'
```

### Example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
      "memory": "2048Mi"
    }
  }
}
```

- Para obtener más información sobre los valores de `addonVersion` admitidos, consulte [Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty](#).
- Como alternativa, puede utilizar AWS CLI. Para obtener más información, consulte [create-addon](#).

### Nombres de DNS privados para el punto de conexión de VPC

De forma predeterminada, el agente de seguridad resuelve el nombre de DNS privado del punto de conexión de VPC y se conecta a este. En el caso de un punto de conexión que no sea FIPS, su DNS privado aparecerá en el siguiente formato:

Non-FIPS punto final — `guardduty-data.us-east-1.amazonaws.com`

El Región de AWS, *us-east-1*, cambiará en función de su región.

## Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS

Si administra el agente GuardDuty de seguridad manualmente, es responsable de actualizarlo para su cuenta. Para recibir notificaciones sobre nuevas versiones del agente, puede suscribirse a una fuente RSS en [GuardDuty versiones de lanzamiento del agente de seguridad](#).

Puede actualizar el agente de seguridad a la versión más reciente para aprovechar la compatibilidad y las mejoras introducidas. Si la compatibilidad estándar de la versión actual del agente está a punto de finalizar, para continuar con el uso de Runtime Monitoring (o Runtime Monitoring de EKS), deberá actualizar a la versión siguiente disponible o la más reciente del agente.

### Requisito previo

Antes de actualizar la versión del agente de seguridad, asegúrese de que la versión del agente que tiene previsto utilizar ahora sea compatible con la versión de Kubernetes. Para obtener más información, consulte [Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty](#).

### Console

1. Abra la consola Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. Elija un nombre para el clúster.
3. En la información del clúster, seleccione la Add-onspestaña.
4. En la Add-onspestaña, selecciona GuardDutyEKS Runtime Monitoring.
5. Elija Editar para actualizar los detalles del agente.
6. En la página Configurar la monitorización del tiempo de ejecución de GuardDuty EKS, actualice los detalles.
7. (Opcional) Actualizar los valores de configuración opcionales

Si la versión del complemento de EKS es la 1.5.0 o una posterior, también puede actualizar el esquema de configuración del complemento.

- a. Amplíe los Ajustes de configuración opcionales para ver el esquema de configuración.
- b. Actualice los valores del parámetro en función del rango proporcionado en [Configurar los parámetros del complemento de EKS](#).
- c. Elija Guardar cambios para iniciar la actualización.

- d. En Método de resolución de conflictos, la opción que elija se utilizará para resolver conflictos en caso de que actualice el valor de un parámetro a un valor que no sea el predeterminado. Para obtener más información sobre las opciones enumeradas, consulte [resolveConflicts](#) en la Referencia de la API de Amazon EKS.

## API/CLI

Para actualizar el agente GuardDuty de seguridad de sus clústeres de Amazon EKS, consulte [Actualización de un complemento](#).

### Note

Para el `complementoversion`, si elige la versión 1.5.0 o superior, Runtime Monitoring permite configurar parámetros específicos del GuardDuty agente. Para obtener información sobre los rangos de parámetros, consulte [Configurar los parámetros del complemento de EKS](#).

Puede usar el siguiente AWS CLI ejemplo cuando utilice valores configurables compatibles con las versiones 1.5.0 y posteriores del complemento. Asegúrese de sustituir los valores del marcador de posición resaltados en rojo y el `Example.json` asociado por los valores configurados.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-name aws-guardduty-agent --addon-version v1.15.0-eksbuild.2 --configuration-values 'file://example.json'
```

## Example.json

```
{
  "priorityClassName": "aws-guardduty-agent.priorityclass-high",
  "dnsPolicy": "Default",
  "resources": {
    "requests": {
      "cpu": "237m",
      "memory": "512Mi"
    },
    "limits": {
      "cpu": "2000m",
```

```
"memory": "2048Mi"
}
}
}
```

Si la versión del complemento de Amazon EKS es 1.5.0 o posterior y ha configurado el esquema del complemento, puede comprobar si los valores aparecen correctamente para el clúster. Para obtener más información, consulte [Verificar las actualizaciones del esquema de configuración](#).

## Configurar los parámetros del agente de GuardDuty seguridad (complemento) para Amazon EKS

Puede configurar parámetros específicos de su agente de GuardDuty seguridad para Amazon EKS. Este soporte está disponible para la versión 1.5.0 y superior del agente de GuardDuty seguridad. Para obtener información sobre las versiones más recientes del complemento, consulte [GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS](#).

¿Por qué debo actualizar el esquema de configuración del agente de seguridad?

El esquema de configuración del agente GuardDuty de seguridad es el mismo en todos los contenedores de los clústeres de Amazon EKS. Cuando los valores predeterminados no se ajusten a las cargas de trabajo asociadas ni al tamaño de la instancia, considere la posibilidad de configurar los ajustes de la CPU, memoria, `PriorityClass` y `dnsPolicy`. Independientemente de cómo administre el GuardDuty agente para sus clústeres de Amazon EKS, puede configurar o actualizar la configuración existente de estos parámetros.

## Comportamiento de configuración automatizada del agente con parámetros configurados

Cuando GuardDuty administra el agente de seguridad (complemento EKS) en su nombre, actualiza el complemento según sea necesario. GuardDuty establecerá el valor de los parámetros configurables en un valor predeterminado. Sin embargo, es posible actualizar los parámetros al valor deseado. Si esto provoca un conflicto, la opción predeterminada para [resolveConflicts](#) es `None`.

## Parámetros y valores que se pueden configurar

Para obtener información sobre los pasos a seguir para configurar los parámetros del complemento, consulte:

- [Instalación manual GuardDuty del agente de seguridad en los recursos de Amazon EKS](#) o
- [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#)

En las siguientes tablas se indican los rangos y valores que puede utilizar para implementar el complemento de Amazon EKS manualmente o actualizar la configuración existente del complemento.

#### Configuración de la CPU

| Parameters                    | Predeterminado     | Rango configurable                     |
|-------------------------------|--------------------|----------------------------------------|
| Solicitudes                   | 200m               | Entre 200m y 10000m, incluidos ambos   |
| Límites                       | 1000m              | Entre 200m y 10000m, incluidos ambos   |
| <code>disableCpuLimits</code> | <code>false</code> | <code>true</code> o <code>false</code> |

El `disableCpuLimits` parámetro está disponible para la versión 1.12.1-eksbuild.3 y posteriores del agente de GuardDuty seguridad. En versiones anteriores, el complemento no admite este parámetro y las API del complemento de Amazon EKS (`CreateAddon`, `UpdateAddon`) devuelven un error de validación si lo especifica.

Si lo configura `disableCpuLimits` `true`, el pod del agente de seguridad no impone un límite de CPU. La configuración de otros recursos no se ve afectada.

Para deshabilitar los límites de la CPU, utilice la siguiente configuración:

```
{"resources":{"disableCpuLimits":true}}
```

#### Configuración de memoria

| Parameters  | Predeterminado | Rango configurable                     |
|-------------|----------------|----------------------------------------|
| Solicitudes | 256Mi          | Entre 256Mi y 20000Mi, ambos incluidos |

| Parameters | Predeterminado | Rango configurable |
|------------|----------------|--------------------|
| Límites    | 1024Mi         |                    |

## Configuración de **PriorityClass**

Cuando GuardDuty crea un complemento de Amazon EKS para usted, el asignado **PriorityClass** es `aws-guarddduty-agent.priorityclass`. Esto significa que no se tomará ninguna medida en función de la prioridad del pod del agente. Para configurar este parámetro del complemento, elija una de las siguientes opciones de **PriorityClass**:

| <b>PriorityClass</b> configura<br>ble                | Valor de<br><b>preemptio<br/>nPolicy</b> | Descripción de <b>preemptio<br/>nPolicy</b>                                                                             | Valor del pod |
|------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------|
| <code>aws-guarddduty-agent.priorityclass</code>      | Never                                    | Sin acciones                                                                                                            | 1000000       |
| <code>aws-guarddduty-agent.priorityclass-high</code> | PreemptLowerPriority                     | Asignar este valor dará prioridad a un pod en ejecución con un valor de prioridad inferior al valor del pod del agente. | 100000000     |
| <code>system-cluster-critical</code> <sup>1</sup>    | PreemptLowerPriority                     |                                                                                                                         | 2000000000    |
| <code>system-node-critical</code> <sup>1</sup>       | PreemptLowerPriority                     |                                                                                                                         | 2000001000    |

<sup>1</sup> Kubernetes proporciona estas dos opciones de **PriorityClass**: `system-cluster-critical` y `system-node-critical`. Para obtener más información, consulte la documentación de [PriorityClass](#) Kubernetes.

## Configuración de **dnsPolicy**

Elija una de las siguientes opciones de política de DNS compatibles con Kubernetes. Cuando no se especifica ninguna configuración, `ClusterFirst` se utiliza como valor predeterminado.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Para obtener información sobre estas políticas, consulte [Política de DNS del pod](#) en la documentación de Kubernetes.

## Verificar las actualizaciones del esquema de configuración

Una vez configurados los parámetros, siga los siguientes pasos para comprobar que el esquema de configuración se ha actualizado:

1. Abra la consola Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación, seleccione Clusters (Clústeres).
3. En la página Clústeres, seleccione el Nombre del clúster cuyas actualizaciones desea verificar.
4. Elija la pestaña Recursos.
5. En el panel Tipos de recursos, en Cargas de trabajo, elija. DaemonSets
6. Seleccione `aws-guardduty-agent`.
7. En la página `aws-guardduty-agent`, elija Vista sin procesar para ver la respuesta JSON sin formato. Compruebe que los parámetros que se pueden configurar muestran el valor proporcionado.

Tras la verificación, cambie a la GuardDuty consola. Seleccione el correspondiente Región de AWS y consulte el estado de cobertura de sus clústeres de Amazon EKS. Para obtener más información, consulte [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#).

## Validar la configuración del punto de conexión de VPC

Tras instalar el agente de seguridad manualmente o mediante una configuración GuardDuty automática, puede utilizar este documento para validar la configuración del punto final de la VPC. También puede seguir estos pasos después de solucionar cualquier [problema de cobertura en](#)

[tiempo de ejecución](#) para un tipo de recurso. Puede asegurarse de que los pasos han funcionado según lo previsto, y la cobertura podría aparecer en Buen estado.

Siga los siguientes pasos para validar que la configuración del punto de conexión de VPC para el tipo de recurso se ha establecido correctamente en la cuenta de propietario de VPC:

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/vpc/>
2. En el panel de navegación, en Nube privada virtual, seleccione Sus VPC.
3. En la página Sus VPC, elija el CIDR de IPv4 asociado a su ID de VPC.
4. En el panel de navegación, en Nube virtual privada, seleccione Puntos de conexión.
5. En la tabla de puntos de conexión, seleccione la fila que tenga el nombre del servicio similar a com.amazonaws. **us-east-1**.guardduty-data. La región (us-east-1) podría ser diferente para el punto de conexión.
6. Aparecerá un panel para los detalles del punto de conexión. En la pestaña Grupos de seguridad, seleccione el enlace correspondiente al ID del grupo asociado para obtener más detalles.
7. En la tabla de Grupos de seguridad, seleccione la fila con el ID del grupo de seguridad asociado para ver los detalles.
8. En la pestaña Reglas de entrada, asegúrese de que exista una política de ingreso con el Rango de puertos configurado como 443 y el Origen como el valor copiado desde el CIDR de IPv4. Las reglas de entrada controlan el tráfico entrante autorizado a alcanzar la instancia. La siguiente imagen muestra las reglas de entrada de un grupo de seguridad que está asociado a la VPC utilizada por GuardDuty el agente de seguridad.

Si aún no tiene un grupo de seguridad que tenga habilitado un puerto de entrada 443, [Cree un grupo de seguridad](#) en la Guía del usuario de Amazon EC2.

Si se produce un problema al restringir los permisos de entrada a su VPC (o clúster), proporcione soporte al puerto 443 entrante desde cualquier dirección IP (0.0.0.0/0).

La siguiente lista incluye elementos que conviene conocer después de instalar o actualizar el agente de seguridad.

Evaluar la cobertura en tiempo de ejecución

El siguiente paso después de instalar o actualizar el agente de seguridad consiste en evaluar la cobertura en tiempo de ejecución de los recursos. Si la cobertura en tiempo de ejecución está en



mal estado, debe solucionar el problema. Para obtener más información, consulte [Problemas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Si la cobertura en tiempo de ejecución está en buen estado, indica que la Supervisión en tiempo de ejecución puede recopilar y recibir eventos en tiempo de ejecución. Para obtener una lista de estos eventos, consulte [Tipos de eventos de tiempo de ejecución recopilados](#).

#### Nombre de DNS privado para puntos de conexión

Después de instalar el agente de GuardDuty seguridad para sus recursos, de forma predeterminada, se resolverá y se conectará al nombre de DNS privado del punto final de la VPC. En el caso de un punto de conexión que no sea FIPS, el DNS privado aparecerá en el siguiente formato:

`guardduty-data.us-east-1.amazonaws.com`

El Región de AWS, *us-east-1*, cambiará en función de su región.

#### Un host se puede instalar con dos agentes de seguridad

Al trabajar con un agente de GuardDuty seguridad para una instancia de Amazon EC2, puede instalar y usar el agente en el host subyacente dentro de un clúster de Amazon EKS. Si ya había implementado un agente de seguridad en ese clúster de EKS, pueden haber dos agentes de seguridad en ejecución en el mismo host al mismo tiempo. Para obtener información sobre cómo GuardDuty funciona en este escenario, consulte [Agentes de seguridad en el mismo host](#).

## Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas

Una vez que habilita Runtime Monitoring y el agente de GuardDuty seguridad se despliega en su recurso, GuardDuty proporciona estadísticas de cobertura para el tipo de recurso correspondiente y el estado de cobertura individual de los recursos que pertenecen a su cuenta. El estado de la cobertura se determina asegurándose de que ha habilitado Runtime Monitoring, de que se ha creado su punto de enlace de Amazon VPC y de que se ha implementado el agente de GuardDuty seguridad del recurso correspondiente. Un estado de cobertura en buen estado indica que, cuando hay un evento de tiempo de ejecución relacionado con su recurso, GuardDuty puede recibir dicho evento de tiempo de ejecución a través del punto de enlace de Amazon VPC y monitorear el comportamiento. Si se produjo un problema al configurar Runtime Monitoring, crear un punto de conexión de Amazon VPC o implementar el agente de GuardDuty seguridad, el estado de

la cobertura aparece como En mal estado. Cuando el estado de la cobertura no sea adecuado, no GuardDuty podrá recibir ni monitorear el comportamiento en tiempo de ejecución del recurso correspondiente ni generar ningún resultado de monitorización del tiempo de ejecución.

Los siguientes temas le ayudarán a revisar las estadísticas de cobertura, configurar EventBridge las notificaciones y solucionar los problemas de cobertura de un tipo de recurso específico.

## Contenido

- [Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2](#)
- [Cobertura y solución de problemas en tiempo de ejecución para clústeres de Amazon ECS](#)
- [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#)

## Cobertura en tiempo de ejecución y resolución de problemas para la instancia de Amazon EC2

Para los recursos de Amazon EC2, la cobertura en tiempo de ejecución se evalúa a nivel de instancia. Las instancias de Amazon EC2 pueden ejecutar varios tipos de aplicaciones y cargas de trabajo, entre otros, en el entorno de AWS . Esta característica también admite las instancias de Amazon EC2 administradas por Amazon ECS y, si tiene clústeres de Amazon ECS que se ejecutan en una instancia de Amazon EC2, los problemas de cobertura a nivel de instancia aparecerán en la cobertura en tiempo de ejecución de Amazon EC2.

## Temas

- [Revisión de las estadísticas de cobertura](#)
- [El estado de la cobertura cambia con EventBridge notificaciones](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#)

## Revisión de las estadísticas de cobertura

Las estadísticas de cobertura para las instancias de Amazon EC2 asociadas a cuentas propias o a cuentas de miembro corresponden al porcentaje de instancias de EC2 en buen estado respecto al total de instancias de EC2 de la Región de AWS seleccionada. La siguiente ecuación lo representa de la siguiente manera:

$$(\text{instances/All Instancias en buen estado}) * 100$$

Si también ha implementado el agente de GuardDuty seguridad para sus clústeres de Amazon ECS, cualquier problema de cobertura a nivel de instancia asociado a los clústeres de Amazon ECS que se ejecuten en una instancia de Amazon EC2 aparecerá como un problema de cobertura del tiempo de ejecución de una instancia de Amazon EC2.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

## Console

- Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Elija la pestaña Cobertura en tiempo de ejecución.
- En la pestaña Cobertura en tiempo de ejecución de instancias de EC2, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada instancia de Amazon EC2 que esté disponible en la tabla de la lista de instancias.
- Puede filtrar la tabla Lista de instancias por las siguientes columnas:
  - ID de cuenta
  - Tipo de administración del agente
  - Versión del agente
  - Estado de la cobertura
  - ID de instancia
  - ARN del clúster
- Si alguna de las instancias de EC2 tiene la cobertura en mal estado, la columna Problema incluye información adicional sobre el motivo del mal estado.

## API/CLI

- Ejecute la [ListCoverage](#) API con su propio ID de detector válido, la región actual y el punto de conexión del servicio. Puede filtrar y ordenar la lista de instancias a través de esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
  - `ACCOUNT_ID`
  - `RESOURCE_TYPE`
  - `COVERAGE_STATUS`

- AGENT\_VERSION
- MANAGEMENT\_TYPE
- INSTANCE\_ID
- CLUSTER\_ARN
- Cuando `filter-criteria` incluye RESOURCE\_TYPE como EC2, la Supervisión en tiempo de ejecución no admite el uso de PROBLEMA como el AttributeName. Si lo utiliza, la respuesta de la API generará una `InvalidInputException`.

Puede cambiar el ejemplo de AttributeName en `sort-criteria` con las siguientes opciones:

- ACCOUNT\_ID
- COVERAGE\_STATUS
- INSTANCE\_ID
- UPDATED\_AT
- Puede cambiar el *max-results* (hasta 50).
- Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"} } ]}' --max-results 5
```

- Ejecute la [GetCoverageStatisticsAPI](#) para recuperar las estadísticas agregadas de cobertura en función de `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
  - COUNT\_BY\_COVERAGE\_STATUS: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
  - COUNT\_BY\_RESOURCE\_TYPE— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
  - Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
    - ACCOUNT\_ID

- RESOURCE\_TYPE
  - COVERAGE\_STATUS
  - AGENT\_VERSION
  - MANAGEMENT\_TYPE
  - INSTANCE\_ID
  - CLUSTER\_ARN
- Para encontrar las detectorId correspondientes a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Si la cobertura de la instancia de EC2 está en mal estado, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#).

## El estado de la cobertura cambia con EventBridge notificaciones

Es posible que la cobertura de la instancia de Amazon EC2 aparezca en mal estado. Para mantenerse informado sobre los cambios en el estado de la cobertura, recomendamos supervisar periódicamente su estado y solucionar cualquier problema si esta se encuentra en mal estado. Como alternativa, puedes crear una EventBridge regla de Amazon para recibir una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o no. De forma predeterminada, la GuardDuty publica en el [EventBridge bus](#) de tu cuenta.

### Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta [Crear regla](#) en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su instancia Amazon EC2 cambie de Healthy

aUnhealthy, detail-type debería ser así. *GuardDuty Runtime Protection Unhealthy*  
 Para recibir una notificación cuando el estado de la cobertura cambie de Unhealthy aHealthy, sustituya el valor de detail-type por. *GuardDuty Runtime Protection Healthy*

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EC2",
      "ec2InstanceDetails": {
        "instanceId": "",
        "instanceType": "",
        "clusterArn": "",
        "agentDetails": {
          "version": ""
        },
        "managementType": ""
      }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

## Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2

Si la cobertura de la instancia de Amazon EC2 está en mal estado, puede ver el motivo en la columna Problema.

Si la instancia de EC2 está asociada a un clúster de EKS y el agente de seguridad para EKS se instaló manualmente o mediante la configuración automatizada del agente, para solucionar el problema de cobertura, consulte [Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS](#).

En la siguiente tabla se enumeran los tipos de problemas y los pasos de resolución de problemas correspondientes.

| Tipo de problema                         | Mensaje del problema               | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | A la espera de la notificación SSM | <p>Recibir la notificación SSM puede tardar unos minutos.</p> <p>Asegúrese de que SSM administra la instancia de Amazon EC2. Para obtener más información, consulte los pasos del Método 1: Mediante AWS Systems Manager en <a href="#">Instalación manual del agente de seguridad</a>.</p>                                                                                                          |
| No hay generación de informes de agentes | (Vacío a propósito)                | <p>Si administra el agente de GuardDuty seguridad manualmente, asegúrese de haber seguido los pasos que se indican a continuación <a href="#">Administrar manualmente el agente de seguridad para el recurso de Amazon EC2</a>.</p> <p>Si ha habilitado la configuración automatizada del agente:</p> <ul style="list-style-type: none"> <li>La instancia de EC2 es administrada por SSM.</li> </ul> |

| Tipo de problema | Mensaje del problema | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                      | <ul style="list-style-type: none"><li>• Consulte periódicamente el estado del agente de seguridad. Para obtener más información, consulte <a href="#">Validación del estado de instalación GuardDuty del agente de seguridad</a>.</li></ul> <p>Compruebe que el punto de conexión de VPC para la instancia de Amazon EC2 está configurado correctamente. Para obtener más información, consulte <a href="#">Validar la configuración del punto de conexión de VPC</a>.</p> <p>Si la organización cuenta con una política de control de servicio (SCP), valide que el límite de permisos no restringe el permiso <code>guardduty:SendSecurityTelemetry</code>. Para obtener más información, consulte <a href="#">Validación de la política de control de servicios de la organización en un entorno de varias cuentas</a>.</p> |



| Tipo de problema       | Mensaje del problema                                                         | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | Agente desconectado                                                          | <ul style="list-style-type: none"> <li>• Consulte el estado del agente de seguridad. Para obtener más información, consulte <a href="#">Validación del estado de instalación GuardDuty del agente de seguridad</a>.</li> <li>• Consulte los registros del agente de seguridad para identificar la posible causa raíz. Los registros proporcionan errores detallados que puede utilizar para solucionar el problema por su cuenta. Los archivos de registro están disponibles en <code>/var/log/amzn-guardduty-agent/</code>.</li> </ul> <p>Realice <code>sudo journalctl -u amazon-guardduty-agent</code>.</p> |
| Agente no provisionado | Las instancias con etiquetas de exclusión se excluyen de Runtime Monitoring. | <p>GuardDuty no recibe eventos de tiempo de ejecución de las instancias de Amazon EC2 que se lanzan con la etiqueta de exclusión:GuardDutyManaged . false</p> <p>Para recibir eventos de tiempo de ejecución de esta instancia de Amazon EC2, elimine la etiqueta de exclusión.</p>                                                                                                                                                                                                                                                                                                                            |

| Tipo de problema | Mensaje del problema                                       | Pasos para la solución de problemas                                                                                                                                                                                       |
|------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | La versión del kernel es inferior a la versión compatible. | Para obtener información sobre las versiones de kernel compatibles en todas las distribuciones de sistemas operativos, consulte <a href="#">Validar los requisitos de arquitectura</a> para las instancias de Amazon EC2. |
|                  | La versión del kernel es superior a la versión compatible. | Para obtener información sobre las versiones de kernel compatibles en todas las distribuciones de sistemas operativos, consulte <a href="#">Validar los requisitos de arquitectura</a> para las instancias de Amazon EC2. |

| Tipo de problema | Mensaje del problema                                            | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | No se puede recuperar el documento de identidad de la instancia | <p>Siga estos pasos:</p> <ol style="list-style-type: none"><li>1. Confirme que su recurso sea una instancia de Amazon EC2 y no una instancia híbrida que no sea EC2.</li><li>2. Confirme que el servicio de metadatos de instancias (IMDS) esté habilitado. Para hacerlo, consulte <a href="#">Configuración de las opciones del servicio de metadatos de instancias</a> en la Guía del usuario de Amazon EC2.</li><li>3. Verifique que el documento de identidad de la instancia existe. Para ello, consulte <a href="#">Recuperar el documento de identidad de la instancia</a> en la Guía del usuario de Amazon EC2.</li><li>4. Si el documento de identidad de la instancia sigue sin existir, reinicie la instancia. El documento de identidad de la instancia se genera cuando la instancia se detiene e inicia, se reinicia o se inicia.</li></ol> |

| Tipo de problema                                  | Mensaje del problema                               | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error al crear la asociación de SSM | GuardDuty La asociación SSM ya existe en su cuenta | <ol style="list-style-type: none"><li>1. Elimine manualmente la asociación existente. Para obtener más información, consulte <a href="#">Eliminar asociaciones</a> en la Guía del usuario de AWS Systems Manager .</li><li>2. Tras eliminar la asociación, deshabilite y vuelva a habilitar la configuración GuardDuty automática del agente para Amazon EC2.</li></ol>                                                                                                                             |
|                                                   | La cuenta tiene demasiadas asociaciones SSM        | <p>Seleccione una de las siguientes dos opciones:</p> <ul style="list-style-type: none"><li>• Elimine cualquier asociación de SSM que no se utilice. Para obtener más información, consulte <a href="#">Eliminar asociaciones</a> en la Guía del usuario de AWS Systems Manager .</li><li>• Verifique si la cuenta cumple los requisitos para un aumento de cuota. Para obtener más información, consulte <a href="#">Service Quotas de Systems Manager</a> en Referencia general de AWS.</li></ul> |

| Tipo de problema                                                | Mensaje del problema                               | Pasos para la solución de problemas                                                                                                                              |
|-----------------------------------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error en la actualización de la asociación de SSM | GuardDuty La asociación SSM no existe en su cuenta | GuardDuty La asociación SSM no está presente en tu cuenta. Desactive y vuelva a habilitar la supervisión en tiempo de ejecución.                                 |
| Se produjo un error al eliminar la asociación de SSM            | GuardDuty La asociación SSM no existe en tu cuenta | La asociación de SSM con GuardDuty no está presente en la cuenta. Si la asociación de SSM se eliminó intencionadamente, no es necesario realizar ninguna acción. |

| Tipo de problema                                                            | Mensaje del problema                                                     | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error en la ejecución de la asociación de la instancia de SSM | No se cumplen los requisitos de arquitectura u otros requisitos previos. | <p>Para obtener información sobre distribuciones de sistemas operativos verificadas, consulte <a href="#">Requisitos previos para la compatibilidad con instancias de Amazon EC2</a>.</p> <p>Si el problema persiste, los siguientes pasos le ayudarán a identificarlo y posiblemente a resolverlo:</p> <ol style="list-style-type: none"><li>1. Abra la AWS Systems Manager consola en. <a href="https://console.aws.amazon.com/systems-manager/">https://console.aws.amazon.com/systems-manager/</a></li><li>2. En el panel de navegación, en Administración de nodos, seleccione Administrador de estados.</li><li>3. Filtre por la propiedad Nombre del documento e ingrese AmazonGuardDuty-ConfigureRuntimeMonitoringSsm Plugin.</li><li>4. Seleccione el ID de asociación correspondiente y consulte su Historial de ejecución.</li></ol> |

| Tipo de problema                                                | Mensaje del problema                                                                                                                                                                                                                                                                               | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                 |                                                                                                                                                                                                                                                                                                    | <p>5. Utilice el historial de ejecución para ver los errores, identificar la posible causa raíz e intentar resolverla.</p>                                                                                                                                                                                                                                                |
| <p>Se produjo un error al crear el punto de conexión de VPC</p> | <p>La creación de puntos de conexión de VPC no es compatible con la VPC compartida <i>vpcId</i></p>                                                                                                                                                                                                | <p>La Supervisión en tiempo de ejecución admite el uso de una VPC compartida dentro de una organización. Para obtener más información, consulte <a href="#">Uso de VPC compartida con Runtime Monitoring</a>.</p>                                                                                                                                                         |
|                                                                 | <p>Solo cuando se utiliza una VPC compartida con una configuración automatizada del agente</p> <p>El ID de cuenta propietario <i>111122223333</i> de la VPC compartida <i>vpcId</i> no tiene habilitada la supervisión del tiempo de ejecución, la configuración automática de agentes o ambas</p> | <p>La cuenta de propietario de la VPC compartida debe habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para al menos un tipo de recurso (Amazon EKS o Amazon ECS [AWS Fargate]). Para obtener más información, consulte <a href="#">Requisitos previos específicos de la supervisión del GuardDuty tiempo de ejecución</a>.</p> |

| Tipo de problema | Mensaje del problema                                                                                                                                                                                                                                                                     | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>Para habilitar el DNS privado, es necesario establecer ambos <code>enableDnsSupport</code> atributos de <code>enableDnsHostnames</code> VPC en <code>true</code> for <i>vpcId</i> (servicio: Ec2, estado Code:400, ID de solicitud:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i></p> | <p>Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte <a href="#">Atributos DNS para la VPC</a>.</p> <p>Si utiliza Amazon VPC Console <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> para crear la Amazon VPC, seleccione <code>Enable DNS hostnames</code> y <code>Enable DNS resolution</code>. Para obtener más información, consulte <a href="#">Opciones de configuración de la VPC</a>.</p> <p>Tras actualizar los atributos de VPC, debe acelerar el reintento de creación del punto de conexión de la VPC al realizar uno de estos cambios:</p> <ul style="list-style-type: none"> <li>• Puede añadir o modificar la etiqueta <code>GuardDutyManaged</code> de su instancia de Amazon EC2 (recomendado). Por ejemplo, puede añadir <code>GuardDutyManaged</code> :<code>true</code> para</li> </ul> |



| Tipo de problema | Mensaje del problema | Pasos para la solución de problemas                                                                                                                                          |
|------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                      | <p>incluir la instancia dRuntime Monitoring.</p> <ul style="list-style-type: none"><li>• Puede cambiar el estado de la instancia Amazon EC2 (detener o reiniciar).</li></ul> |

| Tipo de problema                                                          | Mensaje del problema                                                                                                                                                                        | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error al eliminar el punto de conexión de la VPC compartida | No se permite eliminar el punto final de la VPC compartida para el ID de cuenta <b>111122223333</b> , la VPC <b>vpcId</b> compartida o el ID de cuenta del propietario. <b>555555555555</b> | <p>Medidas posibles:</p> <ul style="list-style-type: none"> <li>Al desactivar el estado de la Supervisión en tiempo de ejecución de la cuenta de participante de la VPC compartida, no se afecta a la política de punto de conexión de VPC compartida ni al grupo de seguridad que existe en la cuenta de propietario.</li> </ul> <p>Para eliminar el punto de conexión de VPC compartida y el grupo de seguridad, debe desactivar la Supervisión en tiempo de ejecución o el estado de la configuración automatizada del agente en la cuenta de propietario de la VPC compartida.</p> <ul style="list-style-type: none"> <li>La cuenta participante de la VPC compartida no puede eliminar el punto de conexión de la VPC compartida ni el grupo de seguridad alojados en la cuenta propietaria de la VPC compartida.</li> </ul> |

| Tipo de problema             | Mensaje del problema | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                       |
|------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| El agente no genera informes | (Vacío a propósito)  | <p>El tipo de problema ya no tiene soporte. Si sigue teniendo este problema y aún no lo ha hecho, active el agente GuardDuty automatizado para Amazon EC2.</p> <p>Si el problema persiste, considere la posibilidad de desactivar la Supervisión en tiempo de ejecución durante unos minutos y, a continuación, vuelva a habilitarla.</p> |

## Cobertura y solución de problemas en tiempo de ejecución para clústeres de Amazon ECS

La cobertura de tiempo de ejecución de los clústeres de Amazon ECS incluye las tareas que se ejecutan en AWS Fargate las instancias de contenedores de Amazon ECS <sup>1</sup>.

Si se trata de un clúster de Amazon ECS que se ejecuta en Fargate, la cobertura en tiempo de ejecución se evalúa a nivel de tarea. La cobertura en tiempo de ejecución de los clústeres de ECS incluye las tareas de Fargate que se han comenzado a ejecutar después de habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para Fargate (solo ECS). De forma predeterminada, las tareas de Fargate son inmutables. GuardDuty no podrá instalar el agente de seguridad para supervisar los contenedores en las tareas que ya estén en ejecución. Para incluir una tarea de Fargate de este tipo, debe detener e iniciar de nuevo la tarea. Asegúrese de verificar si el servicio asociado es compatible.

Para obtener información sobre el contenedor de Amazon ECS, consulte [Creación de capacidad](#).

### Contenido

- [Revisión de las estadísticas de cobertura](#)
- [El estado de la cobertura cambia con EventBridge notificaciones](#)

- [Solución de problemas de cobertura en ECS-Fargate tiempo de ejecución de Amazon](#)

## Revisión de las estadísticas de cobertura

Las estadísticas de cobertura correspondientes a los recursos de Amazon ECS asociados a la cuenta propia o a las cuentas de miembro representan el porcentaje de los clústeres de Amazon ECS en buen estado sobre todos los clústeres de Amazon ECS en la Región de AWS seleccionada. Esto incluye la cobertura para clústeres de Amazon ECS asociados tanto a instancias de Fargate como de Amazon EC2. La siguiente ecuación lo representa de la siguiente manera:

$(\text{clusters/All Clústeres en buen estado}) * 100$

### Consideraciones

- Las estadísticas de cobertura correspondientes al clúster de ECS incluyen el estado de cobertura de las tareas de Fargate o las instancias de contenedor de ECS asociadas a ese clúster de ECS. El estado de cobertura de las tareas de Fargate incluye tareas que están en estado de ejecución o que han terminado de ejecutarse recientemente.
- En la pestaña Cobertura en tiempo de ejecución de clústeres de ECS, el campo Instancias de contenedor cubiertas indica el estado de cobertura de las instancias de contenedor asociadas al clúster de Amazon ECS.

Si su clúster de Amazon ECS contiene solo tareas de Fargate, el recuento aparecerá como. 0/0

- Si el clúster de Amazon ECS está asociado a una instancia de Amazon EC2 que no cuenta con un agente de seguridad, la cobertura del clúster de Amazon ECS también estará en mal estado.

Para identificar y solucionar el problema de cobertura correspondiente a la instancia de Amazon EC2 asociada, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#) para instancias de Amazon EC2.

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

### Console

- Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Elija la pestaña Cobertura en tiempo de ejecución.

- En la pestaña Cobertura en tiempo de ejecución de clústeres de ECS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura de cada clúster de Amazon ECS que esté disponible en la tabla Lista de clústeres.
- Puede filtrar la tabla Lista de clústeres por las siguientes columnas:
  - ID de cuenta
  - Nombre del clúster
  - Tipo de administración del agente
  - Estado de la cobertura
- Si la cobertura de alguno de los clústeres de Amazon ECS está en mal estado, la columna Problema incluye información adicional sobre el motivo del mal estado.

Si los clústeres de Amazon ECS están asociados a una instancia de Amazon EC2, vaya a la pestaña Cobertura en tiempo de ejecución de la instancia de EC2 y filtre por el campo Nombre del clúster para ver el problema asociado.

## API/CLI

- Ejecute la [ListCoverage](#) API con su propio ID de detector válido, la región actual y el punto de conexión del servicio. Puede filtrar y ordenar la lista de instancias a través de esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
- Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
  - `ACCOUNT_ID`
  - `COVERAGE_STATUS`
  - `ISSUE`
  - `ECS_CLUSTER_NAME`
  - `UPDATED_AT`

El campo se actualiza únicamente cuando se crea una nueva tarea en el clúster de Amazon ECS asociado o se produce un cambio en el estado de cobertura correspondiente.

- Puede cambiar el *max-results* (hasta 50).
- Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty --region us-east-1 list-coverage --detector-id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName": "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion": [{"CriterionKey": "ACCOUNT_ID", "FilterCondition": {"EqualsValue": "111122223333"}]}]' --max-results 5
```

- Ejecute la [GetCoverageStatisticsAPI](#) para recuperar las estadísticas agregadas de cobertura en función de `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
  - `COUNT_BY_COVERAGE_STATUS`: representa las estadísticas de cobertura de los clústeres de ECS agregadas por estado de cobertura.
  - `COUNT_BY_RESOURCE_TYPE`— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
  - `ACCOUNT_ID`
  - `ECS_CLUSTER_NAME`
  - `COVERAGE_STATUS`
  - `MANAGEMENT_TYPE`
  - `INSTANCE_ID`
- Para encontrar las `detectorId` correspondientes a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
```

```
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",  
"FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Para obtener más información sobre los problemas de cobertura, consulte [Solución de problemas de cobertura en ECS-Fargate tiempo de ejecución de Amazon](#).

## El estado de la cobertura cambia con EventBridge notificaciones

Es posible que el estado de cobertura del clúster de Amazon ECS aparezca como En mal estado. Para mantenerse informado sobre los cambios en el estado de la cobertura, recomendamos supervisar periódicamente su estado y solucionar cualquier problema si esta se encuentra en mal estado. Como alternativa, puedes crear una EventBridge regla de Amazon para recibir una notificación cuando el estado de la cobertura cambie de Insalubre a Saludable o no. De forma predeterminada, la GuardDuty publica en el [EventBridge bus](#) de tu cuenta.

### Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta [Crear regla](#) en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su clúster de Amazon ECS cambie de Healthy aUnhealthy, detail-type debería ser así*GuardDuty Runtime Protection Unhealthy*. Para recibir una notificación cuando el estado de la cobertura cambie de Unhealthy aHealthy, sustituya el valor detail-type de por*GuardDuty Runtime Protection Healthy*.

```
{  
  "version": "0",  
  "id": "event ID",  
  "detail-type": "GuardDuty Runtime Protection Unhealthy",  
  "source": "aws.guardduty",  
  "account": "Cuenta de AWS ID",  
  "time": "event timestamp (string)",  
  "region": "Región de AWS",  
  "resources": [  
    ],  
  "detail": {
```

```

"schemaVersion": "1.0",
"resourceAccountId": "string",
"currentStatus": "string",
"previousStatus": "string",
"resourceDetails": {
  "resourceType": "ECS",
  "ecsClusterDetails": {
    "clusterName": "",
    "fargateDetails": {
      "issues": [],
      "managementType": ""
    },
    "containerInstanceDetails": {
      "coveredContainerInstances": int,
      "compatibleContainerInstances": int
    }
  },
  "issue": "string",
  "lastUpdatedAt": "timestamp"
}
}

```

## Solución de problemas de cobertura en ECS-Fargate tiempo de ejecución de Amazon

Si la cobertura del clúster de Amazon ECS está en mal estado, puede ver el motivo en la columna Problema.

En la siguiente tabla se indican los pasos recomendados para solucionar los problemas relacionados con Fargate (solo Amazon ECS). Para obtener información sobre problemas de cobertura de instancias de Amazon EC2, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#) para instancias de Amazon EC2.

| Tipo de problema             | Información adicional                                                                       | Pasos recomendados de solución de problemas                                                                                     |
|------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| El agente no genera informes | El agente no genera informes para las tareas en TaskDefinition - ' <b>TASK_DEFINITION</b> ' | Valide que el punto de conexión de VPC para la tarea del clúster de Amazon ECS esté configurado correctamente. Para obtener más |



| Tipo de problema | Información adicional                                                                              | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                                                                                                    | <p>información, consulte <a href="#">Validar la configuración del punto de conexión de VPC</a>.</p> <p>Si la organización cuenta con una política de control de servicio (SCP), valide que el límite de permisos no restringe el permiso <code>guardduty:SendSecurityTelemetry</code>. Para obtener más información, consulte <a href="#">Validación de la política de control de servicios de la organización en un entorno de varias cuentas</a>.</p> |
|                  | <code>VPC_ISSUE ; for task in TaskDefinition - 'TASK_DEFINITION '</code>                           | Consulte los detalles del problema de la VPC en la información adicional.                                                                                                                                                                                                                                                                                                                                                                               |
| El agente salió  | ExitCode: EXIT_CODE para tareas en TaskDefinition - 'TASK_DEFINITION '                             | Consulte los detalles del problema en la información adicional.                                                                                                                                                                                                                                                                                                                                                                                         |
|                  | Motivo: <i>REASON</i> para tareas en TaskDefinition - 'TASK_DEFINITION '                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                  | ExitCode: EXIT_CODE con el motivo: 'EXIT_CODE ' para tareas en TaskDefinition - 'TASK_DEFINITION ' |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Tipo de problema | Información adicional                                                                                                              | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>El agente salió: Motivo: <code>CannotPullContainerError</code> : se ha vuelto a intentar extraer el manifiesto de imagen...</p> | <p>En este escenario, GuardDuty es posible que no pueda ver la imagen del contenedor del sidecar. La tarea seguirá ejecutándose, pero no GuardDuty podrá detectar posibles amenazas. Realice los siguientes pasos de solución de problemas uno por uno para comprobar si esto ayuda a resolver el problema de cobertura:</p> <ul style="list-style-type: none"><li>• <b>Permisos:</b> asegúrese de que su rol de ejecución de tareas tenga los permisos de ECR necesarios que se indican en <a href="#">Requisitos de los permisos</a>.</li><li>• <b>Conectividad de red:</b> verifique que sus tareas de Fargate puedan llegar al ECR a través del acceso público a Internet o de puntos de conexión de VPC configurados correctamente, como se describe en <a href="#">Requisitos de conectividad de red</a>.</li><li>• <b>Configuración del grupo de seguridad:</b> verifique que su grupo de seguridad permite el acceso saliente a la lista</li></ul> |

| Tipo de problema | Información adicional | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                       | <p>de prefijos gestionados de S3 en el puerto 443, como se explica en <a href="#">Configuración del grupo de seguridad</a>.</p> <ul style="list-style-type: none"> <li>• Ejecute el <a href="#">AWS Support t-TroubleshootECSTaskFailedToStart</a> manual en la región de su clúster para identificar problemas específicos.</li> <li>• Consulte los registros de tareas para ver si hay mensajes de error. Para obtener más información sobre cómo hacerlo, consulte <a href="#">Ver registros del agente de contenedores de Amazon ECS</a> en la Guía para desarrolladores de Amazon Elastic Container Service.</li> </ul> <p>Para obtener información sobre errores comunes y solución de problemas, consulte <a href="#">Solución de problemas de Amazon ECS</a> en la Guía para desarrolladores de Amazon Elastic Container Service.</p> <p>Estos tres componentes (permisos, conectividad de</p> |

| Tipo de problema                                                | Información adicional                                                                                                                                                                                                                                                                             | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Se produjo un error al crear el punto de conexión de VPC</p> | <p>La habilitación del DNS privado requiere que ambos <code>enableDnsSupport</code> atributos de <code>enableDnsHostnames</code> VPC estén configurados en <code>true</code> for <i>vpcId</i> (servicio: EC2, estado Code:400, ID de solicitud:). <i>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</i></p> | <p>red y configuración del grupo de seguridad) son independientes, pero todos son necesarios para descargar correctamente la imagen del GuardDuty contenedor de Amazon ECR.</p> <p>Si el problema persiste, consulte <a href="#">Mi AWS Step Functions flujo de trabajo está fallando inesperadamente</a>.</p> <p>Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte <a href="#">Atributos DNS para la VPC</a>.</p> <p>Si utiliza Amazon VPC Console <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> para crear la Amazon VPC, asegúrese de seleccionar <code>Enable DNS hostnames</code> y <code>Enable DNS resolution</code>. Para obtener más información, consulte <a href="#">Opciones de configuración de la VPC</a>.</p> |

| Tipo de problema       | Información adicional                                                                                              | Pasos recomendados de solución de problemas                                                                                                                                                                                                   |
|------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agente no provisionado | Invocación no admitida por parte del <b>SERVICE</b> para tareas en TaskDefinition - <b>'TASK_DEFINITION'</b>       | Esta tarea fue invocada por un <b>SERVICE</b> que no se admite.                                                                                                                                                                               |
|                        | La arquitectura de CPU <b>'TYPE'</b> no es compatible para las tareas de TaskDefinition - <b>'TASK_DEFINITION'</b> | Esta tarea se ejecuta en una arquitectura de CPU no admitida. Para obtener información acerca de las arquitecturas de CPU compatibles, consulte <a href="#">Validación de los requisitos de arquitectura</a> .                                |
|                        | TaskExecutionRole falta en TaskDefinition - <b>'TASK_DEFINITION'</b>                                               | Falta el rol de ejecución de tareas de ECS. Para obtener información sobre cómo proporcionar el rol de ejecución de tareas y los permisos necesarios, consulte <a href="#">Requisitos previos para el acceso a imágenes de contenedores</a> . |

| Tipo de problema | Información adicional                                                                                                                                           | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>Falta la configuración de red “<i>CONFIGURATION_DETA<br/>ILS</i>” para las tareas en TaskDefinition - <i>'TASK_DEFINITION'</i></p>                           | <p>Los problemas de configuración de red pueden surgir debido a la falta de configuración de la VPC, o a la falta de subredes o subredes vacías.</p> <p>Compruebe que la configuración de la red es correcta. Para obtener más información, consulte <a href="#">Requisitos previos para el acceso a imágenes de contenedores</a>.</p> <p>Para obtener más información, consulte <a href="#">Parámetros de definición de tareas de Amazon ECS</a> en la Guía para desarrolladores de Amazon Elastic Container Service.</p> |
|                  | <p>Las tareas iniciadas cuando los clústeres tenían una etiqueta de exclusión se excluyen de Runtime Monitoring. ID de tarea afectada (s): <i>'TASK_ID'</i></p> | <p>Al cambiar la GuardDuty etiqueta predefinida de GuardDutyManaged - true a GuardDutyManaged -false, no GuardDuty recibirá los eventos de tiempo de ejecución de este clúster de Amazon ECS.</p> <p>Actualice la etiqueta a GuardDutyManaged -true y, a continuación, vuelva a iniciar la tarea.</p>                                                                                                                                                                                                                      |

| Tipo de problema | Información adicional                                                                                                                                                              | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>Los tareas implementadas cuando los clústeres tenían una etiqueta de exclusión se excluyen dRuntime Monitoring. Nombre(s) de los servicios afectados: '<b>SERVICE_NAME</b>'</p> | <p>Cuando los servicios se despliegan con la etiqueta de exclusión GuardDuty Managed -false, no GuardDuty recibirán eventos de tiempo de ejecución para este clúster de Amazon ECS.</p> <p>Actualice la etiqueta a GuardDutyManaged -true y, a continuación, vuelva a implementar el servicio.</p> |
|                  | <p>No se incluyen las tareas iniciadas antes de habilitar la configuración automática del agente. ID(s) de tarea afectada: '<b>TASK_ID</b>'</p>                                    | <p>Si el clúster contiene una tarea que se lanzó antes de habilitar la configuración del agente automatizado para Amazon ECS, no GuardDuty podrá protegerla. Vuelva a iniciar la tarea para que la supervise GuardDuty.</p>                                                                        |
|                  | <p>No se incluyen los servicios implementados antes de habilitar la configuración automática del agente. Nombre(s) de los servicios afectados: '<b>SERVICE_NAME</b>'</p>           | <p>Cuando los servicios se implementen antes de habilitar la configuración automática de agentes para Amazon ECS, no GuardDuty recibirán eventos de tiempo de ejecución para los clústeres de ECS.</p>                                                                                             |

| Tipo de problema | Información adicional                                                                                                                                                                                                                                                                                                                                         | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | <p>El servicio <b><i>SERVICE_NAME</i></b> " también requiere una nueva implementación fix/troubleshoot. Consulte la documentación y los nombres de los servicios afectados: <b><i>'SERVICE_NAME'</i></b></p> <p>Las tareas iniciadas antes de habilitar Runtime Monitoring requieren un relanzamiento. ID(s) de tarea afectada: <b><i>'TASK_ID_1'</i></b></p> | <p>No se admite un servicio que se inició antes de habilitar Runtime Monitoring.</p> <p>Puede reiniciar el servicio o actualizarlo con la opción <code>forceNewDeployment</code> según los pasos que se indican en <a href="#">Actualización de un servicio de Amazon ECS mediante la consola</a> en la Guía para desarrolladores de Amazon Elastic Container Service. Como alternativa, también puedes seguir los pasos que se indican <a href="#">UpdateService</a> en la referencia de la API de Amazon Elastic Container Service.</p> <p>Las tareas son inmutables en Amazon ECS. Para evaluar el comportamiento en tiempo de ejecución de una AWS Fargate tarea en ejecución, asegúrese de que la monitorización del tiempo de ejecución ya esté habilitada y, a continuación, reinicie la tarea GuardDuty para añadir el sidecar del contenedor.</p> |



| Tipo de problema | Información adicional                                                                                                                       | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Otros            | <p>Problema no identificado, para tareas en TaskDefinition</p> <ul style="list-style-type: none"> <li>- '<b>TASK_DEFINITION</b>'</li> </ul> | <p>Utilice las siguientes preguntas para identificar la causa raíz del problema:</p> <ul style="list-style-type: none"> <li>• ¿La tarea se inició antes de habilitar la Supervisión en tiempo de ejecución?</li> </ul> <p>Las tareas son inmutables en Amazon ECS. Para evaluar el comportamiento en tiempo de ejecución de una tarea de Fargate en ejecución, asegúrese de que Runtime Monitoring ya esté habilitada y, a continuación, reinicie la tarea GuardDuty para añadir el sidecar del contenedor.</p> <ul style="list-style-type: none"> <li>• ¿Esta tarea forma parte de una implementación de servicios que se inició antes de habilitar la Supervisión en tiempo de ejecución?</li> </ul> <p>En tal caso, puede reiniciar el servicio o actualizarlo con <code>forceNewDeployment</code>. Para ello, siga los pasos indicados en <a href="#">Actualizar un servicio</a>.</p> <p>También puede usar <a href="#">UpdateService</a> o <a href="#">AWS CLI</a></p> |

| Tipo de problema | Información adicional | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  |                       | <ul style="list-style-type: none"> <li>• ¿La tarea se lanzó después de excluir el clúster de ECS de la Supervisión en tiempo de ejecución?</li> </ul> <p>Si cambias la GuardDuty etiqueta predefinida de GuardDutyManaged - true a GuardDuty Managed -false, no GuardDuty recibirá los eventos de tiempo de ejecución del clúster de ECS.</p> <ul style="list-style-type: none"> <li>• ¿El servicio contiene una tarea que tiene un formato antiguo de taskArn?</li> </ul> <p>GuardDuty Runtime Monitoring no admite la cobertura de tareas que tienen el formato anterior de taskArn.</p> <p>Para obtener información sobre los nombres de recursos de Amazon (ARN) para los recursos de Amazon ECS, consulte <a href="#">Nombres de recursos de Amazon (ARN) e ID</a>.</p> |

# Cobertura en tiempo de ejecución y resolución de problemas para clústeres de Amazon EKS

Tras activar Runtime Monitoring e instalar el agente de GuardDuty seguridad (complemento) para EKS de forma manual o mediante una configuración automática del agente, podrá empezar a evaluar la cobertura de sus clústeres de EKS.

## Contenido

- [Revisión de las estadísticas de cobertura](#)
- [El estado de la cobertura cambia con EventBridge notificaciones](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#)

## Revisión de las estadísticas de cobertura

Las estadísticas de cobertura de los clústeres de EKS asociados a sus propias cuentas o a las de sus miembros representan el porcentaje de los clústeres de EKS en buen estado con respecto a todos los clústeres de EKS de la Región de AWS seleccionada. La siguiente ecuación lo representa de la siguiente manera:

$$(\text{clusters/All Clústeres en buen estado}) * 100$$

Elija uno de los métodos de acceso para revisar las estadísticas de cobertura de sus cuentas.

## Console

- Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
- En el panel de navegación, elija Supervisión en tiempo de ejecución.
- Seleccione la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS.
- En la pestaña Cobertura del tiempo de ejecución de los clústeres de EKS, puede ver las estadísticas de cobertura agregadas por el estado de cobertura que está disponible en la tabla Lista de clústeres.
  - Puede filtrar la tabla Lista de clústeres por las siguientes columnas:
    - Cluster name (Nombre del clúster)
    - ID de cuenta
    - Tipo de administración del agente

- Estado de la cobertura
- Add-on versión
- Si el valor de Estado de la cobertura de alguno de sus clústeres de EKS es En mal estado, en la columna Problema se puede incluir información adicional sobre el motivo del estado En mal estado.

## API/CLI

- Ejecute la [ListCoverage](#) API con su propio ID de detector, región y punto de conexión de servicio válidos. Puede filtrar y ordenar la lista de clústeres con esta API.
- Puede cambiar el ejemplo de `filter-criteria` con una de las siguientes opciones para `CriterionKey`:
  - ACCOUNT\_ID
  - CLUSTER\_NAME
  - RESOURCE\_TYPE
  - COVERAGE\_STATUS
  - ADDON\_VERSION
  - MANAGEMENT\_TYPE
- Puede cambiar el ejemplo de `AttributeName` en `sort-criteria` con las siguientes opciones:
  - ACCOUNT\_ID
  - CLUSTER\_NAME
  - COVERAGE\_STATUS
  - ISSUE
  - ADDON\_VERSION
  - UPDATED\_AT
- Puedes cambiarlos *max-results* (hasta 50).
- Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty --region us-east-1 list-coverage --detector-
```

```
Id 12abc34d567e87a901bc2d34e56789f0 --sort-criteria '{"AttributeName":
```

```
"EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
'{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}]}] }' --max-results 5
```

- Ejecute la [GetCoverageStatistics](#) API para recuperar las estadísticas agregadas de cobertura en función de `statisticsType`.
- Puede cambiar el ejemplo de `statisticsType` a una de las siguientes opciones:
  - `COUNT_BY_COVERAGE_STATUS`: representa las estadísticas de cobertura de los clústeres de EKS agregadas por estado de cobertura.
  - `COUNT_BY_RESOURCE_TYPE`— Estadísticas de cobertura agregadas en función del tipo de AWS recurso de la lista.
- Puede cambiar el ejemplo de `filter-criteria` en el comando. Puede usar las siguientes opciones para `CriterionKey`:
  - `ACCOUNT_ID`
  - `CLUSTER_NAME`
  - `RESOURCE_TYPE`
  - `COVERAGE_STATUS`
  - `ADDON_VERSION`
  - `MANAGEMENT_TYPE`
- Para encontrar las `detectorId` correspondientes a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-id
12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
--filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
"FilterCondition":{"EqualsValue":"123456789012"}]}] }'
```

Si el estado de cobertura de su clúster de EKS es En mal estado, consulte [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#).

## El estado de la cobertura cambia con EventBridge notificaciones

El estado de cobertura de un clúster de EKS de su cuenta puede aparecer como En mal estado. Para detectar cuándo el estado de cobertura pasa a ser En mal estado, le recomendamos que supervise el estado de cobertura periódicamente y que solucione los problemas si el estado es

En mal estado. Como alternativa, puedes crear una EventBridge regla de Amazon que te notifique cuando el estado de la cobertura cambie de Unhealthy a Healthy o no. De forma predeterminada, la GuardDuty publica en el [EventBridge bus](#) de tu cuenta.

### Ejemplo de esquema de notificaciones

Como EventBridge regla general, puede utilizar los ejemplos de eventos y patrones de eventos predefinidos para recibir la notificación del estado de la cobertura. Para obtener más información sobre cómo crear una EventBridge regla, consulta [Crear regla](#) en la Guía del EventBridge usuario de Amazon.

Además, puede crear un patrón de eventos personalizado mediante el siguiente ejemplo de esquema de notificaciones. Asegúrese de sustituir los valores de su cuenta. Para recibir una notificación cuando el estado de cobertura de su clúster de Amazon EKS cambie de Healthy a Unhealthy, detail-type debería ser así *GuardDuty Runtime Protection Unhealthy*. Para recibir una notificación cuando el estado de la cobertura cambie de Unhealthy a Healthy, sustituya el valor detail-type de por *GuardDuty Runtime Protection Healthy*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Cuenta de AWS ID",
  "time": "event timestamp (string)",
  "region": "Región de AWS",
  "resources": [
    ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
      "resourceType": "EKS",
      "eksClusterDetails": {
        "clusterName": "string",
        "availableNodes": "string",
        "desiredNodes": "string",
        "addonVersion": "string"
      }
    }
  },
}
```

```

    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}

```

## Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS

Si el estado de cobertura de su clúster EKS es `Unhealthy`, puede ver el error correspondiente en la columna Problema de la GuardDuty consola o utilizando el tipo de [CoverageResource](#) datos.

Cuando trabaje con etiquetas de inclusión o exclusión para supervisar los clústeres de EKS de forma selectiva, es posible que las etiquetas tarden algún tiempo en sincronizarse. Esto puede afectar al estado de cobertura del clúster de EKS asociado. Puede intentar eliminar y volver a agregar la etiqueta correspondiente (inclusión o exclusión). Para obtener más información, consulte [Etiquetado de los recursos de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

La estructura de un problema de cobertura es `Issue type:Extra information`. Por lo general, los problemas tienen información adicional opcional que puede incluir una excepción específica del cliente o una descripción del problema. Con base en la Información adicional, las siguientes tablas indican los pasos recomendados para solucionar los problemas de cobertura de los clústeres de EKS.

| Tipo de problema (prefijo)                  | Información adicional                                                                                                                                             | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error al crear el complemento | El complemento no <code>aws-guardduty-agent</code> es compatible con la versión actual del clúster <i>ClusterName</i> . No se admite el complemento especificado. | Asegúrese de utilizar una de esas versiones de Kubernetes que admiten la implementación del complemento de EKS <code>aws-guardduty-agent</code> . Para obtener más información, consulte <a href="#">Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty</a> . Para obtener información sobre cómo actualizar su versión de Kubernetes, consulte |

| Tipo de problema (prefijo)                                                                                                                          | Información adicional                                                                               | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                     |                                                                                                     | <a href="#">Actualización de una versión de Kubernetes de clúster de Amazon EKS.</a>                                                                                                                                                                                                                                                                                                                   |
| <p>Se produjo un error al crear el complemento</p> <p>Se produjo un error al actualizar el complemento</p> <p>El complemento está en mal estado</p> | <p>Problema con el complemento de EKS: AddonIssueCode : AddonIssueMessage</p>                       | <p>Para obtener información sobre los pasos recomendados para un código de problema de complemento específico, consulte <a href="#">Troubleshooting steps for Addon creation/updatation error with Addon issue code</a>.</p> <p>Para obtener una lista de los códigos de problemas relacionados con los complementos que podrían producirse en este problema, consulte. <a href="#">AddonIssue</a></p> |
| <p>Se produjo un error al crear el punto de conexión de VPC</p>                                                                                     | <p>La creación de puntos de conexión de VPC no es compatible con la VPC compartida <i>vpcId</i></p> | <p>La Supervisión en tiempo de ejecución ahora admite el uso de una VPC compartida dentro de una organización. Asegúrese de que las cuentas cumplen todos los requisitos previos. Para obtener más información, consulte <a href="#">Requisitos previos para utilizar una VPC compartida</a>.</p>                                                                                                      |



| Tipo de problema (prefijo) | Información adicional                                                                                                                                                                                                                                                                               | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <p>Solo cuando se utiliza una VPC compartida con una configuración automatizada del agente</p> <p>El ID de cuenta propietario <b>111122223333</b> de la VPC compartida <b>vpcId</b> no tiene habilitada la supervisión del tiempo de ejecución, la configuración automática de agentes o ambas.</p> | <p>La cuenta de propietario de la VPC compartida debe habilitar la Supervisión en tiempo de ejecución y la configuración automatizada del agente para al menos un tipo de recurso (Amazon EKS o Amazon ECS [AWS Fargate]). Para obtener más información, consulte <a href="#">Requisitos previos específicos de la supervisión del GuardDuty tiempo de ejecución</a>.</p>                                                                                                                                                                                                                               |
|                            | <p>Para habilitar el DNS privado, es necesario establecer ambos <code>enableDnsSupport</code> atributos de <code>enableDnsHostnames</code> VPC en <code>true</code> for <b>vpcId</b> (servicio: Ec2, estado Code:400, ID de solicitud:). <b>a1b2c3d4-5678-90ab-cdef-EXAMPLE11111</b></p>            | <p>Asegúrese de que los siguientes atributos de VPC estén establecidos en <code>true</code> - <code>enableDnsSupport</code> y <code>enableDnsHostnames</code> . Para obtener más información, consulte <a href="#">Atributos DNS para la VPC</a>.</p> <p>Si utiliza Amazon VPC Console <a href="https://console.aws.amazon.com/vpc/">https://console.aws.amazon.com/vpc/</a> para crear la Amazon VPC, asegúrese de seleccionar <code>Enable DNS hostnames</code> y <code>Enable DNS resolution</code>. Para obtener más información, consulte <a href="#">Opciones de configuración de la VPC</a>.</p> |

| Tipo de problema (prefijo)                                                | Información adicional                                                                                                                                                                       | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se produjo un error al eliminar el punto de conexión de la VPC compartida | No se permite eliminar el punto final de la VPC compartida para el ID de cuenta <b>111122223333</b> , la VPC <b>vpcId</b> compartida o el ID de cuenta del propietario. <b>555555555555</b> | <p>Medidas posibles:</p> <ul style="list-style-type: none"> <li>Al desactivar el estado de la Supervisión en tiempo de ejecución de la cuenta de participante de la VPC compartida, no se afecta a la política de punto de conexión de VPC compartida ni al grupo de seguridad que existe en la cuenta de propietario.</li> </ul> <p>Para eliminar el punto de conexión de VPC compartida y el grupo de seguridad, debe desactivar la Supervisión en tiempo de ejecución o el estado de la configuración automatizada del agente en la cuenta de propietario de la VPC compartida.</p> <ul style="list-style-type: none"> <li>La cuenta participante de la VPC compartida no puede eliminar el punto de conexión de la VPC compartida ni el grupo de seguridad alojados en la cuenta propietaria de la VPC compartida.</li> </ul> |

| Tipo de problema (prefijo)                                                                              | Información adicional                                                       | Pasos recomendados de solución de problemas                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Clústeres de EKS locales                                                                                | Los complementos de EKS no se admiten en los clústeres de Outposts locales. | <p>No se puede procesar.</p> <p>Para obtener más información, consulte <a href="#">Amazon EKS on AWS outposts</a>.</p>                                                                                                                                                                                                                                                  |
| No se ha concedido el permiso de habilitación de la supervisión en tiempo de ejecución de EKS           | (puede o no mostrar información adicional)                                  | <ol style="list-style-type: none"> <li>1. Si hay información adicional disponible sobre este problema, corrija la causa raíz y avance al siguiente paso.</li> <li>2. Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla. Asegúrese de que el GuardDuty agente también se despliegue, ya sea de forma automática GuardDuty o manual.</li> </ol> |
| Aprovisionamiento de recursos de habilitación de la supervisión en tiempo de ejecución de EKS en curso. | (puede o no mostrar información adicional)                                  | <p>No se puede procesar.</p> <p>Después de habilitar la supervisión en tiempo de ejecución de EKS, el estado de cobertura puede seguir siendo <code>Unhealthy</code> hasta que se complete el paso de aprovisionamiento de recursos. El estado de cobertura se supervisa y actualiza periódicamente.</p>                                                                |

| Tipo de problema (prefijo)      | Información adicional                    | Pasos recomendados de solución de problemas                                                                                                                                      |
|---------------------------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Otros (cualquier otro problema) | Error debido a una falla de autorización | Desactive la supervisión en tiempo de ejecución de EKS y vuelva a activarla. Asegúrese de que el GuardDuty agente también se despliegue, de forma automática GuardDuty o manual. |

### Pasos para solucionar un error de Addon con creation/updation el código de error del Addon

| Error de creación o actualización del complemento                                                                                                                                | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento EKS</p> <p><code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque no tiene la cantidad deseada de réplicas.</p> | <ul style="list-style-type: none"> <li>Con el mensaje del problema, puede identificar y solucionar la causa raíz. Puede comenzar por describir el clúster. Por ejemplo, utilice <a href="#">kubectl describe pods</a> para identificar la causa raíz del fallo de un pod.</li> </ul> <p>Después de solucionar la causa raíz, vuelva a intentar el paso (creación o actualización del complemento).</p> <ul style="list-style-type: none"> <li>Si el problema persiste, compruebe que el punto de conexión de VPC para el clúster de Amazon EKS está configurado correctamente. Para obtener más información, consulte <a href="#">Validar la configuración del punto de conexión de VPC</a>.</li> </ul> |
| <p>Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el</p>                                                                                          | <p>Para resolver este problema, puede seguir uno de estos pasos:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Error de creación o actualización del complemento                                                                                                                                                                                                                    | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: x Insufficient cpu. preemption: not eligible due to preemptionPolicy=Never .</p>                                                                        | <ul style="list-style-type: none"> <li>• Actualice la prioridad del pod del GuardDuty agente: <a href="#">Parámetros y valores que se pueden configurar</a> configurando cualquiera de las opciones que admiten el preemptionPolicy valor como. PriorityClass PreemptLowerPriority Para obtener más información sobre la prioridad de los pods, consulte <a href="#">Prioridad y preferencia de pods</a> en la Documentación de Kubernetes.</li> <li>• Escale verticalmente la instancia: para administrar sus recursos y realizar una selección óptima de instancias, consulte <a href="#">Administrar los recursos informáticos mediante nodos</a> y <a href="#">Elegir un tipo de instancia de nodo óptimo de Amazon EC2</a> en la Guía del usuario de Amazon EKS.</li> </ul> |
| <p>Problema con el complemento EKS - InsufficientNumberOfReplicas : el complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: x Too many pods. preemption: not eligible due to preemptionPolicy=Never .</p>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>Problema con el complemento EKS - InsufficientNumberOfReplicas : el complemento no está en buen estado porque uno o más pods no están programados. Hay 0/x nodos disponibles: 1 Insufficient memory. preemption: not eligible due to preemptionPolicy=Never .</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

 Note

El mensaje se muestra o/x GuardDuty porque solo muestra el primer error encontrado. El número real de pods en ejecución en el GuardDuty daemonset puede ser superior a 0.

| Error de creación o actualización del complemento                                                                                                                                                                       | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods tienen contenedores <code>CrashLoopBackOff: Completed</code> en espera</p> | <p>Puede ver los registros asociados al pod e identificar el problema. Para obtener información sobre cómo hacerlo, consulte <a href="#">Depurar pods en ejecución</a> en la Documentación de Kubernetes.</p> <p>Use la siguiente lista de verificación para solucionar el problema de este complemento:</p> <ul style="list-style-type: none"><li>• Valide que el monitoreo del tiempo de ejecución esté habilitado.</li><li>• Valide que se cumple <a href="#">Requisitos previos para la compatibilidad con clústeres de Amazon EKS</a>, como las distribuciones de sistema operativo verificadas y las versiones de Kubernetes compatibles.</li><li>• Si administra el agente de seguridad de manera manual, confirme que ha creado un punto de conexión de VPC para todas las VPC. Al habilitar la configuración GuardDuty automatizada, aún debe validar que se haya creado el punto final de la VPC. Por ejemplo, cuando se utiliza una VPC compartida en una configuración automática.</li></ul> <p>Para validar esto, consulte <a href="#">Validar la configuración del punto de conexión de VPC</a>.</p> <ul style="list-style-type: none"><li>• Confirme que el agente GuardDuty de seguridad puede resolver el DNS privado del punto final de la GuardDuty VPC. Para conocer los puntos de conexión, consulte Nombres de DNS privados de los puntos de</li></ul> |

| Error de creación o actualización del complemento | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | <p>conexión en <a href="#">Administrar agentes GuardDuty de seguridad</a>.</p> <p>Para ello, puede utilizar cualquier herramienta nslookup en Windows o Mac o la herramienta dig en Linux. Al usar nslookup, puede usar el siguiente comando después de reemplazar la región por la <i>us-west-2</i> suya:</p> <div data-bbox="862 779 1507 898"><pre>nslookup guardduty-data. <i>us-west-2</i>.amazonaws.com</pre></div> <ul style="list-style-type: none"><li>• Valide que su política de puntos finales de GuardDuty VPC o la política de control de servicios no guardduty:SendSecurityTelemetry afecten a la acción.</li></ul> |

| Error de creación o actualización del complemento                                                                                                                                                                   | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento EKS - <code>InsufficientNumberOfReplicas</code> : el complemento no está en buen estado porque uno o más pods tienen contenedores <code>CrashLoopBackOff: Error</code> en espera</p> | <p>Puede ver los registros asociados al pod e identificar el problema. Para obtener información sobre cómo hacerlo, consulte <a href="#">Depurar pods en ejecución</a> en la Documentación de Kubernetes.</p> <p>Una vez que se haya identificado el problema, use la siguiente lista de verificación para solucionarlo:</p> <ul style="list-style-type: none"><li>• Valide que el monitoreo del tiempo de ejecución esté habilitado.</li><li>• Valide que se cumple <a href="#">Requisitos previos para la compatibilidad con clústeres de Amazon EKS</a>, como las distribuciones de sistema operativo verificadas y las versiones de Kubernetes compatibles.</li><li>• El agente GuardDuty de seguridad puede resolver el DNS privado del punto final de la GuardDuty VPC. Para conocer los puntos de conexión, consulte Nombres de DNS privados de los puntos de conexión en <a href="#">Administrar agentes GuardDuty de seguridad</a>.</li></ul> |



| Error de creación o actualización del complemento                                                                                                                                                                                                                                                                | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento de EKS:</p> <pre>AdmissionRequestDenied : "validate .kyverno.svc-fail" de webhook de admisión denegó la solicitud: política DaemonSet/amazon-guardduty/aws- guardduty-agent para infracción de recursos: restrict-image-registries: autogen-v alidate-registries :...</pre>       | <ol style="list-style-type: none"><li>1. El clúster de Amazon EKS o el administrador de seguridad deben revisar la política de seguridad que bloquea la actualización del complemento.</li><li>2. Debe desactivar el controlador (webhook) o hacer que el controlador acepte las solicitudes de Amazon EKS.</li></ol>                                                                                                           |
| <p>Problema con el complemento de EKS:</p> <pre>ConfigurationConflict : se encontrar on conflictos al intentar la aplicación. No continuará debido al modo de resolución de conflictos. Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.tem plate.spec.containers[name= "aws-guardduty-agent"].image</pre> | <p>Al crear o actualizar el complemento, indique la marca de resolución de conflictos <code>OVERWRITE</code>. Esto sobrescribirá potencialmente cualquier cambio que se haya realizado directamente en los recursos relacionados en Kubernetes a través de la API de Kubernetes.</p> <p>En primer lugar, se puede <a href="#">Quitar un complemento de Amazon EKS de un clúster</a> y, a continuación, volver a instalarlo.</p> |

| Error de creación o actualización del complemento                                                                                                                                                                                                                                | Pasos para la solución de problemas                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento de EKS:</p> <pre>AccessDenied: priorityclasses.scheduling.k8s.io "aws-guarddduty-agent.priorityclass" is forbidden : User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope</pre> | <p>Debe agregar el permiso que falta al <code>eks:addon-cluster-admin ClusterRoleBinding</code> manualmente. Agregue el siguiente <code>yaml</code> al <code>eks:addon-cluster-admin</code> :</p> <pre>--- kind: ClusterRoleBinding apiVersion: rbac.authorization.k8s.io/v1 metadata:   name: eks:addon-cluster-admin subjects: - kind: User   name: eks:addon-manager   apiGroup: rbac.authorization.k8s.io roleRef:   kind: ClusterRole   name: cluster-admin   apiGroup: rbac.authorization.k8s.io ---</pre> |
| <pre>AddonUpdationFailed: EKSAaddonIssue - AccessDenied: namespaces\"amazon-guarddduty\"isforbidden:User\"eks:addon-manager\"cannotpatchresource\"namespaces\"inAPIgroup\"\"inthenamespace\"amazon-guarddduty\"</pre>                                                            | <p>Ahora puede aplicar este <code>yaml</code> al clúster de Amazon EKS mediante el siguiente comando:</p> <pre>kubectl apply -f eks-addon-cluster-admin.yaml</pre>                                                                                                                                                                                                                                                                                                                                               |

| Error de creación o actualización del complemento                                                                                                                                                                                          | Pasos para la solución de problemas                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Problema con el complemento de EKS:</p> <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must- have-label-owner] All namespaces must have an `owner` label</pre>                      | <p>Debe desactivar el controlador o hacer que este acepte las solicitudes del clúster de Amazon EKS.</p> <p>Antes de crear o actualizar el complemento, también puedes crear un espacio de GuardDuty nombres y etiquetarlo como. owner</p>                                     |
| <p>Problema con el complemento de EKS:</p> <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must- have-label-owner] All namespaces must have an `owner` label</pre>                      | <p>Debe desactivar el controlador o hacer que este acepte las solicitudes del clúster de Amazon EKS.</p> <p>Antes de crear o actualizar el complemento, también puedes crear un espacio de GuardDuty nombres y etiquetarlo como. owner</p>                                     |
| <p>Problema con el complemento de EKS:</p> <pre>AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [allowed-container- registries] container &lt;aws-guar- dduty-agent&gt; has an invalid image registry</pre> | <p>Añade el registro de imágenes GuardDuty a tu controlador allowed-container-registries de admisión. Para obtener más información, consulte el repositorio ECR para EKS v1.8.1-eks-build.2 en <a href="#">Agente de alojamiento GuardDuty de repositorios Amazon ECR</a>.</p> |

## Configuración de la supervisión de la CPU y la memoria

Después de habilitar la Supervisión en tiempo de ejecución y evaluar que la cobertura del clúster esté en buen estado, podrá configurar y ver las métricas de Información.

Los siguientes temas pueden ayudarle a evaluar el rendimiento del agente desplegado en relación con los límites de CPU y memoria del GuardDuty agente.

## Configurar la supervisión en el clúster de Amazon ECS

Los siguientes pasos de la Guía del CloudWatch usuario de Amazon pueden ayudarle a evaluar el rendimiento del agente desplegado en comparación con los límites de CPU y memoria del GuardDuty agente:

1. [Configurar Información de contenedores en Amazon ECS para métricas a nivel de clúster y de servicio](#)
2. [Métricas de Información de contenedores de Amazon ECS](#)

## Configurar la supervisión en el clúster de Amazon EKS

Una vez que se haya desplegado el agente de GuardDuty seguridad y hayas evaluado que el estado de cobertura del clúster es correcto, podrás configurar y ver las métricas de Container Insight.

Evalúe el rendimiento del agente de seguridad

1. [Configuración de Container Insights en Amazon EKS y Kubernetes en la Guía](#) del usuario de Amazon CloudWatch
2. [Métricas de Amazon EKS y Kubernetes Container Insights en la Guía](#) del usuario de Amazon CloudWatch

Administrar el rendimiento con la versión 1.5.0 o superior del agente de seguridad

Con el agente de seguridad [v1.5.0 y versiones posteriores](#), cuando los datos indican que el GuardDuty agente asociado está alcanzando los límites asignados, puede configurar parámetros específicos. Para obtener más información, consulte [Configurar los parámetros del complemento de EKS](#).

## Uso de VPC compartida con Runtime Monitoring

GuardDuty Runtime Monitoring admite el uso de Amazon Virtual Private Cloud (Amazon VPC) compartida para usted Cuentas de AWS que pertenezca a la misma organización. AWS Organizations Se puede usar la VPC compartida de dos maneras:

- Configuración automática del agente (recomendada): cuando gestione GuardDuty automáticamente el agente de seguridad, también configurará la política de puntos finales de Amazon VPC. Esta política se basa en la configuración de VPC compartida de su organización.

Se debe habilitar la configuración automática del agente en la cuenta del propietario de la VPC compartida y en todas las cuentas participantes que compartirán esta VPC.

- Agente administrado de manera manual: al administrar de manera manual el agente de seguridad con una VPC compartida, debe actualizar la política de puntos de conexión de VPC para permitir que las cuentas correspondientes accedan a la VPC compartida. Para ello, se puede usar el ejemplo de política que se comparte en la siguiente sección [Funcionamiento](#).

En los escenarios de administración manual que involucran cuentas participantes para una VPC compartida, es posible que el estado de la cobertura no sea exacto. Para garantizar un estado actualizado de protección y cobertura de sus recursos, GuardDuty recomienda habilitar la configuración automática de agentes para todas las cuentas que utilizarán una VPC compartida.

## Temas

- [Funcionamiento](#)
- [Requisitos previos para utilizar una VPC compartida](#)

## Funcionamiento

Las Cuentas de AWS que pertenezcan a la misma organización que la cuenta de propietario de Amazon VPC compartida también pueden compartir el mismo punto de enlace de Amazon VPC. Cada una de las cuentas que utilizan la misma política de puntos de conexión de Amazon VPC se denomina AWS cuenta participante de la Amazon VPC compartida asociada.

El siguiente ejemplo muestra la política de punto de conexión de VPC predeterminada de la cuenta de propietario de la VPC compartida y la cuenta participante. `aws:PrincipalOrgID` mostrará el ID de la organización asociado al recurso de la VPC compartida. El uso de esta política se limita a las cuentas participantes presentes en la organización de la cuenta de propietario.

Example Ejemplo de política de punto de conexión de VPC compartida

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "*",
```

```
        "Resource": "*",
        "Effect": "Allow",
        "Principal": "*"
    },
    {
        "Condition": {
            "StringNotEquals": {
                "aws:PrincipalOrgID": "o-abcdef0123"
            }
        },
        "Action": "*",
        "Resource": "*",
        "Effect": "Deny",
        "Principal": "*"
    }
]
```

## Con configuración GuardDuty automática de agentes

Cuando la cuenta de propietario de la VPC compartida habilita la supervisión del tiempo de ejecución y la configuración automática de los agentes para cualquiera de los recursos (Amazon EKS o (solo AWS Fargate Amazon ECS)), todas las VPC compartidas pueden instalarse automáticamente en el punto de enlace de Amazon VPC compartido y el grupo de seguridad asociado en la cuenta de propietario de la VPC compartida. GuardDuty recupera el ID de la organización que está asociado a la Amazon VPC compartida.

GuardDuty crea un punto de enlace de Amazon VPC cuando la cuenta del propietario de la VPC compartida o la cuenta participante lo necesitan. Algunos ejemplos de cómo se necesita un punto de conexión de Amazon VPC son la activación GuardDuty, la supervisión del tiempo de ejecución, la supervisión del tiempo de ejecución de EKS o el lanzamiento de una nueva tarea de Amazon ECS-Fargate . Cuando estas cuentas habilitan Runtime Monitoring y la configuración automática de agentes para cualquier tipo de recurso, GuardDuty crea un punto de enlace de Amazon VPC y establece la política de puntos de enlace con el mismo ID de organización que el de la cuenta de propietario de la VPC compartida. GuardDuty añade una `GuardDutyManaged` etiqueta y la establece `true` para el punto de enlace de Amazon VPC que GuardDuty crea. Si la cuenta de propietario de Amazon VPC compartida no ha habilitado la monitorización del tiempo de ejecución o la configuración automática de agentes para ninguno de los recursos, no GuardDuty establecerá la política de puntos de conexión de Amazon VPC. Para obtener información sobre cómo configurar

la Supervisión en tiempo de ejecución y administrar el agente de seguridad automáticamente en la cuenta de propietario de la VPC compartida, consulte [¿Habilitar la GuardDuty supervisión del tiempo.](#)

Se utiliza con un agente administrado de manera manual

Cuando utilice una VPC compartida con un agente administrado de manera manual, compruebe que no haya una política de punto de conexión Deny explícita que bloquee una cuenta que necesite usar la VPC compartida. Esto impedirá que el agente de seguridad envíe datos telemétricos a GuardDuty, lo que generará un estado de cobertura. Unhealthy Para configurar la política de puntos de conexión, consulte [Example shared VPC endpoint policy](#).

Es posible que la cobertura del tiempo de ejecución no sea precisa en situaciones como la falta de permisos para la VPC compartida. Puede monitorear de forma continua la cobertura de los recursos siguiendo los pasos correspondientes al tipo de recurso indicado [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para garantizar la protección continua de sus recursos informáticos con Runtime Monitoring, le GuardDuty recomienda habilitar la configuración automática de agentes para la cuenta propietaria de la VPC compartida y todas las cuentas participantes de sus recursos.

## Requisitos previos para utilizar una VPC compartida

Como parte de la configuración inicial, lleve a cabo los siguientes pasos en la Cuenta de AWS que desee que sea el propietario de la VPC compartida:

1. Crear una organización: para crear una organización, siga los pasos que se indican en [Crear y administrar una organización](#) en la Guía del usuario de AWS Organizations .

Para obtener información sobre cómo añadir o eliminar cuentas de miembros, consulte [Administrar Cuentas de AWS en su organización](#).

2. Crear un recurso de VPC compartida: puede crear un recurso de VPC compartida desde la cuenta de propietario. Para obtener más información, consulte [Compartir las subredes de VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

## Requisitos previos específicos de la supervisión del GuardDuty tiempo de ejecución

La siguiente lista proporciona los requisitos previos específicos de: GuardDuty

- La cuenta de propietario de la VPC compartida y la cuenta participante pueden ser de diferentes organizaciones en. GuardDuty Sin embargo, deben pertenecer a la misma organización en AWS

Organizations. Esto es necesario GuardDuty para crear un punto de enlace de Amazon VPC y un grupo de seguridad para la VPC compartida. Para obtener información sobre cómo funcionan las VPC compartidas, consulte [Compartir la VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

- Habilite Runtime Monitoring o EKS Runtime Monitoring y GuardDuty automatice la configuración de agentes para cualquier recurso de la cuenta de propietario de la VPC compartida y de la cuenta de participante. Para obtener más información, consulte [Habilitación de la supervisión en tiempo de ejecución](#).

Si ya ha completado estas configuraciones, continúe con el siguiente paso.

- Cuando trabaje con una tarea de Amazon EKS o una de Amazon ECS (AWS Fargate únicamente), asegúrese de elegir el recurso de VPC compartido asociado a la cuenta del propietario y de seleccionar sus subredes.

## Uso de la infraestructura como código (IaC) con GuardDuty agentes de seguridad automatizados

Utilice esta sección únicamente si la siguiente lista se aplica a su caso de uso:

- Utiliza herramientas de infraestructura como código (IaC), como Terraform, para administrar sus AWS recursos, AWS Cloud Development Kit (AWS CDK) y
- Debe habilitar la configuración GuardDuty automática de agentes para uno o más tipos de recursos: Amazon EKS, Amazon EC2 o Amazon. ECS-Fargate

## Información general sobre el gráfico de dependencia de recursos de IaC

Al habilitar la configuración GuardDuty automática de agentes para un tipo de recurso, crea GuardDuty automáticamente un punto de enlace de VPC y un grupo de seguridad asociados a este punto de enlace de VPC e instala el agente de seguridad para este tipo de recurso. De forma predeterminada, GuardDuty eliminará el punto final de la VPC y el grupo de seguridad asociado solo después de deshabilitar Runtime Monitoring. Para obtener más información, consulte [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#).

Cuando utiliza una herramienta de IaC, esta mantiene un gráfico de dependencia de los recursos. Cuando se eliminan recursos con la herramienta de IaC, únicamente se eliminan los recursos de los que se puede hacer un seguimiento como parte del gráfico de dependencia de recursos. Es posible



que las herramientas de IaC no tengan conocimiento de los recursos que se crean fuera de su configuración especificada. Por ejemplo, crea una VPC con una herramienta IaC y, a continuación, agrega un grupo de seguridad a esta VPC mediante una AWS consola o una operación de API. En el gráfico de dependencias de recursos, el recurso de la VPC que crea dependerá del grupo de seguridad asociado. Si elimina este recurso de la VPC con la herramienta de IaC, se producirá un error. La forma de evitar este error es eliminar manualmente el grupo de seguridad asociado o actualizar la configuración de IaC para incluir este recurso agregado.

## Problema común: eliminar recursos en IaC

Al utilizar la configuración de agentes GuardDuty automatizada, es posible que desee eliminar un recurso (Amazon EKS, Amazon EC2 o Amazon ECS-Fargate) que haya creado mediante una herramienta de IaC. Sin embargo, este recurso depende del punto final de la VPC que GuardDuty haya creado. Esto impide que la herramienta IaC elimine el recurso por sí misma y requiere que desactive la Supervisión en tiempo de ejecución, que además elimina el punto de conexión de VPC automáticamente.

Por ejemplo, cuando intentes eliminar el punto de enlace de la VPC que GuardDuty se creó en tu nombre, aparecerá un error similar al de los ejemplos siguientes.

### Example

#### Ejemplo de error al usar CDK

The following resource(s) failed to delete:

```
[mycdkvpccapplicationpublicsubnet1Subnet1SubnetEXAMPLE1, mycdkvpccapplicationprivatesubnet1Subnet1SubnetEXAMPLE1]
Resource handler returned message: "The subnet 'subnet-APKAEIVFHP46CEXAMPLE' has
dependencies and cannot be deleted. (Service: Ec2, Status Code: 400, Request
ID: e071c3c5-7442-4489-838c-0dfc6EXAMPLE)" (RequestToken: 4381cff8-6240-208a-8357-5557b7EXAMPLE)
HandlerErrorCode: InvalidRequest)
```

### Example

#### Ejemplo de error al usar Terraform

```
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
19m50s elapsed]
module.vpc.aws_subnet.private[1]: Still destroying... [id=subnet-APKAEIVFHP46CEXAMPLE,
20m0s elapsed]
```

```
Error: deleting EC2 Subnet (subnet-APKAEIBAERJR2EXAMPLE): DependencyViolation: The
  subnet 'subnet-APKAEIBAERJR2EXAMPLE' has dependencies and cannot be deleted.
  status code: 400, request id: e071c3c5-7442-4489-838c-0dfc6EXAMPLE
```

## Solución: evite el problema de eliminación de recursos

Esta sección le ayuda a administrar el punto final de la VPC y el grupo de seguridad de forma independiente de GuardDuty.

Para adquirir la propiedad completa de los recursos configurados mediante la herramienta de laC, siga los siguientes pasos en el orden indicado:

1. Cree una VPC. Para permitir el permiso de entrada, asocie un punto final de GuardDuty VPC al grupo de seguridad a esta VPC.
2. Habilite la configuración GuardDuty automática de agentes para su tipo de recurso.

Tras completar los pasos anteriores, no GuardDuty creará su propio punto final de VPC y reutilizará el que creó con la herramienta laC.

Para obtener información sobre cómo crear una VPC propia, consulte [Crear una VPC únicamente](#) en las Puertas de enlace de tránsito de Amazon VPC. Para obtener información sobre cómo crear un punto de conexión de VPC, consulte la siguiente sección para el tipo de recurso:

- Para Amazon EC2, consulte [Requisito previo: crear manualmente el punto de conexión de Amazon VPC](#).
- Para Amazon EKS, consulte [Requisito previo: crear un punto de conexión de Amazon VPC](#).

## Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty

El agente GuardDuty de seguridad recopila los siguientes tipos de eventos y los envía al GuardDuty backend para detectar y analizar las amenazas. GuardDuty no hace que estos eventos sean accesibles para usted. Si GuardDuty detecta una amenaza potencial y genera una [Tipos de resultados de la supervisión en tiempo de ejecución](#), puede ver los detalles del hallazgo correspondiente.

Para obtener información sobre cómo se GuardDuty utilizan los tipos de eventos recopilados en Runtime Monitoring, consulte [Desactivación del uso de los datos para mejorar el servicio](#).

## Eventos de procesos

Los eventos de los procesos representan información asociada a los procesos que se ejecutan en las instancias de Amazon EC2 y las cargas de trabajo de contenedores. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de los procesos que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                  | Description (Descripción)                                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process name (Nombre del proceso) | Nombre del proceso observado.                                                                                                                                                                                               |
| Ruta de proceso                   | Ruta absoluta del ejecutable del proceso.                                                                                                                                                                                   |
| ID de proceso                     | ID asignado al proceso por el sistema operativo .                                                                                                                                                                           |
| PID de espacio de nombres         | ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID de nivel de host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor. |
| ID de usuario del proceso         | ID único del usuario que ha ejecutado el proceso.                                                                                                                                                                           |
| UUID de proceso                   | El identificador único asignado al proceso por GuardDuty.                                                                                                                                                                   |
| GID de proceso                    | ID del proceso del grupo de procesos.                                                                                                                                                                                       |
| EGID de proceso                   | ID del grupo efectivo del grupo de procesos.                                                                                                                                                                                |
| EUID de proceso                   | ID del usuario efectivo del proceso.                                                                                                                                                                                        |
| Nombre de usuario de proceso      | Nombre del usuario que ha ejecutado el proceso.                                                                                                                                                                             |

| Nombre del campo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Description (Descripción)                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hora de inicio de proceso                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Hora de creación del proceso. Este campo está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z ).                                              |
| Proceso ejecutable SHA-256                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Hash SHA256 del ejecutable del proceso.                                                                                                                   |
| Ruta de script de proceso                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Ruta del archivo del script que se ha ejecutado.                                                                                                          |
| Variable de entorno de proceso                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Variable de entorno puesta a disposición del proceso. Solo se recopilan LD_PRELOAD y LD_LIBRARY_PATH .                                                    |
| Directorio de trabajo actual (PWD) de proceso                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Directorio de trabajo actual del proceso.                                                                                                                 |
| Proceso principal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Detalles del proceso principal. Un proceso principal es un proceso que creó el proceso observado.                                                         |
| Argumentos de línea de comandos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Command-line arguments proporcionados en el momento de la ejecución del proceso. Es posible que este campo contenga información confidencial del cliente. |
| <p>Actualmente, este campo está limitado a versiones específicas del agente correspondientes al tipo de recurso:</p> <ul style="list-style-type: none"> <li>• Fargate (solo Amazon ECS) con agente de GuardDuty seguridad v1.0.0 y versiones posteriores.</li> <li>• Instancias de Amazon EC2 con agente de GuardDuty seguridad v1.0.0 y versiones posteriores.</li> <li>• Los clústeres de Amazon EKS con la versión 1.4.0 o posterior del agente de seguridad.</li> </ul> <p>Para obtener más información, consulte <a href="#">GuardDuty versiones de lanzamiento del agente de seguridad</a>.</p> |                                                                                                                                                           |

## Eventos de contenedores

Los eventos de contenedores representan información asociada a las actividades de las cargas de trabajo de los contenedores. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de la carga de trabajo del contenedor que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                  | Description (Descripción)                                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de contenedor              | Nombre del contenedor.<br><br>Cuando está disponible, este campo muestra el valor de la etiqueta <code>io.kubernetes.container.name</code> . |
| UID de contenedor                 | ID único del contenedor asignado por el tiempo de ejecución del contenedor.                                                                  |
| Tiempo de ejecución de contenedor | Tiempo de ejecución del contenedor (por ejemplo, <code>docker</code> o <code>containerd</code> ) utilizado para ejecutar el contenedor.      |
| ID de imagen de contenedor        | ID de la imagen del contenedor.                                                                                                              |
| Nombre de imagen de contenedor    | Nombre de la imagen del contenedor.                                                                                                          |

## AWS Fargate Eventos de tareas (solo en Amazon ECS)

Fargate-Amazon Los eventos de tareas de ECS representan las actividades asociadas a las tareas de Amazon ECS que se ejecutan en los ordenadores de Fargate. La siguiente tabla incluye los nombres de campo y las descripciones de los eventos de ECS-Fargate tareas de Amazon que Runtime Monitoring recopila para detectar posibles amenazas.

| Nombre del campo                              | Description (Descripción)            |
|-----------------------------------------------|--------------------------------------|
| Nombre de recurso de Amazon (ARN) de la tarea | El ARN de la tarea.                  |
| Nombre del clúster                            | El nombre del clúster de Amazon ECS. |

| Nombre del campo    | Description (Descripción)                                                                                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apellido            | El apellido de la definición de la tarea. El <code>family</code> se utiliza como nombre para la definición de la tarea que se utiliza para lanzar la tarea.                                                                   |
| Nombre del servicio | El nombre del servicio de Amazon ECS, si la tarea se lanzó como parte de un servicio.                                                                                                                                         |
| Tipo de lanzamiento | La infraestructura en la que se ejecuta la tarea. Para la Supervisión en tiempo de ejecución con el tipo de recurso como <code>ECSCluster</code> , el tipo de lanzamiento puede ser <code>EC2</code> o <code>FARGATE</code> . |
| CPU                 | La cantidad de unidades de CPU utilizadas por la tarea, tal como se expresa en la definición de la tarea.                                                                                                                     |

## Eventos de pod de Kubernetes

En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos del pod de Kubernetes que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                | Description (Descripción)                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------|
| ID de pod                       | ID del pod de Kubernetes.                                                                       |
| Nombre de pod                   | Nombre del pod de Kubernetes.                                                                   |
| Espacio de nombres de pod       | Nombre del espacio de nombres de Kubernetes al que pertenece la carga de trabajo de Kubernetes. |
| Nombre de clúster de Kubernetes | Nombre del clúster de Kubernetes.                                                               |

## Eventos del sistema de nombres de dominio (DNS)

Los eventos del sistema de nombres de dominio (DNS) incluyen detalles de las consultas DNS realizadas por los tipos de recursos y las respuestas correspondientes. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de DNS que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                          | Description (Descripción)                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Tipo de socket                            | Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.                                                                 |
| Familia de direcciones                    | Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4. |
| ID de dirección                           | ID de la dirección de conexión.                                                                                                                     |
| Número de protocolo                       | Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).                                                                              |
| IP de punto de conexión remoto de DNS     | IP remota de la conexión.                                                                                                                           |
| Puerto de punto de conexión remoto de DNS | Número del puerto de la conexión.                                                                                                                   |
| IP de punto de conexión local de DNS      | IP local de la conexión.                                                                                                                            |
| Puerto de punto de conexión local de DNS  | Número del puerto de la conexión.                                                                                                                   |
| Carga de DNS                              | Carga de los paquetes de DNS que contiene consultas y respuestas de DNS.                                                                            |

## Eventos abiertos

Los eventos de apertura están asociados al acceso y modificación de archivos. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de apertura que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                                                                     |
|------------------|-----------------------------------------------------------------------------------------------|
| Ruta de archivo  | Ruta del archivo que se abre en este evento.                                                  |
| Indicadores      | Describe el modo de acceso a archivos, como solo lectura, solo escritura y lectura-escritura. |

## Evento de carga de módulo

En la siguiente tabla se incluyen el nombre del campo y la descripción del evento del módulo de carga que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)               |
|------------------|-----------------------------------------|
| Nombre de módulo | Nombre del módulo cargado en el kernel. |

## Eventos de Mprotect

Los eventos de Mprotect proporcionan información sobre los cambios en la configuración de protección de memoria de los procesos que se ejecutan en los sistemas supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de Mprotect que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo     | Description (Descripción)                                                                |
|----------------------|------------------------------------------------------------------------------------------|
| Rango de direcciones | Rango de direcciones para el que se modificaron las protecciones de acceso.              |
| Regiones de memoria  | Especifica la región del espacio de direcciones de un proceso, como la pila y el montón. |



| Nombre del campo | Description (Descripción)                                               |
|------------------|-------------------------------------------------------------------------|
| Indicadores      | Representa las opciones que controlan el comportamiento de este evento. |

## Eventos de montaje

Los eventos de montaje proporcionan información asociada al montaje y desmontaje de sistemas de archivos en el recurso supervisado. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de montaje que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo            | Description (Descripción)                                               |
|-----------------------------|-------------------------------------------------------------------------|
| Destino de montaje          | Ruta en la que se monta el origen del montaje.                          |
| Origen de montaje           | Ruta del host que se monta en el destino de montaje.                    |
| Tipo de sistema de archivos | Representa el tipo de sistema de archivos montado.                      |
| Indicadores                 | Representa las opciones que controlan el comportamiento de este evento. |

## Eventos de enlace

Los eventos de enlaces proporcionan visibilidad de las actividades de administración de enlaces del sistema de archivos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de enlaces que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                        |
|------------------|--------------------------------------------------|
| Ruta de enlace   | Ruta en la que se crea el enlace físico.         |
| Ruta de destino  | Ruta del archivo al que apunta el enlace físico. |

## Eventos de enlace simbólico

Los eventos de enlaces simbólicos (symlink) proporcionan visibilidad de las actividades de administración de enlaces simbólicos del sistema de archivos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de enlaces simbólicos que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                           |
|------------------|-----------------------------------------------------|
| Ruta de enlace   | Ruta en la que se crea el enlace simbólico.         |
| Ruta de destino  | Ruta del archivo al que apunta el enlace simbólico. |

## Eventos duplicados

Los eventos de duplicación (dup) proporcionan visibilidad sobre la duplicación de descriptores de archivo por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de duplicación que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                                  | Description (Descripción)                                                                                                                                                               |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descriptor de archivo antiguo                     | Descriptor de archivo que representa un objeto de archivo abierto.                                                                                                                      |
| Descriptor de archivo nuevo                       | Descriptor de archivo nuevo que es un duplicado del descriptor de archivo antiguo. Tanto el descriptor de archivo antiguo como el nuevo representan el mismo objeto de archivo abierto. |
| IP de punto de conexión remoto de duplicación     | Dirección IP remota del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.              |
| Puerto de punto de conexión remoto de duplicación | Puerto remoto del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.                    |

| Nombre del campo                                 | Description (Descripción)                                                                                                                                                 |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP de punto de conexión local de duplicación     | Dirección IP local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red. |
| Puerto de punto de conexión local de duplicación | Puerto local del socket de red que representa el descriptor de archivo antiguo. Solo se aplica cuando el descriptor de archivo antiguo representa un socket de red.       |

## Evento de mapa de memoria

En la siguiente tabla se incluye el nombre del campo y la descripción de los eventos del mapa de memoria que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                     |
|------------------|-----------------------------------------------|
| Ruta de archivo  | Ruta del archivo al que se asigna la memoria. |

## Eventos de socket

Los eventos de socket proporcionan información sobre las conexiones de socket de red utilizadas en las actividades de los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de socket que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo       | Description (Descripción)                                                                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Familia de direcciones | Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para la versión de IP del protocolo 4. |
| Tipo de socket         | Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.                                                                               |
| Número de protocolo    | Especifica un protocolo concreto de la familia de direcciones. Por lo general, hay un único protocolo en las familias de                                          |

| Nombre del campo | Description (Descripción)                                                                  |
|------------------|--------------------------------------------------------------------------------------------|
|                  | direcciones. Por ejemplo, la familia de direcciones AF_INET solo tiene el protocolo de IP. |

## Eventos de conexión

Los eventos de conexión proporcionan visibilidad de las conexiones de red establecidas por los procesos en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de conexión que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                   | Description (Descripción)                                                                                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Familia de direcciones             | Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4.                                                                 |
| Tipo de socket                     | Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.                                                                                                                                 |
| Número de protocolo                | Especifica un protocolo concreto de la familia de direcciones. Por lo general, hay un único protocolo en las familias de direcciones. Por ejemplo, la familia de direcciones AF_INET solo tiene el protocolo de IP. |
| Ruta de archivo                    | Ruta del archivo de socket si la familia de direcciones es AF_UNIX.                                                                                                                                                 |
| IP de punto de conexión remoto     | IP remota de la conexión.                                                                                                                                                                                           |
| Puerto de punto de conexión remoto | Número del puerto de la conexión.                                                                                                                                                                                   |
| IP de punto de conexión local      | IP local de la conexión.                                                                                                                                                                                            |

| Nombre del campo                  | Description (Descripción)         |
|-----------------------------------|-----------------------------------|
| Puerto de punto de conexión local | Número del puerto de la conexión. |

## Eventos de Readv de VM de proceso

Los eventos de procesos de lectura de memoria virtual (VM readv) proporcionan visibilidad de las operaciones de lectura realizadas por los procesos en sus propias regiones de memoria virtual. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de procesos de lectura de memoria virtual que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo              | Description (Descripción)                                               |
|-------------------------------|-------------------------------------------------------------------------|
| Indicadores                   | Representa las opciones que controlan el comportamiento de este evento. |
| PID de destino                | ID del proceso desde el que se lee la memoria.                          |
| UUID de proceso de destino    | ID único del proceso de destino.                                        |
| Ruta de ejecutable de destino | Ruta absoluta del archivo ejecutable del proceso de destino.            |

## Eventos de Writev de VM de proceso

Los eventos de procesos de escritura de memoria virtual (VM writev) proporcionan visibilidad de las operaciones de escritura realizadas por los procesos en sus propias regiones de memoria virtual. La siguiente tabla incluye los nombres de los campos y las descripciones de los eventos de los procesos de escritura de memoria virtual que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                                               |
|------------------|-------------------------------------------------------------------------|
| Indicadores      | Representa las opciones que controlan el comportamiento de este evento. |

| Nombre del campo              | Description (Descripción)                                    |
|-------------------------------|--------------------------------------------------------------|
| PID de destino                | ID del proceso en el que se escribe la memoria.              |
| UUID de proceso de destino    | ID único del proceso de destino.                             |
| Ruta de ejecutable de destino | Ruta absoluta del archivo ejecutable del proceso de destino. |

## Eventos de rastreo de procesos (Ptrace)

La llamada al sistema de rastreo de procesos (Ptrace) es un mecanismo de depuración y rastreo que permite a un proceso (rastreador) observar y controlar la ejecución de otro proceso (rastreado). Esto proporciona al rastreador la capacidad de inspeccionar y modificar la memoria, los registros y el flujo de ejecución del proceso de destino.

Los eventos ptrace proporcionan visibilidad sobre el uso de la llamada al sistema ptrace por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos ptrace que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo              | Description (Descripción)                                               |
|-------------------------------|-------------------------------------------------------------------------|
| PID de destino                | ID del proceso de destino.                                              |
| UUID de proceso de destino    | ID único del proceso de destino.                                        |
| Ruta de ejecutable de destino | Ruta absoluta del archivo ejecutable del proceso de destino.            |
| Indicadores                   | Representa las opciones que controlan el comportamiento de este evento. |

## Enviar de vinculación

Los eventos de vinculación proporcionan visibilidad sobre la vinculación de sockets de red por parte de los procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de vinculación que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo                  | Description (Descripción)                                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Familia de direcciones            | Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4. |
| Tipo de socket                    | Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.                                                                 |
| Número de protocolo               | Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).                                                                              |
| IP de punto de conexión local     | IP local de la conexión.                                                                                                                            |
| Puerto de punto de conexión local | Número del puerto de la conexión.                                                                                                                   |

## Eventos de escucha

Los eventos de escucha proporcionan visibilidad sobre el estado de escucha de los sockets de red, e indican si un socket de red está listo o no para aceptar conexiones entrantes. Un proceso que se ejecuta en el recurso supervisado establece el socket de red en estado de escucha. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de escucha que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo              | Description (Descripción)                                                                                                                           |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Familia de direcciones        | Representa el protocolo de comunicación asociado a la dirección. Por ejemplo, la familia de direcciones AF_INET se utiliza para el protocolo IP v4. |
| Tipo de socket                | Tipo de socket para indicar la semántica de la comunicación. Por ejemplo, SOCK_RAW.                                                                 |
| Número de protocolo           | Número de protocolo de capa 4 (por ejemplo, 17 para UDP y 6 para TCP).                                                                              |
| IP de punto de conexión local | IP local de la conexión.                                                                                                                            |

| Nombre del campo                  | Description (Descripción)         |
|-----------------------------------|-----------------------------------|
| Puerto de punto de conexión local | Número del puerto de la conexión. |

## Eventos de cambio de nombre

Los eventos de cambio de nombre proporcionan información sobre el cambio de nombre de archivos y directorios por parte de procesos que se ejecutan en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de cambio de nombre que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                                      |
|------------------|----------------------------------------------------------------|
| Ruta de archivo  | Ruta donde se encuentra el archivo cuyo nombre se ha cambiado. |
| Target           | La nueva ruta del archivo.                                     |

## Eventos de establecimiento de ID de usuario (UID)

Los eventos de establecimiento de ID de usuario (UID) proporcionan visibilidad de los cambios realizados en el ID de usuario (UID) asociado a los procesos en ejecución en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos de establecimiento de ID de usuario (UID) que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                    |
|------------------|----------------------------------------------|
| Nuevo EUID       | El nuevo ID de usuario efectivo del proceso. |
| Nuevo UID        | El nuevo ID de usuario del proceso.          |



## Eventos chmod

Los eventos chmod proporcionan visibilidad de los cambios en los permisos (modo) de archivos y directorios en los recursos supervisados. En la siguiente tabla se incluyen los nombres de los campos y las descripciones de los eventos chmod que la Supervisión en tiempo de ejecución recopila para detectar posibles amenazas.

| Nombre del campo | Description (Descripción)                                     |
|------------------|---------------------------------------------------------------|
| Ruta de archivo  | Ruta del archivo que invoca este evento.                      |
| Modo de archivo  | Los permisos de acceso actualizados para el archivo asociado. |

## Agente de alojamiento GuardDuty de repositorios Amazon ECR

En las siguientes secciones se enumeran los repositorios de Amazon Elastic Container Registry (Amazon ECR) GuardDuty donde se aloja el agente de seguridad que se implementa en los clústeres de Amazon EKS y Amazon ECS.

El requisito previo para [Requisitos previos para el acceso a imágenes de contenedores](#) requiere que proporcione un rol de ejecución de tareas que tenga determinados permisos de Amazon Elastic Container Registry (Amazon ECR). Para restringir aún más estos permisos, puede añadir el URI del repositorio de Amazon ECR que aloja el GuardDuty agente para los recursos de Fargate-Amazon ECS.

### Contenido

- [Repositorio de ECR para las versiones 1.15.0 a 1.8.1 del agente EKS \(eks.build.2\)](#)
- [Repositorio de ECR para el agente EKS, versión 1.8.1 \(eks.build.1\)](#)
- [Repositorio ECR para el agente en GuardDuty AWS Fargate \(solo Amazon ECS\)](#)

## Repositorio de ECR para las versiones 1.15.0 a 1.8.1 del agente EKS (eks.build.2)

Cuando habilite la configuración GuardDuty automática de Runtime Monitoring for EKS, GuardDuty implementará esta versión del agente en sus clústeres de Amazon EKS. Para obtener información

acerca de cómo habilitar el agente automatizado, consulte [Administración automática del agente de seguridad para los recursos de Amazon EKS](#).

En la siguiente tabla se muestran los URI del repositorio de Amazon ECR donde se alojan las versiones del agente de GuardDuty seguridad 1.15.0.eks.build.2, 1.11.0.eks.build.2, 1.10.0.eks.build.2, 1.9.0.eks.build.2, y para 1.8.0.eks.build.2 Amazon EKS.

| Región de AWS             | URI del repositorio de Amazon ECR               |
|---------------------------|-------------------------------------------------|
| Oeste de EE. UU. (Oregón) | 602401143452.dkr.ecr.us-west-2.amazonaws.com    |
|                           | 039403964562.dkr.ecr.us-west-2.amazonaws.com    |
| Europa (París)            | 602401143452.dkr.ecr.eu-west-3.amazonaws.com    |
|                           | 113643092156.dkr.ecr.eu-west-3.amazonaws.com    |
| Asia-Pacífico (Mumbai)    | 602401143452.dkr.ecr.ap-south-1.amazonaws.com   |
|                           | 610108029387.dkr.ecr.ap-south-1.amazonaws.com   |
| Asia-Pacífico (Hyderabad) | 900889452093.dkr.ecr.ap-south-2.amazonaws.com   |
|                           | 618745550137.dkr.ecr.ap-south-2.amazonaws.com   |
| Canadá (centro)           | 602401143452.dkr.ecr.ca-central-1.amazonaws.com |
|                           | 001188825231.dkr.ecr.ca-central-1.amazonaws.com |

| Región de AWS                          | URI del repositorio de Amazon ECR               |
|----------------------------------------|-------------------------------------------------|
| Oeste de Canadá (Calgary)              | 761377655185.dkr.ecr.ca-west-1.amazonaws.com    |
|                                        | –                                               |
| Medio Oriente (EAU)                    | 759879836304.dkr.ecr.me-central-1.amazonaws.com |
|                                        | 601769779514.dkr.ecr.me-central-1.amazonaws.com |
| Europa (Londres)                       | 602401143452.dkr.ecr.eu-west-2.amazonaws.com    |
|                                        | 109118265657.dkr.ecr.eu-west-2.amazonaws.com    |
| Oeste de EE. UU. (Norte de California) | 602401143452.dkr.ecr.us-west-1.amazonaws.com    |
|                                        | 373421517865.dkr.ecr.us-west-1.amazonaws.com    |
| Este de EE. UU. (Norte de Virginia)    | 602401143452.dkr.ecr.us-east-1.amazonaws.com    |
|                                        | 031903291036.dkr.ecr.us-east-1.amazonaws.com    |
| Este de EE. UU. (Ohio)                 | 602401143452.dkr.ecr.us-east-2.amazonaws.com    |
|                                        | 591382732059.dkr.ecr.us-east-2.amazonaws.com    |
| Europa (Irlanda)                       | 602401143452.dkr.ecr.eu-west-1.amazonaws.com    |

| Región de AWS               | URI del repositorio de Amazon ECR                              |
|-----------------------------|----------------------------------------------------------------|
|                             | <code>673884943994.dkr.ecr.eu-west-1.amazonaws.com</code>      |
| América del Sur (São Paulo) | <code>602401143452.dkr.ecr.sa-east-1.amazonaws.com</code>      |
|                             | <code>941219317354.dkr.ecr.sa-east-1.amazonaws.com</code>      |
| Europa (Estocolmo)          | <code>602401143452.dkr.ecr.eu-north-1.amazonaws.com</code>     |
|                             | <code>366771026645.dkr.ecr.eu-north-1.amazonaws.com</code>     |
| Europa (Fráncfort)          | <code>602401143452.dkr.ecr.eu-central-1.amazonaws.com</code>   |
|                             | <code>409493279830.dkr.ecr.eu-central-1.amazonaws.com</code>   |
| Europa (Zúrich)             | <code>900612956339.dkr.ecr.eu-central-2.amazonaws.com</code>   |
|                             | <code>718440343717.dkr.ecr.eu-central-2.amazonaws.com</code>   |
| Asia-Pacífico (Singapur)    | <code>602401143452.dkr.ecr.ap-southeast-1.amazonaws.com</code> |
|                             | <code>584580519942.dkr.ecr.ap-southeast-1.amazonaws.com</code> |
| Asia-Pacífico (Sídney)      | <code>602401143452.dkr.ecr.ap-southeast-2.amazonaws.com</code> |
|                             | <code>011662287384.dkr.ecr.ap-southeast-2.amazonaws.com</code> |

| Región de AWS             | URI del repositorio de Amazon ECR                 |
|---------------------------|---------------------------------------------------|
| Asia-Pacífico (Yakarta)   | 296578399912.dkr.ecr.ap-southeast-3.amazonaws.com |
|                           | 617474730032.dkr.ecr.ap-southeast-3.amazonaws.com |
| Asia-Pacífico (Tokio)     | 602401143452.dkr.ecr.ap-northeast-1.amazonaws.com |
|                           | 781592569369.dkr.ecr.ap-northeast-1.amazonaws.com |
| Asia-Pacífico (Seúl)      | 602401143452.dkr.ecr.ap-northeast-2.amazonaws.com |
|                           | 732248494576.dkr.ecr.ap-northeast-2.amazonaws.com |
| Asia-Pacífico (Osaka)     | 602401143452.dkr.ecr.ap-northeast-3.amazonaws.com |
|                           | 810724417379.dkr.ecr.ap-northeast-3.amazonaws.com |
| Asia-Pacífico (Hong Kong) | 800184023465.dkr.ecr.ap-east-1.amazonaws.com      |
|                           | 790429075973.dkr.ecr.ap-east-1.amazonaws.com      |
| Middle East (Bahrain)     | 558608220178.dkr.ecr.me-south-1.amazonaws.com     |
|                           | 541829937850.dkr.ecr.me-south-1.amazonaws.com     |
| Europa (Milán)            | 590381155156.dkr.ecr.eu-south-1.amazonaws.com     |

| Región de AWS             | URI del repositorio de Amazon ECR                 |
|---------------------------|---------------------------------------------------|
|                           | 528450769569.dkr.ecr.eu-south-1.amazonaws.com     |
|                           | 455263428931.dkr.ecr.eu-south-2.amazonaws.com     |
| Europa (España)           | 531047660167.dkr.ecr.eu-south-2.amazonaws.com     |
|                           | 877085696533.dkr.ecr.af-south-1.amazonaws.com     |
| África (Ciudad del Cabo)  | 379032919888.dkr.ecr.af-south-1.amazonaws.com     |
|                           | 491585149902.dkr.ecr.ap-southeast-4.amazonaws.com |
| Asia-Pacífico (Melbourne) | 750462861327.dkr.ecr.ap-southeast-4.amazonaws.com |
|                           | 066635153087.dkr.ecr.il-central-1.amazonaws.com   |
| Israel (Tel Aviv)         | 292660727137.dkr.ecr.il-central-1.amazonaws.com   |
| Asia-Pacífico (Malasia)   | 151610086707.dkr.ecr.ap-southeast-5.amazonaws.com |
| Asia-Pacífico (Tailandia) | 121268973566.dkr.ecr.ap-southeast-7.amazonaws.com |
| México (centro)           | 730335286997.dkr.ecr.mx-central-1.amazonaws.com   |
| Asia-Pacífico (Taipéi)    | 533267051163.dkr.ecr.ap-east-2.amazonaws.com      |

## Repositorio de ECR para el agente EKS, versión 1.8.1 (eks.build.1)

En esta sección se proporciona el repositorio de Amazon ECR para la versión 1.8.1 del agente Amazon EKS (v1.8.1-eks-build.1). Si utiliza la v1.8.1-eks-build.1, le recomendamos que cambie a la versión predeterminada del agente, GuardDuty que suele ser la versión más reciente del agente. Para ello, identifique el agente más reciente de [Se lanzaron versiones de agente publicadas para los recursos de Amazon EKS](#) y, a continuación, lleve a cabo los pasos que se indican en [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#).

En la siguiente tabla se muestran los URI del repositorio de Amazon ECR donde se aloja GuardDuty la versión del agente de seguridad para 1.8.1-eks-build.1 Amazon EKS.

| Región de AWS                          | URI del repositorio de Amazon ECR               |
|----------------------------------------|-------------------------------------------------|
| Oeste de EE. UU. (Oregón)              | 039403964562.dkr.ecr.us-west-2.amazonaws.com    |
| Europa (París)                         | 113643092156.dkr.ecr.eu-west-3.amazonaws.com    |
| Asia-Pacífico (Mumbai)                 | 610108029387.dkr.ecr.ap-south-1.amazonaws.com   |
| Asia-Pacífico (Hyderabad)              | 618745550137.dkr.ecr.ap-south-2.amazonaws.com   |
| Canadá (centro)                        | 001188825231.dkr.ecr.ca-central-1.amazonaws.com |
| Medio Oriente (EAU)                    | 601769779514.dkr.ecr.me-central-1.amazonaws.com |
| Europa (Londres)                       | 109118265657.dkr.ecr.eu-west-2.amazonaws.com    |
| Oeste de EE. UU. (Norte de California) | 373421517865.dkr.ecr.us-west-1.amazonaws.com    |

| Región de AWS                       | URI del repositorio de Amazon ECR                 |
|-------------------------------------|---------------------------------------------------|
| Este de EE. UU. (Norte de Virginia) | 031903291036.dkr.ecr.us-east-1.amazonaws.com      |
| Este de EE. UU. (Ohio)              | 591382732059.dkr.ecr.us-east-2.amazonaws.com      |
| Europa (Irlanda)                    | 673884943994.dkr.ecr.eu-west-1.amazonaws.com      |
| América del Sur (São Paulo)         | 941219317354.dkr.ecr.sa-east-1.amazonaws.com      |
| Europa (Estocolmo)                  | 366771026645.dkr.ecr.eu-north-1.amazonaws.com     |
| Europa (Fráncfort)                  | 409493279830.dkr.ecr.eu-central-1.amazonaws.com   |
| Europa (Zúrich)                     | 718440343717.dkr.ecr.eu-central-2.amazonaws.com   |
| Asia-Pacífico (Singapur)            | 584580519942.dkr.ecr.ap-southeast-1.amazonaws.com |
| Asia-Pacífico (Sídney)              | 011662287384.dkr.ecr.ap-southeast-2.amazonaws.com |
| Asia-Pacífico (Yakarta)             | 617474730032.dkr.ecr.ap-southeast-3.amazonaws.com |
| Asia-Pacífico (Tokio)               | 781592569369.dkr.ecr.ap-northeast-1.amazonaws.com |
| Asia-Pacífico (Seúl)                | 732248494576.dkr.ecr.ap-northeast-2.amazonaws.com |
| Asia-Pacífico (Osaka)               | 810724417379.dkr.ecr.ap-northeast-3.amazonaws.com |



| Región de AWS             | URI del repositorio de Amazon ECR                 |
|---------------------------|---------------------------------------------------|
| Asia-Pacífico (Hong Kong) | 790429075973.dkr.ecr.ap-east-1.amazonaws.com      |
| Middle East (Bahrain)     | 541829937850.dkr.ecr.me-south-1.amazonaws.com     |
| Europa (Milán)            | 528450769569.dkr.ecr.eu-south-1.amazonaws.com     |
| Europa (España)           | 531047660167.dkr.ecr.eu-south-2.amazonaws.com     |
| África (Ciudad del Cabo)  | 379032919888.dkr.ecr.af-south-1.amazonaws.com     |
| Asia-Pacífico (Melbourne) | 750462861327.dkr.ecr.ap-southeast-4.amazonaws.com |
| Israel (Tel Aviv)         | 292660727137.dkr.ecr.il-central-1.amazonaws.com   |

## Repositorio ECR para el agente en GuardDuty AWS Fargate (solo Amazon ECS)

Como requisito previo para utilizar Runtime Monitoring for Amazon ECS-Fargate, debe hacerlo [Requisitos previos para el acceso a imágenes de contenedores](#). La imagen del contenedor sidecar del GuardDuty agente se almacena en Amazon ECR y sus capas de imágenes se almacenan en Amazon S3. Para obtener más información, consulte [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

En la siguiente tabla se muestran los repositorios de Amazon ECR que alojan el GuardDuty agente para cada uno de ellos (solo AWS Fargate Amazon ECS). Región de AWS

| Región de AWS                          | URI del repositorio de Amazon ECR                                            |
|----------------------------------------|------------------------------------------------------------------------------|
| Oeste de EE. UU. (Oregón)              | 733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guard-duty-agent-fargate    |
| Europa (París)                         | 665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guard-duty-agent-fargate    |
| Asia-Pacífico (Mumbai)                 | 251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guard-duty-agent-fargate   |
| Asia-Pacífico (Hyderabad)              | 950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guard-duty-agent-fargate   |
| Canadá (centro)                        | 354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guard-duty-agent-fargate |
| Medio Oriente (EAU)                    | 000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guard-duty-agent-fargate |
| Europa (Londres)                       | 892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guard-duty-agent-fargate    |
| Oeste de EE. UU. (Norte de California) | 684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guard-duty-agent-fargate    |
| Este de EE. UU. (Norte de Virginia)    | 593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guard-duty-agent-fargate    |

| Región de AWS               | URI del repositorio de Amazon ECR                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------|
| Este de EE. UU. (Ohio)      | <code>307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guard-duty-agent-fargate</code>      |
| Europa (Irlanda)            | <code>694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guard-duty-agent-fargate</code>      |
| América del Sur (São Paulo) | <code>758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guard-duty-agent-fargate</code>      |
| Europa (Estocolmo)          | <code>591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guard-duty-agent-fargate</code>     |
| Europa (Fráncfort)          | <code>323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guard-duty-agent-fargate</code>   |
| Europa (Zúrich)             | <code>529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guard-duty-agent-fargate</code>   |
| Asia-Pacífico (Singapur)    | <code>174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guard-duty-agent-fargate</code> |
| Asia-Pacífico (Sídney)      | <code>005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guard-duty-agent-fargate</code> |
| Asia-Pacífico (Yakarta)     | <code>510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guard-duty-agent-fargate</code> |

| Región de AWS             | URI del repositorio de Amazon ECR                                             |
|---------------------------|-------------------------------------------------------------------------------|
| Asia-Pacífico (Tokio)     | 533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate |
| Asia-Pacífico (Seúl)      | 914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate |
| Asia-Pacífico (Osaka)     | 273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate |
| Asia-Pacífico (Hong Kong) | 258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate      |
| Middle East (Bahrain)     | 536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Europa (Milán)            | 266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Europa (España)           | 919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate     |
| África (Ciudad del Cabo)  | 197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate     |
| Asia-Pacífico (Melbourne) | 251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate |

| Región de AWS             | URI del repositorio de Amazon ECR                                             |
|---------------------------|-------------------------------------------------------------------------------|
| Israel (Tel Aviv)         | 870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate   |
| Asia-Pacífico (Malasia)   | 156041399949.dkr.ecr.ap-southeast-5.amazonaws.com/aws-guardduty-agent-fargate |
| Asia-Pacífico (Tailandia) | 054037130133.dkr.ecr.ap-southeast-7.amazonaws.com/aws-guardduty-agent-fargate |
| Oeste de Canadá (Calgary) | 339712888787.dkr.ecr.ca-west-1.amazonaws.com/aws-guardduty-agent-fargate      |
| México (centro)           | 311141559934.dkr.ecr.mx-central-1.amazonaws.com/aws-guardduty-agent-fargate   |
| Asia-Pacífico (Taipéi)    | 259886477082.dkr.ecr.ap-east-2.amazonaws.com/aws-guardduty-agent-fargate      |

## Dos agentes de seguridad en el mismo host subyacente

Las instancias de Amazon EC2 pueden admitir varios tipos de cargas de trabajo. Cuando se configura un agente de seguridad automatizado en una instancia de Amazon EC2, es posible que la misma instancia de EC2 tenga otro agente de seguridad a través de EKS.

### Descripción general de

Considere un escenario en el que ha habilitado la Supervisión en tiempo de ejecución. Ahora, habilita el agente automatizado para Amazon EKS mediante GuardDuty. Además, ha habilitado el agente automatizado para Amazon EC2. Puede ocurrir que el mismo host subyacente se instale con dos agentes de seguridad: uno para Amazon EKS y otro para Amazon EC2. Esto podría provocar que

dos agentes de seguridad se ejecutaran en el mismo host y recopilaran los eventos en tiempo de ejecución y los enviaran a ellos GuardDuty, lo que podría generar resultados duplicados.

## Impact

- Cuando hay más de un agente de seguridad en ejecución en el mismo host, es posible que la cuenta experimente el doble de demanda de CPU y memoria. Para obtener más información acerca de los límites de CPU y memoria para cada tipo de recurso, consulte [Requisitos previos](#) para ese recurso.
- GuardDuty ha diseñado la función de monitorización del tiempo de ejecución de forma que, aunque se superpongan dos agentes de seguridad que recopilen eventos en tiempo de ejecución del mismo host subyacente, solo se le cobre a su cuenta por una transmisión de eventos en tiempo de ejecución.

## ¿Cómo GuardDuty gestiona varios agentes

GuardDuty detecta cuando dos agentes de seguridad se están ejecutando en el mismo host y designa solo a uno de ellos como el agente de seguridad que recopila activamente los eventos de tiempo de ejecución. El segundo agente consumirá un mínimo de recursos del sistema para evitar cualquier impacto en el rendimiento de las aplicaciones.

GuardDuty considera los siguientes escenarios:

- Cuando una instancia de EC2 entra en el ámbito tanto de los agentes de seguridad de Amazon EKS como de Amazon EC2, el agente de seguridad de EKS tiene prioridad. Esto se aplicará únicamente si utiliza la versión 1.1.0 o posterior del agente de seguridad para Amazon EC2. Las versiones más antiguas de los agentes seguirán en ejecución y aún recopilarán eventos en tiempo de ejecución, ya que las versiones más antiguas no se ven afectadas por la priorización.
- Cuando Amazon EKS y Amazon EC2 hayan GuardDuty gestionado agentes de seguridad y su instancia de Amazon EC2 también esté gestionada por SSM, ambos agentes de seguridad se instalarán en el nivel de host. Una vez instalados los agentes, GuardDuty decide qué agente de seguridad seguirá ejecutándose. Cuando ambos agentes de seguridad se ejecutan, finalmente solo uno de ellos recopila eventos en tiempo de ejecución.
- Cuando los agentes de seguridad asociados a EC2 y EKS se ejecutan al mismo tiempo, es GuardDuty posible que solo se generen resultados duplicados durante el período de superposición.

Esto puede ocurrir si:

- Los agentes de seguridad tanto para EC2 como para EKS se configuran mediante GuardDuty (automáticamente), o
- El recurso de Amazon EKS cuenta con un agente de seguridad automatizado.
- Cuando el agente de seguridad EKS ya está en ejecución, si lo implementa manualmente en el mismo host subyacente y cumple todos los requisitos previos, es GuardDuty posible que no instale un segundo agente de seguridad.

## Supervisión del tiempo de ejecución de EKS en GuardDuty

EKS Runtime Monitoring proporciona cobertura de detección de amenazas en tiempo de ejecución para los nodos y contenedores de Amazon Elastic Kubernetes Service (Amazon EKS) de su entorno. AWS EKS Runtime Monitoring utiliza un agente de GuardDuty seguridad que añade visibilidad en tiempo de ejecución a las cargas de trabajo individuales de EKS, por ejemplo, el acceso a los archivos, la ejecución de procesos y las conexiones de red. El agente GuardDuty de seguridad ayuda a GuardDuty identificar los contenedores específicos de los clústeres de EKS que pueden estar en peligro. También puede detectar los intentos de transferir los privilegios de un contenedor individual al host EC2 subyacente y al entorno más amplio AWS .

Con la disponibilidad de Runtime Monitoring, se GuardDuty ha consolidado la experiencia de consola de EKS Runtime Monitoring en Runtime Monitoring. GuardDuty no migrará automáticamente la configuración de EKS Runtime Monitoring en su nombre. Para ello, es necesario que actúe. Si desea seguir utilizando únicamente EKS Runtime Monitoring, puede usar las API o AWS CLI comprobar y actualizar el estado de la configuración actual de EKS Runtime Monitoring. Sin embargo, GuardDuty recomienda [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#) usar Runtime Monitoring para monitorear los clústeres de Amazon EKS.

### Temas

- [Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas \(API\)](#)
- [Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente \(API\)](#)
- [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#)

## Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas (API)

En entornos con varias cuentas, solo la cuenta de GuardDuty administrador delegado puede habilitar o deshabilitar EKS Runtime Monitoring para las cuentas de los miembros y administrar los GuardDuty agentes de los clústeres de EKS que pertenecen a las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Para más información sobre los entornos con varias cuentas, consulte [Managing multiple accounts](#).

### Configuración de EKS Runtime Monitoring para la cuenta de administrador delegado GuardDuty

En esta sección se proporcionan los pasos para configurar EKS Runtime Monitoring y administrar el agente de GuardDuty seguridad para los clústeres de EKS que pertenecen a la cuenta de GuardDuty administrador delegado.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Método preferido para administrar el agente GuardDuty de seguridad                        | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS) | <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>.</p> <p>Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>ENABLED</code>.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región</p> |



| Método preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <p>actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectorsAPI</a>.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="654 552 1507 831">aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] }]'</pre> |

| Método preferido para administrar el agente GuardDuty de seguridad                                               | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Método preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <p>3.</p> <div data-bbox="716 254 1507 667"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <div data-bbox="716 1749 1507 1879"> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONIT</pre> </div> |

| Método preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                              |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <pre>ORING", "Status" : " <b>ENABLED</b>", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " <b>ENABLED</b>"}] }]'</pre> |

| Método preferido para administrar el agente GuardDuty de seguridad                | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li data-bbox="654 275 1485 548">1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li data-bbox="654 569 1485 1283">2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li data-bbox="716 884 1409 968">• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li data-bbox="716 989 1409 1073">• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li data-bbox="716 1094 1442 1178">• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li data-bbox="716 1199 1479 1283">• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p data-bbox="748 1325 1463 1461">Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre data-bbox="768 1524 1390 1713">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="654 1755 1398 1831">3. Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto</li> </ol> |

| Método preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    | <p>features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el true par GuardDutyManaged -.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectorsAPI</a>.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'</pre> |

| Método preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                      | <ol style="list-style-type: none"> <li> <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>.</p> <p>Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>.</p> <p>Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'</pre> </li> <li> <p>Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</p> </li> </ol> |

Auto-enable Supervisión del tiempo de ejecución de EKS para todas las cuentas de los miembros

En esta sección se incluyen los pasos para habilitar la Supervisión en tiempo de ejecución de EKS y administrar el agente de seguridad para todas las cuentas de miembro. Esto incluye la cuenta de

GuardDuty administrador delegado, las cuentas de los miembros existentes y las nuevas cuentas que se unen a la organización.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Enfoque preferido para administrar el agente GuardDuty de seguridad                              | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS)</p> | <p>Para habilitar EKS Runtime Monitoring de forma selectiva para sus cuentas de miembros, ejecute la operación de <a href="#">updateMemberDetectorsAPI</a> con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detector ID correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectorsAPI</a>.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> |



Enfoque preferido para  
administrar el agente  
GuardDuty de seguridad

## Pasos

### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                              | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li data-bbox="524 321 1510 552">1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -false. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li data-bbox="524 573 1510 1224">2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li data-bbox="586 842 1425 877">• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li data-bbox="586 898 1463 934">• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li data-bbox="586 955 1446 991">• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li data-bbox="586 1012 1471 1098">• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p data-bbox="618 1140 1474 1224">Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre data-bbox="639 1283 1406 1434">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="524 1476 1510 1812">3. <div data-bbox="618 1507 1463 1801"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> <div>  <b>Note</b><br/> También puede pasar una lista de ID de cuentas separadas por un espacio. </div> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad                | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determina dos clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li data-bbox="524 321 1510 548">1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -true. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li data-bbox="524 569 1510 1094">2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li data-bbox="586 842 1425 877">• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li data-bbox="586 898 1463 934">• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li data-bbox="586 955 1446 991">• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li data-bbox="586 1012 1471 1094">• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p data-bbox="618 1140 1474 1222">Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre data-bbox="639 1283 1406 1434">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="524 1476 1446 1608">3. Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>.</li> </ol> <p data-bbox="586 1650 1442 1732">Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>.</p> <p data-bbox="586 1776 1466 1860">GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS</p> |

## Enfoque preferido para administrar el agente GuardDuty de seguridad

### Pasos

que se hayan etiquetado con el `true` par `GuardDutyManaged`.

Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorID correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] ]'
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                       | <ol style="list-style-type: none"> <li> <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] } ]'</pre> </li> <li> <p>Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</p> </li> </ol> |

## Configuración de la supervisión en tiempo de ejecución de EKS para todas las cuentas de miembros activas existentes

En esta sección se incluyen los pasos para habilitar EKS Runtime Monitoring y administrar el agente de GuardDuty seguridad para las cuentas de los miembros activos existentes en su organización.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Método preferido para gestionar el agente GuardDuty de seguridad                          | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS) | <p>Para habilitar EKS Runtime Monitoring de forma selectiva para sus cuentas de miembros, ejecute la operación de <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> <div> <p> <b>Note</b></p> <p>También puede pasar una lista de ID de cuentas separadas por un espacio.</p> </div> |



| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos |
|------------------------------------------------------------------|-------|
|------------------------------------------------------------------|-------|

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

| Método preferido para gestionar el agente GuardDuty de seguridad                                                 | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li data-bbox="524 321 1510 548">1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -false. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li data-bbox="524 573 1510 1220">2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li data-bbox="586 842 1425 877">• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li data-bbox="586 898 1463 934">• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li data-bbox="586 955 1446 991">• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li data-bbox="586 1012 1471 1094">• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p data-bbox="618 1140 1474 1220">Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre data-bbox="639 1283 1406 1430">"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li data-bbox="524 1476 1510 1797">3. <div data-bbox="618 1507 1463 1797"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> </li> </ol> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>Para activar EKS Runtime Monitoring de forma selectiva en las cuentas de sus miembros, ejecute la operación de la <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detector ID correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] ]'</pre> <div>  <b>Note</b><br/> También puede pasar una lista de ID de cuentas separadas por un espacio. </div> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Método preferido para gestionar el agente GuardDuty de seguridad                   | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determina dos clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDuty Managed -true. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Para habilitar de forma selectiva EKS Runtime Monitoring para sus cuentas de miembros, ejecute la operación de <a href="#">updateMemberDetectors</a> API con la suya propia <code>detector ID</code>.</li> </ol> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS</p> |

## Método preferido para gestionar el agente GuardDuty de seguridad

### Pasos

que se hayan etiquetado con el `true` par `GuardDutyManaged`.

Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorID correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

En el siguiente ejemplo se habilita `EKS_RUNTIME_MONITORING` y se deshabilita `EKS_ADDON_MANAGEMENT` :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] ]'
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                    | <ol style="list-style-type: none"> <li>Para activar EKS Runtime Monitoring de forma selectiva en sus cuentas de miembros, ejecute la operación de la <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.<br/><br/>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.<br/><br/>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detector ID correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/">https://console.aws.amazon.com/guardduty/</a> consola o ejecute la <a href="#">ListDetectors</a> API.<br/><br/>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :<br/><br/> <pre>aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name": "EKS_RUNTIME_MONITORING", "Status": "ENABLED", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "Status": "ENABLED"}] } ]'</pre> </li> <li>Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</li> </ol> |

## Auto-enable EKS Runtime Monitoring para nuevos miembros

La cuenta de GuardDuty administrador delegado puede habilitar automáticamente EKS Runtime Monitoring y elegir un enfoque para administrar el agente de GuardDuty seguridad para las nuevas cuentas que se unan a su organización.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Método preferido para gestionar el agente de seguridad GuardDuty                          | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS) | <p>Para activar EKS Runtime Monitoring de forma selectiva para sus nuevas cuentas, invoque la operación de la <a href="#">UpdateOrganizationConfiguration</a> API con la suya propia.</p> <p><i>detector ID</i></p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilitan EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio.</p> <p>Para encontrar la <code>detectorId</code> correspondiente a tu cuenta y región actual, consulta la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecuta la <a href="#">ListDetectors</a> API.</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNT</pre> |



| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <div data-bbox="654 254 1507 394"><pre>IME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre></div> <p data-bbox="654 430 1507 667">Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Método preferido para gestionar el agente de seguridad GuardDuty                                                 | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>3.</p> <div data-bbox="714 262 1507 667"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <p>Para activar EKS Runtime Monitoring de forma selectiva para sus nuevas cuentas, invoque la operación de la <a href="#">UpdateOrganizationConfiguration</a> API con la suya propia. <i>detector ID</i></p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilitan EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio.</p> |

| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>Para encontrar la <code>detectorId</code> correspondiente a tu cuenta y región actual, consulta la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecuta la <a href="#">ListDetectors</a> API.</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'</pre> <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Método preferido para gestionar el agente de seguridad GuardDuty                  | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Para habilitar de forma selectiva la monitorización de tiempo de ejecución de EKS para sus nuevas cuentas,</li> </ol> |

| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>invoque la operación de la <a href="#">UpdateOrganizationConfiguration</a> API con la suya propia. <i>detector ID</i></p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el true par GuardDutyManaged -.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio.</p> <p>Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecuta la <a href="#">ListDetectors</a> API.</p> <pre>aws guardduty update-organization-configuration --detector-id <i>12abc34d567e8fa901bc2d34e56789f0</i> --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> |

| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                    | <p>1. Para activar EKS Runtime Monitoring de forma selectiva para sus nuevas cuentas, invoque la operación de la <a href="#">UpdateOrganizationConfiguration</a> API con la suya propia. <i>detector ID</i></p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT para una sola cuenta. También puede pasar una lista de ID de cuentas separadas por un espacio.</p> <p>Para encontrar la <code>detectorId</code> correspondiente a tu cuenta y región actual, consulta la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecuta la <a href="#">ListDetectors</a> API.</p> <pre>aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name": "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration": [{"Name": "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] }]'</pre> <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code></p> |



| Método preferido para gestionar el agente de seguridad GuardDuty | Pasos                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> <p>2. Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</p> |

## Habilitación de la Supervisión en tiempo de ejecución de EKS para cuentas de miembros activas individuales

En esta sección se incluyen los pasos para configurar la Supervisión en tiempo de ejecución de EKS y administrar el agente de seguridad para cuentas de miembro activas individuales.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Método preferido para gestionar el agente GuardDuty de seguridad                          | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS) | <p>Para habilitar EKS Runtime Monitoring de forma selectiva para sus cuentas de miembros, ejecute la operación de <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región</p> |

## Método preferido para gestionar el agente GuardDuty de seguridad

### Pasos

actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectorsAPI](#).

En el ejemplo siguiente se habilita EKS\_RUNTIME\_MONITORING y EKS\_ADDON\_MANAGEMENT :

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

| Método preferido para gestionar el agente GuardDuty de seguridad                                                 | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDutyManaged -false. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por eks:TagResource .</li> <li>• Sustituya <i>ec2:DeleteTags</i> por eks:UntagResource .</li> <li>• Reemplace <i>access-project</i> por GuardDutyManaged</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>3.</p> <div data-bbox="716 254 1507 667"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <p>Para activar EKS Runtime Monitoring de forma selectiva en las cuentas de sus miembros, ejecute la operación de la <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <div data-bbox="716 1749 1507 1879"> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature</pre> </div> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <div data-bbox="716 254 1507 432"><pre>s ' [{"Name" : "EKS_RUNTIME_MONITORING",<br/>      "Status" : "<b>ENABLED</b>", "AdditionalConfigu<br/>ration" : [{"Name" : "EKS_ADDON_MANAGEMENT",<br/>            "Status" : "<b>ENABLED</b>"}] } ] '</pre></div> <div data-bbox="716 470 1507 688"><p> <b>Note</b></p><p>También puede pasar una lista de ID de cuentas separadas por un espacio.</p></div> <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de UnprocessedAccounts vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |

| Método preferido para gestionar el agente GuardDuty de seguridad                  | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -true</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Para habilitar de forma selectiva EKS Runtime Monitoring para sus cuentas de miembros, ejecute la</li> </ol> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>operación de <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el true par GuardDutyManaged -.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 111122223333 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] }]'</pre> <div>  <b>Note</b><br/> También puede pasar una lista de ID de cuentas separadas por un espacio. </div> |

| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                  | <p>Cuando el código se haya ejecutado correctamente, devolverá una lista de <code>UnprocessedAccounts</code> vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.</p> |



| Método preferido para gestionar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                    | <ol style="list-style-type: none"> <li> <p>Para activar EKS Runtime Monitoring de forma selectiva en sus cuentas de miembros, ejecute la operación de la <a href="#">updateMemberDetectors</a> API con la suya propia <i>detector ID</i>.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-member-detectors -- detector-id 12abc34d567e8fa901bc2d34e56 789f0 --account-ids 5555555555 --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfigu ration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] } ]'</pre> </li> <li> <p>Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</p> </li> </ol> |

## Configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente (API)

Una cuenta independiente es la que decide activar o desactivar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Configurar la Supervisión en tiempo de ejecución de EKS para entornos con varias cuentas \(API\)](#).

Después de activar Runtime Monitoring, asegúrese de instalar el agente GuardDuty de seguridad mediante una configuración automática o un despliegue manual. Como parte de completar todos los pasos que se indican en el siguiente procedimiento, asegúrese de instalar el agente de seguridad.

Según los [Enfoques para administrar los agentes GuardDuty de seguridad en los clústeres de Amazon EKS](#), puede elegir el enfoque que prefiera y seguir los pasos que se indican en la siguiente tabla.

| Enfoque preferido para administrar el agente GuardDuty de seguridad                       | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestione el agente de seguridad mediante GuardDuty (supervise todos los clústeres de EKS) | <ol style="list-style-type: none"><li>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>.<br/><br/>Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>ENABLED</code>.<br/><br/>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS de su cuenta.</li><li>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configura</li></ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>ción de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'</pre> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad                                              | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de todos los clústeres de EKS con exclusión de algunos de ellos (mediante una etiqueta de exclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es <code>GuardDutyManaged -false</code>. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <code>ec2:CreateTags</code> por <code>eks:TagResource</code> .</li> <li>• Sustituya <code>ec2:DeleteTags</code> por <code>eks:UntagResource</code> .</li> <li>• Reemplace <code>access-project</code> por <code>GuardDutyManaged</code></li> <li>• <code>123456789012</code> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de <code>PrincipalArn</code> :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>3.</p> <div data-bbox="716 254 1507 667"> <p> <b>Note</b></p> <p>Añada siempre la etiqueta de exclusión a su clúster de EKS antes de establecer el valor STATUS de EKS_RUNTIME_MONITORING en ENABLED; de lo contrario, el agente de GuardDuty seguridad se desplegará en todos los clústeres de EKS de su cuenta.</p> </div> <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como ENABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que no se hayan excluido de la supervisión.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el ejemplo siguiente se habilita EKS_RUNTIME_MONITORING y EKS_ADDON_MANAGEMENT :</p> <div data-bbox="716 1749 1507 1879"> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONIT</pre> </div> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                              |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <pre>ORING", "Status" : " <i>ENABLED</i>", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " <i>ENABLED</i>"}] }]'</pre> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad               | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supervisión de determinados clústeres de EKS (mediante una etiqueta de inclusión) | <ol style="list-style-type: none"> <li>1. Agregue una etiqueta al clúster de EKS que desee excluir de la supervisión. El par de clave-valor es GuardDutyManaged -true. Para obtener más información sobre cómo agregar la etiqueta, consulte <a href="#">Uso de etiquetas mediante la CLI, la API o eksctl</a> en la Guía del usuario de Amazon EKS.</li> <li>2. Para evitar la modificación de las etiquetas, excepto por parte de entidades de confianza, utilice la política que se proporciona en <a href="#">Impedir que las etiquetas se modifiquen excepto por entidades autorizadas</a> en la Guía del usuario de AWS Organizations . En esta política, sustituya los detalles siguientes: <ul style="list-style-type: none"> <li>• Sustituya <i>ec2:CreateTags</i> por eks:TagResource .</li> <li>• Sustituya <i>ec2&gt;DeleteTags</i> por eks:UntagResource .</li> <li>• Reemplace <i>access-project</i> por GuardDutyManaged</li> <li>• <i>123456789012</i> Sustitúyalo por el Cuenta de AWS ID de la entidad de confianza.</li> </ul> <p>Si tiene más de una entidad de confianza, utilice el siguiente ejemplo para agregar varios valores de PrincipalArn :</p> <pre>"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]</pre> </li> <li>3. Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto</li> </ol> |

| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     | <p>features como EKS_RUNTIME_MONITORING y el estado como ENABLED.</p> <p>Establezca el estado de EKS_ADDON_MANAGEMENT como DISABLED.</p> <p>GuardDuty gestionará el despliegue y las actualizaciones del agente de seguridad para todos los clústeres de Amazon EKS que se hayan etiquetado con el true par GuardDutyManaged -.</p> <p>Como alternativa, puede utilizar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectorsAPI</a>.</p> <p>En el siguiente ejemplo se habilita EKS_RUNTIME_MONITORING y se deshabilita EKS_ADDON_MANAGEMENT :</p> <pre data-bbox="716 1224 1507 1505">aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'</pre> |



| Enfoque preferido para administrar el agente GuardDuty de seguridad | Pasos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administración manual del agente de seguridad                       | <ol style="list-style-type: none"> <li> <p>Ejecute la API <a href="#">updateDetector</a> con su propio ID de detector regional y pase el nombre del objeto <code>features</code> como <code>EKS_RUNTIME_MONITORING</code> y el estado como <code>ENABLED</code>.</p> <p>Establezca el estado de <code>EKS_ADDON_MANAGEMENT</code> como <code>DISABLED</code>.</p> <p>Como alternativa, puede usar el AWS CLI comando utilizando su propio ID de detector regional. Para encontrar el <code>detectorId</code> correspondiente a su cuenta y región actual, consulte la página de configuración de la <a href="https://console.aws.amazon.com/guardduty/console">https://console.aws.amazon.com/guardduty/console</a> o ejecute la <a href="#">ListDetectors</a> API.</p> <p>En el siguiente ejemplo se habilita <code>EKS_RUNTIME_MONITORING</code> y se deshabilita <code>EKS_ADDON_MANAGEMENT</code> :</p> <pre>aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "DISABLED"}] ]'</pre> </li> <li> <p>Para administrar el agente de seguridad, consulte <a href="#">Administrar manualmente el agente de seguridad para el clúster de Amazon EKS</a>.</p> </li> </ol> |

## Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución

Con el lanzamiento de GuardDuty Runtime Monitoring, la cobertura de detección de amenazas se ha ampliado a los contenedores de Amazon ECS y a las instancias de Amazon EC2. La experiencia

de Supervisión en tiempo de ejecución de EKS se ha consolidado ahora en Supervisión en tiempo de ejecución. Puede habilitar Runtime Monitoring y administrar agentes de GuardDuty seguridad individuales para cada tipo de recurso (instancia de Amazon EC2, clúster de Amazon ECS y clúster de Amazon EKS) cuyo comportamiento en tiempo de ejecución desee supervisar.

GuardDuty ha consolidado la experiencia de consola de EKS Runtime Monitoring en Runtime Monitoring. GuardDuty recomienda [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#) y [Migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución](#).

Como parte de la migración a la Supervisión en tiempo de ejecución, asegúrese de [Desactivar la Supervisión en tiempo de ejecución de EKS](#). Esto es crucial porque, si en el futuro decide desactivar la Supervisión en tiempo de ejecución pero no desactiva la Supervisión en tiempo de ejecución de EKS, no dejará de incurrir en costos asociados al uso de esta última.

Para migrar de la Supervisión en tiempo de ejecución de EKS a la Supervisión en tiempo de ejecución

1. La GuardDuty consola es compatible con EKS Runtime Monitoring como parte de Runtime Monitoring.

Para comenzar a utilizar la Supervisión en tiempo de ejecución, puede [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#) de la organización y las cuentas.

Asegúrese de no desactivar la Supervisión en tiempo de ejecución de EKS antes de habilitar la Supervisión en tiempo de ejecución. Si desactiva la Supervisión en tiempo de ejecución de EKS, también se desactivará la administración del complemento de Amazon EKS. Siga los pasos que se indican a continuación en el mismo orden.

2. Asegúrese de cumplir todos los [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#).
3. Habilite la Supervisión en tiempo de ejecución. Para hacerlo, replique los mismos ajustes de configuración de la organización que utiliza para la Supervisión en tiempo de ejecución de EKS. Para obtener más información, consulte [Habilitación de la supervisión en tiempo de ejecución](#).
  - Si tiene una cuenta independiente, debe habilitar la Supervisión en tiempo de ejecución.

Si su agente de GuardDuty seguridad ya está desplegado, los ajustes correspondientes se replican automáticamente y no es necesario volver a configurarlos.

- Si una organización utiliza la configuración de habilitación automática, asegúrese de replicar la misma configuración de habilitación automática para la Supervisión en tiempo de ejecución.
  - Si tiene una organización con ajustes configurados individualmente para las cuentas de los miembros activos existentes, asegúrese de habilitar Runtime Monitoring y configurar el agente de GuardDuty seguridad para estos miembros de forma individual.
4. Una vez que se haya asegurado de que la configuración de Runtime Monitoring y del agente de GuardDuty seguridad es correcta, [desactive EKS Runtime Monitoring](#) mediante la API o el AWS CLI comando.
  5. (Opcional) si desea limpiar cualquier recurso asociado al agente GuardDuty de seguridad, consulte [Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución](#).

Si desea continuar con el uso de la Supervisión en tiempo de ejecución de EKS sin activar la Supervisión en tiempo de ejecución, consulte [Supervisión del tiempo de ejecución de EKS en GuardDuty](#). En función de su caso de uso, elija los pasos para configurar la Supervisión en tiempo de ejecución de EKS para una cuenta independiente o para varias cuentas de miembro.

## Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS

Utilice las siguientes API o AWS CLI comandos para comprobar el estado de configuración actual de EKS Runtime Monitoring.

Para comprobar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS existente en la cuenta

- Ejecute [GetDetector](#) para comprobar el estado de configuración de su propia cuenta.
- Como alternativa, puede ejecutar el siguiente comando. Para ello, utilice la AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1
```

Asegúrese de reemplazar el ID del detector de su región Cuenta de AWS y el de la región actual. Para encontrar el detectorId de tu cuenta y tu región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

Para comprobar el estado de la configuración actual de EKS Runtime Monitoring en su organización (solo como cuenta de GuardDuty administrador delegado)

- Ejecute [DescribeOrganizationConfiguration](#) para comprobar el estado de configuración de su organización.

También puede ejecutar el siguiente comando mediante la AWS CLI:

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Asegúrese de sustituir el ID del detector por el ID del detector de su cuenta de GuardDuty administrador delegado y la región por la región actual. Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

## Desactivar la Supervisión en tiempo de ejecución de EKS después de migrar a la Supervisión en tiempo de ejecución

Una vez que se haya asegurado de que la configuración existente para la cuenta u organización se ha replicado en la Supervisión en tiempo de ejecución, podrá desactivar la Supervisión en tiempo de ejecución de EKS.

Para desactivar la Supervisión en tiempo de ejecución de EKS

- Para desactivar la Supervisión en tiempo de ejecución de EKS en una cuenta propia

Ejecuta la [UpdateDetector](#) API con tu propia región *detector-id*.

Como alternativa, puedes usar el siguiente AWS CLI comando.

*12abc34d567e8fa901bc2d34e56789f0* Sustitúyalo por su propia región *detector-id*.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Para desactivar la Supervisión en tiempo de ejecución de EKS para las cuentas de miembro de la organización

Ejecute la [UpdateMemberDetectors](#) API con la región *detector-id* de la cuenta de GuardDuty administrador delegado de la organización.

Como alternativa, puede usar el siguiente AWS CLI comando.

**12abc34d567e8fa901bc2d34e56789f0** Sustitúyala por la región *detector-id* de la cuenta de GuardDuty administrador delegado de la organización y **111122223333** por el Cuenta de AWS ID de la cuenta de miembro para la que quieres deshabilitar esta función.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
"Status" : "DISABLED"}]'
```

- Para actualizar la configuración de habilitación automática de la Supervisión en tiempo de ejecución de EKS para la organización

Siga este paso únicamente si ha configurado la habilitación automática de la Supervisión en tiempo de ejecución de EKS para las cuentas nuevas (NEW) o para todas (ALL) las cuentas de miembro de la organización. Si ya ha establecido este ajuste como NONE, puede omitir este paso.

#### Note

Establecer la configuración de habilitación automática de la Supervisión en tiempo de ejecución de EKS en NONE significa que la Supervisión en tiempo de ejecución de EKS no se habilitará automáticamente para ninguna cuenta de miembro existente o cuando una nueva cuenta de miembro se una a la organización.

Ejecute la [UpdateOrganizationConfiguration](#) API con la región *detector-id* de la cuenta de GuardDuty administrador delegado de la organización.

Como alternativa, puede usar el siguiente AWS CLI comando.

**12abc34d567e8fa901bc2d34e56789f0** Sustitúyala por la regional *detector-id* de la cuenta de GuardDuty administrador delegado de la organización. Sustituya *EXISTING\_VALUE* el por su configuración actual para la activación automática GuardDuty.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
--features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
```

# GuardDuty versiones de lanzamiento del agente de seguridad

GuardDuty publica periódicamente una versión actualizada del agente. Cuando GuardDuty gestiona el agente automáticamente, GuardDuty está diseñado para actualizar el agente en su nombre. Si administra el agente manualmente, será responsable de actualizar la versión del agente para los tipos de recursos: instancias de Amazon EC2, clústeres de Amazon ECS y clústeres de Amazon EKS.

En las siguientes secciones se proporcionan las versiones de lanzamiento de los agentes de GuardDuty seguridad y las notas de versión asociadas para todos los tipos de recursos compatibles.

## Temas

- [GuardDuty versiones de agentes de seguridad para instancias de Amazon EC2](#)
- [GuardDuty versiones de agentes de seguridad para AWS Fargate \(solo Amazon ECS\)](#)
- [GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS](#)
- [Recursos adicionales: próximos pasos](#)

## GuardDuty versiones de agentes de seguridad para instancias de Amazon EC2

En la siguiente tabla se muestra el historial de versiones del agente GuardDuty de seguridad para Amazon EC2.

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                              | Fecha de disponibilidad |
|------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Versión 1.15.0                     | Versión 1.15.0     | Las nuevas capacidades del agente permiten optimizar la recopilación de eventos, lo que permite una implementación más rápida de los filtros y una mejor velocidad de detección. | 14 de mayo de 2026      |

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                                                                                                                                                                                       | Fecha de disponibilidad |
|------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|                                    |                    | Actualizaciones generales de las funciones de seguridad.                                                                                                                                                                                                                                                                                                  |                         |
| v1.9.2                             | v1.9.2             | <p>Se agregó soporte para los núcleos 6.15, 6.16, 6.17 y 6.18.</p> <p>Se ha añadido soporte para Alma Linux 9, Alma Linux 10 y SUSE Linux Enterprise Server 16. Para obtener una lista de todas las distribuciones de sistema operativo verificadas para los recursos de Amazon EC2, consulte <a href="#">Validar los requisitos de arquitectura</a>.</p> | 24 de febrero de 2026   |
| v1.9.1                             | v1.9.1             | Ajustes generales del rendimiento y actualizaciones de las funciones de seguridad.                                                                                                                                                                                                                                                                        | 10 de noviembre de 2025 |
| Versión 1.9.0                      | Versión 1.9.0      | Mejoras y ajustes generales de rendimiento.                                                                                                                                                                                                                                                                                                               | 23 de octubre de 2025   |

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                                                                                                                                  | Fecha de disponibilidad |
|------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.8.0                             | v1.8.0             | Mejoras y ajustes generales de rendimiento.                                                                                                                                                                                                                                                          | 12 de agosto de 2025    |
| v1.7.2                             | v1.7.1             | Compatibilidad mejorada para la instalación de agentes locales para distribuciones de Linux basadas en RPM.                                                                                                                                                                                          | 23 de julio de 2025     |
| v1.7.1                             | 1.7.1              | <p>Se agregó compatibilidad para Fedora 40 y Fedora 41. Para obtener una lista de todas las distribuciones de sistema operativo verificadas para los recursos de Amazon EC2, consulte <a href="#">Validar los requisitos de arquitectura</a>.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 3 de junio de 2025      |



| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                                                                                                                                                                                                                                         | Fecha de disponibilidad |
|------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.7.0                             | v1.7.0             | <p>Se agregó compatibilidad para las versiones 8.9 y 9.3 de Oracle Linux y para la versión 9.5 de Rocky Linux. Para obtener una lista de todas las distribuciones de sistema operativo verificadas para los recursos de Amazon EC2, consulte <a href="#">Validar los requisitos de arquitectura</a>.</p> <p>Resolución de ID de contenedor mejorada.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 3 de abril de 2025      |
| Versión 1.6.0                      | Versión 1.6.0      | Mejoras y ajustes generales de rendimiento.                                                                                                                                                                                                                                                                                                                                                                 | 6 de febrero de 2025    |

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                                                              | Fecha de disponibilidad  |
|------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| v1.5.0                             | v1.5.0             | <p>Se agregó soporte para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 y Ubuntu 24.04.</p> <p>Compatibilidad con instancias de ARM para resultados .../ MetadataDNSRebind .</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 20 de noviembre de 2024  |
| v1.3.1                             | v1.3.1             | Compatibilidad con resolutores de DNS personalizados.                                                                                                                                                                            | 12 de septiembre de 2024 |
| v1.3.0                             | v1.3.0             | <p>Mejoras y ajustes generales de rendimiento.</p> <p>Incluye compatibilidad para capturar señales de seguridad adicionales para futuros <a href="#">GuardDuty Tipos de búsqueda de Runtime Monitoring</a>.</p>                  | 19 de agosto de 2024     |

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                                                                                                                                                                | Fecha de disponibilidad |
|------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.2.0                             | v1.2.0             | <p>Compatible con las distribuciones del sistema operativo Ubuntu 20.04, Ubuntu 22.04, Debian 11 y Debian 12.</p> <p>Compatible con los kernel 6.5 y 6.8</p> <p>Mejoras y ajustes generales de rendimiento.</p>                                                                                                                    | 13 de junio de 2024     |
| v1.1.0                             | v1.1.0             | <p>Admite la configuración GuardDuty automática de agentes en Runtime Monitoring para instancias de Amazon EC2.</p> <p>Admite nuevas señales de seguridad y resultados publicados con el anuncio de la disponibilidad general de Runtime Monitoring para instancias de EC2.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 26 de marzo de 2024     |

| Versión para distribuidores de SSM | Versión del agente | Notas de la versión                                                                                                                                                                       | Fecha de disponibilidad |
|------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.0.2                             | v1.0.2             | Es compatible con las AMI más recientes de Amazon ECS.                                                                                                                                    | 2 de febrero de 2024    |
| v1.0.1                             | v1.0.1             | Las versiones del agente anteriores a la v1.0.2 no son compatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024.<br><br>Mejoras y ajustes generales de rendimiento. | 23 de enero de 2024     |
| v1.0.0                             | v1.0.0             | Versión inicial de la instalación RPM.<br><br>Las versiones del agente anteriores a la v1.0.2 no son compatibles con las AMI de Amazon ECS lanzadas después del 31 de enero de 2024.      | 26 de noviembre de 2023 |

GuardDuty versiones de agentes de seguridad para AWS Fargate (solo Amazon ECS)

En la siguiente tabla se muestra el historial de versiones del agente de GuardDuty seguridad de Fargate (solo en Amazon ECS).

| Versión del agente | Imagen de contenedor                                                                                                                                                                                           | Notas de la versión                                                                                                                                                                                                                                     | Fecha de disponibilidad |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Versión 1.15.0     | <p>x86_64 (AMD64):</p> <p>sha256:66446df341bee1a1e218aa46b7807d0d0470266c8f374c5dbd97efcd b8356348</p> <p>Graviton (ARM64):</p> <p>sha256:b0def2aa8cab6b2060c703f386fdb29dc4166054e0509a9362b21a6ed7f9def7</p> | <p>Las nuevas capacidades del agente permiten optimizar la recopilación de eventos, lo que permite una implementación más rápida de los filtros y una mejor velocidad de detección.</p> <p>Actualizaciones generales de las funciones de seguridad.</p> | 28 de mayo de 2026      |
| Versión 1.9.0      | <p>x86_64 (AMD64):</p> <p>sha256:fd9acaa2326f180f0ed0c5a25d8ff0a2d0498a6e900c34c68d4e973ea7fb26a8</p> <p>Graviton (ARM64):</p> <p>sha256:0b04f8c28956684e7526</p>                                              | Mejoras de seguridad y ajustes generales de rendimiento.                                                                                                                                                                                                | 28 de octubre de 2025   |

| Versión del agente | Imagen de contenedo<br>r                                                                                                                                                                                                                               | Notas de la versión                               | Fecha de disponibi<br>lidad |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-----------------------------|
|                    | 77bfd83db<br>c45afc8a4<br>3f7791fa4<br>4667b8078<br>ba48a295                                                                                                                                                                                           |                                                   |                             |
| v1.8.0             | x86_64 (AMD64):<br>sha256:44<br>25417f39e<br>38b24c1be<br>428bacad1<br>dad53e064<br>5530dcf44<br>22436353b<br>fe358e3a<br><br>Graviton (ARM64):<br>sha256:af<br>f069418fd<br>6825846f8<br>f575c4990<br>6a67c8a44<br>6d12d9ed0<br>d21ab95bd<br>0d05497b | Mejoras y ajustes<br>generales de<br>rendimiento. | 12 de agosto de 2025        |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                          | Notas de la versión                                                                                | Fecha de disponibilidad |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------|
| v1.7.0             | <p>x86_64 (AMD64):</p> <p>sha256:bf9197abdf853607e5fa392b4f97ccdd6ca56dd179be3ce8849e552d96582ac8</p> <p>Graviton (ARM64):</p> <p>sha256:56c8683c948bcd82c0dbcebf755204365ac7285994693c11717bd45f86e279c2</p> | <p>Resolución de ID de contenedor mejorada.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 04 de abril de 2025     |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                          | Notas de la versión                         | Fecha de disponibilidad |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|
| Versión 1.6.0      | <p>x86_64 (AMD64):</p> <p>sha256:c8dea71d372bc47b2f236f7a091b9a9b06bc8193c1cfe4c9346eb50f89258897</p> <p>Graviton (ARM64):</p> <p>sha256:f4032a566b90537646c2a987bef42eca1b498078ccc58a848603f877971a8dbe</p> | Mejoras y ajustes generales de rendimiento. | 6 de febrero de 2025    |



| Versión del agente | Imagen de contenedor                                                                                                                                                                                           | Notas de la versión                                                                                                                 | Fecha de disponibilidad |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.5.0             | <p>x86_64 (AMD64):</p> <p>sha256:5e6fdc41f9e6b748219d0498cd6c1dba6a19d875daec50167a0ac80e5028eac54</p> <p>Graviton (ARM64):</p> <p>sha256:d56801ff6864d6014740103b70b1c38431851358d182613bede20fe21090e734</p> | <p>Compatibilidad con tareas de ARM para resultados .../ MetadataDNSRebind .</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 14 de noviembre de 2024 |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                          | Notas de la versión                                                                                 | Fecha de disponibilidad |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-------------------------|
| v1.4.1             | <p>x86_64 (AMD64):</p> <p>sha256:ef36a11151ec2d3d7db22273bfb954750dee76f0ac7bec37a7ba7e74c3de1c78</p> <p>Graviton (ARM64):</p> <p>sha256:a8844544a59d6b4cba98f8e528b513ac2d97432f208e3ad497cc16b331aa9faa</p> | <p>Endurecimiento de imágenes de contenedor.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 24 de octubre de 2024   |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                  | Notas de la versión                                   | Fecha de disponibilidad  |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|--------------------------|
| v1.3.1             | <div><div>x86_64 (AMD64):</div><div>sha256:a6e2307d796e2875907bc4c1c69622c906f3192ddc42ef27b99e0a8f0979f3e0</div><div>Graviton (ARM64):</div><div>sha256:ad1b6539d806edb504f17e6bcfb8b4026c5e822300afc31c0d23c6a08f9b99e9</div></div> | Compatibilidad con resolutores de DNS personalizados. | 11 de septiembre de 2024 |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                         | Notas de la versión                                                                                                                                                                                                       | Fecha de disponibilidad |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.3.0             | <p>x86_64 (AMD64):</p> <p>sha256:f1ad3fb2dc55a1110c60eecf4453b9f9c02f29acb261df39814e7d29296bf831</p> <p>Graviton (ARM64):</p> <p>sha256:ff81a755d46681e409f55a95beeda9ebbcf5336e1c0b1e6348af7c6518bdbb1</p> | <p>Mejoras y ajustes generales de rendimiento.</p> <p>Incluye compatibilidad para capturar señales de seguridad adicionales para futuros GuardDuty <a href="#">GuardDuty Tipos de búsqueda de Runtime Monitoring</a>.</p> | 9 de agosto de 2024     |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                                                | Notas de la versión                         | Fecha de disponibilidad |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|
| v1.2.0             | <p>x86_64 (AMD64):</p> <p>sha256:1d<br/>bad20ac2d<br/>c66d52d00<br/>bb28dde42<br/>81fe0d3c5<br/>f261b1649<br/>b247c2369<br/>d9e26b93</p> <p>Graviton (ARM64):</p> <p>sha256:91<br/>930f8446f<br/>5f95b93b8<br/>ccb187739<br/>92affa401<br/>eb3f42da8<br/>9d68077a5<br/>6bafa6cd</p> | Mejoras y ajustes generales de rendimiento. | 31 de mayo de 2024      |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                           | Notas de la versión                                                                                        | Fecha de disponibilidad |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------|
| v1.1.0             | <p>x86_64 (AMD64):</p> <p>sha256:83ce3cf2ef85a349ed1797a8cf30a008ac5d8c9f673f2835823957e9dcf71657</p> <p>Graviton (ARM64):</p> <p>sha256:0d4b61648d7bdeab8ab8d94684f805498927c7d437d318204dccccfe8c9383dc7</p> | <p>Admite nuevas señales y resultados de seguridad.</p> <p>Mejoras y ajustes generales de rendimiento.</p> | 1 de mayo de 2024       |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                          | Notas de la versión                         | Fecha de disponibilidad |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|
| v1.0.1             | <p>x86_64 (AMD64):</p> <p>sha256:9f8cd438fb66f62d09bfc641286439f7ed5177988a314a6021ef4ff880642e68</p> <p>Graviton (ARM64):</p> <p>sha256:82c66bb615bd0d1e96db77b1f1fb51dc03220caa593b1962249571bf7147d1b7</p> | Mejoras y ajustes generales de rendimiento. | 26 de enero de 2024     |

| Versión del agente | Imagen de contenedor                                                                                                                                                                           | Notas de la versión                                                                   | Fecha de disponibilidad |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------------------------|
| v1.0.0             | x86_64 (AMD64):<br>sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017<br><br>Graviton (ARM64):<br>sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984 | Versión inicial del agente de GuardDuty seguridad para AWS Fargate (solo Amazon ECS). | 26 de noviembre de 2023 |

## GuardDuty versiones de agentes de seguridad para los recursos de Amazon EKS

GuardDuty publica periódicamente una versión actualizada del agente. Cuando GuardDuty gestiona el agente automáticamente, está diseñado para gestionar las actualizaciones del agente en su nombre. Si administra el agente de manera manual, es responsable de actualizar la versión del agente para los clústeres de Amazon EC2.

Antes de actualizar el agente a una versión específica, añada el registro de imágenes GuardDuty al `allowed-container-registries` controlador de admisión. Para obtener más información, consulte [Agente de alojamiento GuardDuty de repositorios Amazon ECR](#).

En la siguiente tabla se muestra el historial de versiones del [GuardDuty agente complementario Amazon EKS](#).



| Versión del agente | Imagen de contenedor                                                                                                                                                                                  | Notas de la versión                                                                                                                                                                                                                              | Fecha de disponibilidad | Finalización del soporte estándar <a href="#">1</a> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| Versión 1.15.0     | x86_64<br>(AMD64):<br>sha256:512642a5f9d9a316aa9100368acfdbae2481be7a5cfe9929571c1bb6e19c66fe<br><br>Graviton<br>(ARM64):<br>sha256:f017e755615ae999fe5f163886f681508e8f53f6ea7e64e7ada733cde9db368d8 | Las nuevas capacidades del agente permiten optimizar la recopilación de eventos, lo que permite una implementación más rápida de los filtros y una mejor velocidad de detección.<br><br>Actualizaciones generales de las funciones de seguridad. | 14 de mayo de 2026      | –                                                   |
| v1.12.2            | x86_64<br>(AMD64):<br>sha256:06c25ab9ffff7ee93048e5f34148c96273663235937199b4bd2e28b5ee2e5c080                                                                                                        | Actualizaciones generales de las funciones de seguridad.                                                                                                                                                                                         | 26 de marzo de 2026     | –                                                   |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                        | Notas de la versión                                                                | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
|                    | Graviton<br>(ARM64):<br>sha256:f8<br>9962d9713<br>50ff6ab40<br>8cf6ec7bc<br>a9dd06152<br>f0172b7f9<br>c68ae770c<br>c0fc4598                                                                                                                                 |                                                                                    |                         |                                                            |
| v1.12.1            | x86_64<br>(AMD64):<br>sha256:f2<br>9a597745e<br>5acff4880<br>9bebac7d8<br>091bbc382<br>29453dd26<br>710c549b8<br>17362491<br><br>Graviton<br>(ARM64):<br>sha256:08<br>9cebd7e8<br>91177e107<br>a099c9a4e<br>362d9d74b<br>5362cd374<br>b448a1607<br>8040f6c6 | Ajustes generales del rendimiento y actualizaciones de las funciones de seguridad. | 17 de noviembre de 2025 | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                | Notas de la versión                                                                                                                                                                                                                                                                   | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.11.0            | x86_64<br>(AMD64):<br>sha256:7c398fd50de5fe493c361aa7fe191e094ddfa000c65b449a9ed6a5cd53610e7<br><br>Graviton<br>(ARM64):<br>sha256:98a547b47d4770f45e75eb9730c807d9265722ca2f391e0aa5cb19e487ab455f | Se agregó compatibilidad para las distribuciones de sistemas operativos Fedora 40 y Fedora 41.<br><br>Para obtener más información, consulte <a href="#">Validación de los requisitos de arquitectura</a> (para EKS).<br><br>Mejoras de seguridad y ajustes generales de rendimiento. | 29 de agosto de 2025    | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                         | Notas de la versión                                                                                        | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.10.0            | x86_64<br>(AMD64):<br>sha256:6d<br>cbe5b055e<br>1ef0af903<br>071ede0b0<br>8f755ad5b<br>7e9774a67<br>df5399efd<br>aa1f3d7d<br><br>Graviton<br>(ARM64):<br>sha256:f0<br>536882268<br>9610a4bab<br>543abf93d<br>3e070b1b5<br>59e62a2e6<br>7d82dfa98<br>37600f72 | Resolución de ID<br>de contenedor<br>mejorada.<br><br>Mejoras<br>y ajustes<br>generales de<br>rendimiento. | 04 de abril de 2025     | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                 | Notas de la versión                         | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|------------------------------------------------------------|
| Versión 1.9.0      | x86_64<br>(AMD64):<br>sha256:51c5789ef6570f9bec879ac48a8f4769718cbc31e45430032569917e219af63f<br><br>Graviton<br>(ARM64):<br>sha256:9c2f74e7ea0827b7e422ae4c91fffc6c2bc41a1cdb96c7191d05259d337154e1 | Mejoras y ajustes generales de rendimiento. | 02 de marzo de 2025     | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                | Notas de la versión                                                                                                                                                                                                         | Fecha de disponibilidad | Finalización del soporte estándar <a href="#">1</a> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| v1.8.1             | x86_64<br>(AMD64):<br>sha256:f2ce8cf89db<br>e17e3388c<br>ecb350535<br>44dadf21a<br>f7770545f<br>8d4b50384<br>076aff47<br><br>Graviton<br>(ARM64):<br>sha256:30f586e4b69<br>4e704bcaf<br>adfa9081a<br>b0aef3cf<br>bcde39743<br>a0f1e24f7<br>7d79627f | Se agregó soporte para CentOS Stream 9.0, RedHat 9.4, Fedora 34.0 y Ubuntu 24.04.<br><br>Compatibilidad con instancias de ARM para resultados<br>.../MetadataDNSRebind .<br><br>Mejoras y ajustes generales de rendimiento. | 23 de noviembre de 2024 | –                                                   |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                 | Notas de la versión                                                                                                                                                                                                                                                           | Fecha de disponibilidad  | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------------------------------|
| v1.7.1             | x86_64<br>(AMD64):<br>sha256:b8b86b5d0872c8b67fecf64ec3d172666360545435a1752447d510951a7fd749<br><br>Graviton<br>(ARM64):<br>sha256:40ac4cfc354fd430ba7897ca1632e9a500ed13eeb0c315c5bcad38680e76b6e9 | Mejoras y ajustes generales de rendimiento.<br><br>Incluye compatibilidad para capturar señales de seguridad adicionales para futuros <a href="#"><u>GuardDuty Tipos de búsqueda de Runtime Monitoring</u></a> .<br><br>Compatibilidad con resolutores de DNS personalizados. | 13 de septiembre de 2024 | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                       | Notas de la versión                                                                                                                                                                                             | Fecha de disponibilidad | Finalización del soporte estándar <sup>1</sup> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------|
| v1.7.0             | <p>x86_64</p> <p>(AMD64):</p> <p>sha256:f3a2a8806e6c2a7fd63a91cccf6f7dffc7e68554a423d610cea8c7e8f2185ec</p> <p>Graviton</p> <p>(ARM64):</p> <p>sha256:b1a6db35a072c0de3c695e5e909a03e6c4e1fdbe47ecfaeb2784435cf67ebe0a</p> | <p>Mejoras y ajustes generales de rendimiento.</p> <p>Incluye compatibilidad para capturar señales de seguridad adicionales para futuros <a href="#">GuardDuty Tipos de búsqueda de Runtime Monitoring</a>.</p> | 17 de agosto de 2024    | –                                              |



| Versión del agente | Imagen de contenedor                                                                                                                                                                                                 | Notas de la versión                         | Fecha de disponibilidad | Finalización del soporte estándar <a href="#">1</a> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|-----------------------------------------------------|
| v1.6.1             | <p>x86_64<br/>(AMD64):<br/>sha256:30650708a6601f6d6b9046f54b30f5fd65af296b1e40b8c24426b9bd<br/>b07c3ab1</p> <p>Graviton<br/>(ARM64):<br/>sha256:5f637c42ffb306b20f776d9d83e1e0b4be40ce245be44afcf43a8902b4d71019</p> | Mejoras y ajustes generales de rendimiento. | 14 de mayo de 2024      | –                                                   |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                                                  | Notas de la versión                                                                                                                                                                                                                                                                                                                                                                                                                                                | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| Versión 1.6.0      | <p>x86_64<br/>(AMD64):<br/>sha256:7d<br/>abcb3e30d<br/>8b0536767<br/>52fbc19e8<br/>9f77272d9<br/>a6a53cc93<br/>731f58721<br/>80ef9010</p> <p>Graviton<br/>(ARM64):<br/>sha256:97<br/>10f53afcc<br/>df4f22b26<br/>5a1a6fc27<br/>f1469403a<br/>f1f7d5d08<br/>c4869a726<br/>9cdd2650</p> | <ul style="list-style-type: none"> <li>• Admite la configuración GuardDuty automatizada de agentes para EKS/EC2 los recursos.</li> <li>• Admite nuevas señales y resultados de seguridad. Para obtener más información, consulte <a href="#">Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty</a> y <a href="#">GuardDuty Tipos de búsqueda de Runtime Monitoring</a>.</li> <li>• Mejoras y ajustes generales de rendimiento.</li> </ul> | 29 de abril de 2024     | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                 | Notas de la versión                                                                                                                                                                                                                                                                                                    | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.5.0             | x86_64<br>(AMD64):<br>sha256:e09a4e70af4058a212f172cc8eb3fc23ad9bed547ed609faa2bb82cf7cc5532d<br><br>Graviton<br>(ARM64):<br>sha256:afc9a3f8f17ae12499d76069efcf1b46271a5a4b2b3f6ba5de54637b8f55d5c6 | <ul style="list-style-type: none"> <li>• Mejoras y ajustes generales de rendimiento.</li> <li>• Mejoras de seguridad , incluidos nuevos tipos de eventos en <a href="#"><u>Tipos de eventos de tiempo de ejecución recopilados</u></a>.</li> <li>• Mejoras de rendimiento en relación con el uso de la CPU.</li> </ul> | 7 de marzo de 2024      | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                 | Notas de la versión                         | Fecha de disponibilidad | Finalización del soporte estándar <a href="#">1</a> |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------|-----------------------------------------------------|
| v1.4.1             | <p>x86_64<br/>(AMD64):<br/>sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c</p> <p>Graviton<br/>(ARM64):<br/>sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dff<br/>e0792c9e6d0778b40</p> | Mejoras y ajustes generales de rendimiento. | 16 de enero de 2024     | –                                                   |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                             | Notas de la versión                                                                                                                                                                                                                  | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.4.0             | <p>x86_64<br/>(AMD64):<br/>sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f</p> <p>Graviton<br/>(ARM64):<br/>sha256:0c650aeafee b5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e</p> | <p>El punto de montaje del manifiesto admite una mejor recopilación de datos</p> <p>AppArmor configuración en el manifiesto</p> <p>Argumento recopilar de la línea de comandos</p> <p>Mejoras y ajustes generales de rendimiento</p> | 21 de diciembre de 2023 | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                         | Notas de la versión                                    | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.3.1             | x86_64<br>(AMD64):<br>sha256:55<br>578fcb7b7<br>3097ade5c<br>8404390ef<br>16cf76a7b<br>568490aba<br>ae01ac759<br>92b3ea29<br><br>Graviton<br>(ARM64):<br>sha256:e3<br>ce8d66ac2<br>121f8d476<br>eb58f8bc5<br>0ab513366<br>47615eb7c<br>f514c2142<br>1cb818fd | Actualizaciones y revisiones de seguridad importantes. | 23 de octubre de 2023   | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                                                                         | Notas de la versión                                                                                                                               | Fecha de disponibilidad | Finalización del soporte estándar <a href="#"><u>1</u></a> |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------|
| v1.3.0             | x86_64<br>(AMD64):<br>sha256:6d<br>ace2337df<br>bb7609811<br>be89fb4b2<br>3ae0b865f<br>1027ad78f<br>be69530bf<br>bd46c694<br><br>Graviton<br>(ARM64):<br>sha256:49<br>28a7c6ef4<br>0e77c8ec9<br>5841323bb<br>9a110db31<br>f12c0ee7a<br>b965e08b4<br>3efd01bb | Compatible con la plataforma Ubuntu<br><br>Compatible con la versión 1.28 de Kubernetes<br><br>Mejoras generales de rendimiento y de estabilidad. | 5 de octubre de 2023    | –                                                          |

| Versión del agente | Imagen de contenedor                                                                                                                                                                                 | Notas de la versión                                                                                                                                                                                                                                                                  | Fecha de disponibilidad | Finalización del soporte estándar <a href="#">1</a> |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------|
| v1.2.0             | x86_64<br>(AMD64):<br>sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3<br><br>Graviton<br>(ARM64):<br>sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa | Además de las AMD64-based instancias, la versión 1.2.0 ahora también admite ARM64-based instancias. Se ha agregado compatibilidad con Bottlerocket y se ha verificado.<br><br>Compatible con la versión 1.27 de Kubernetes<br><br>Mejoras generales de rendimiento y de estabilidad. | 16 de junio de 2023     | –                                                   |



| Versión del agente | Imagen de contenedor                                                    | Notas de la versión                                                                                                                                                                                                                                 | Fecha de disponibilidad | Finalización del soporte estándar <sup>1</sup> |
|--------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------|
| v1.1.0             | sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c | Además de las <a href="#">Versiones de Kubernetes compatibles con el agente de seguridad GuardDuty</a> , esta versión del agente también es compatible con la versión 1.26 de Kubernetes.<br><br>Mejoras generales de rendimiento y de estabilidad. | 2 de mayo de 2023       | 14 de mayo de 2024                             |
| v1.0.0             | sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e | Versión inicial del agente del complemento de Amazon EKS.                                                                                                                                                                                           | 30 de marzo de 2023     | 14 de mayo de 2024                             |

<sup>1</sup>Para obtener información sobre cómo actualizar la versión actual del agente que está a punto de finalizar su soporte estándar, consulte [Actualizar manualmente el agente de seguridad para los recursos de Amazon EKS](#).

## Recursos adicionales: próximos pasos

Para obtener más información sobre los próximos pasos, consulte los siguientes temas:

- [Requisitos previos para habilitar la Supervisión en tiempo de ejecución](#): con las nuevas versiones de los agentes, es posible que se actualice la sección de requisitos previos. Verifique y valide que sus recursos cumplen los requisitos previos más recientes.
- [Administrar agentes GuardDuty de seguridad](#): si administra el agente manualmente, es responsable de administrar las actualizaciones de la versión del agente que se ejecuta en sus recursos. Según el tipo de recurso (Amazon EKS o Amazon EC2-Amazon ECS), lleve a cabo los pasos para actualizar el agente de seguridad. Asegúrese también de validar la [configuración de punto de conexión de VPC](#).
- [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#): una vez que haya actualizado el agente de seguridad, podrá evaluar la cobertura de tiempo de ejecución de su recurso. Si hay algún problema de cobertura, siga los pasos de solución de problemas asociados.

## Desactivar, desinstalar y limpiar recursos en la Supervisión en tiempo de ejecución

Esta sección se aplica Cuenta de AWS si decide deshabilitar Runtime Monitoring o solo la configuración GuardDuty automática del agente para un tipo de recurso.

### Deshabilitar la configuración GuardDuty automática de agentes

GuardDuty no elimina el agente de seguridad que está desplegado en el recurso. Sin embargo, GuardDuty dejará de administrar las actualizaciones del agente de seguridad.

GuardDuty sigue recibiendo los eventos de tiempo de ejecución de su tipo de recurso. Para evitar que sus estadísticas de uso se vean afectadas, asegúrese de eliminar el agente de GuardDuty seguridad del recurso.

Ya sea que Cuenta de AWS utilice o no un punto de enlace de VPC compartido, GuardDuty no elimina el punto de enlace de VPC. Si es necesario, tendrá que eliminar el punto de conexión de VPC manualmente.

### Desactivar la Supervisión en tiempo de ejecución y la Supervisión en tiempo de ejecución de EKS

Esta sección se aplica en los siguientes casos:

- Nunca habilitó la Supervisión en tiempo de ejecución de EKS por separado y ahora desactivó la Supervisión en tiempo de ejecución.
- Va a desactivar tanto la Supervisión en tiempo de ejecución como la Supervisión en tiempo de ejecución de EKS. Si no está seguro del estado de configuración de la Supervisión en tiempo de ejecución de EKS, consulte [Verificar el estado de la configuración de la Supervisión en tiempo de ejecución de EKS](#).

**i** Desactivar la Supervisión en tiempo de ejecución sin desactivar la Supervisión en tiempo de ejecución de EKS

En este caso, en algún momento, habilitó la Supervisión en tiempo de ejecución de EKS y, posteriormente, también habilitó la Supervisión en tiempo de ejecución sin desactivar la Supervisión en tiempo de ejecución de EKS.

Ahora, al desactivar la Supervisión en tiempo de ejecución, también deberá desactivar la Supervisión en tiempo de ejecución de EKS; de lo contrario, no dejará de incurrir en gastos por el uso de la Supervisión en tiempo de ejecución de EKS.

Si se dan las situaciones enumeradas anteriormente, GuardDuty realizará las siguientes acciones en su cuenta:

- GuardDuty elimina el punto final de la VPC que tiene GuardDutyManaged la `true` etiqueta:. Esta es la VPC que se GuardDuty creó para administrar el agente de seguridad automatizado.
- GuardDuty elimina el grupo de seguridad que estaba etiquetado como GuardDutyManaged:. `true`
- En el caso de una VPC compartida que haya sido utilizada por al menos una cuenta participante, GuardDuty no se elimina el punto final de la VPC ni el grupo de seguridad asociado al recurso de VPC compartido.
- En el caso de un recurso de Amazon EKS, GuardDuty elimina el agente de seguridad. Esto es independiente de si se administra de forma manual o automática. GuardDuty

En el caso de un recurso de Amazon ECS, dado que una tarea de ECS es inmutable, no GuardDuty se puede desinstalar el agente de seguridad de ese recurso. Esto es independiente de cómo administre el agente de seguridad, ya sea de forma manual o automática. GuardDuty Después de deshabilitar Runtime Monitoring, no GuardDuty conectará un contenedor lateral cuando comience a ejecutarse una nueva tarea de ECS. Para obtener información sobre cómo trabajar con Fargate-ECS tareas, consulte [Cómo funciona la supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

En el caso de un recurso de Amazon EC2, GuardDuty desinstala el agente de seguridad de todas las instancias de Amazon EC2 gestionadas por Systems Manager (SSM) únicamente cuando cumpla las siguientes condiciones:

- El recurso no está etiquetado con la etiqueta de exclusión `GuardDutyManaged:false`.
- GuardDuty debe tener permisos para acceder a las etiquetas de los metadatos de la instancia. Para este recurso de EC2, el Acceso a etiquetas en metadatos de instancia está establecido en Permitir.

Al dejar de administrar manualmente el agente de seguridad

Independientemente del enfoque que utilice para implementar y administrar el agente de GuardDuty seguridad, para dejar de monitorear los eventos de tiempo de ejecución en su recurso, debe eliminar el agente GuardDuty de seguridad. Cuando desee dejar de supervisar los eventos en tiempo de ejecución de un tipo de recurso en una cuenta, también puede eliminar el punto de conexión de Amazon VPC.

## Desinstalar manualmente el agente de seguridad para los recursos de Amazon EC2

En esta sección se proporcionan métodos para desinstalar el agente de GuardDuty seguridad de los recursos de Amazon EC2. Cuando administra el agente de seguridad manualmente, es responsable de eliminarlo de los recursos. GuardDuty no realizará ninguna acción con respecto a los recursos que usted administra.

Si creó un punto de conexión de Amazon VPC manualmente, después de desinstalar el agente de seguridad en todos los tipos de recursos supervisados de la cuenta, podrá optar por eliminar el punto de conexión de VPC. Se trata de un paso separado. Para obtener más información, consulte [To delete a VPC endpoint](#).

En función de cómo haya instalado el agente de seguridad en el recurso, elija uno de los siguientes métodos para desinstalarlo.

### Temas

- [Método 1: mediante el Comando de ejecución](#)
- [Método 2: mediante administradores de paquetes de Linux](#)

## Método 1: mediante el Comando de ejecución

Si instaló el agente de seguridad con [Método 1: usar AWS Systems Manager](#), siga estos pasos para desinstalarlo:

Para desinstalar el agente GuardDuty de seguridad

1. Puede desinstalar el agente de GuardDuty seguridad siguiendo los pasos que se especifican en la sección [AWS Systems Manager Ejecutar comando](#) de la Guía del AWS Systems Manager usuario. Utilice la acción Desinstalar en los parámetros para desinstalar el agente GuardDuty de seguridad.

En la sección Destinos, asegúrese de que el impacto se produce únicamente en las instancias de Amazon EC2 de las que desea desinstalar el agente de seguridad.

Utilice el siguiente GuardDuty documento y distribuidor:

- Nombre del documento: AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin
  - Distributor: AmazonGuardDuty-RuntimeMonitoringSsmPlugin
2. Después de proporcionar todos los detalles, cuando elija Ejecutar, se eliminará el agente de seguridad que implementó en las instancias de Amazon EC2 de destino.

Para eliminar la configuración del punto de conexión de Amazon VPC, debe desactivar tanto la Supervisión en tiempo de ejecución como la Supervisión en tiempo de ejecución de Amazon EKS.

3. Si también desea eliminar el punto de conexión de VPC asociado a este agente de seguridad, consulte [To delete a VPC endpoint](#).

## Método 2: mediante administradores de paquetes de Linux

Si instaló el agente de seguridad con [Método 2: utilizar administradores de paquetes de Linux](#), siga estos pasos para desinstalarlo:

Para desinstalar el agente GuardDuty de seguridad

1. Conecte con la instancia. Para conocer los pasos necesarios, consulte [Establecer conexión con la instancia de Linux mediante un cliente SSH](#) en la Guía del usuario de Amazon EC2.

## 2. Comando para la desinstalación

El siguiente comando desinstalará el agente de GuardDuty seguridad de la instancia de Amazon EC2 a la que se conecte:

- Para RPM:

```
sudo rpm -e amazon-guardduty-agent
```

- Para Debian:

```
sudo dpkg --purge amazon-guardduty-agent
```

Después de ejecutar el comando, también puede comprobar los registros asociados a este.

3. Si también desea eliminar el punto de conexión de VPC asociado a este agente de seguridad, consulte [To delete a VPC endpoint](#).

## Limpiar los recursos de los agentes de seguridad

En esta sección se explica cómo puede limpiar los AWS recursos asociados al agente de seguridad. Como se indica en [Desactivar, desinstalar y limpiar recursos](#), no GuardDuty eliminará ni quitará todos los recursos del agente de seguridad. En la siguiente sección se ofrecen instrucciones sobre cómo eliminar los recursos del agente de seguridad.

### Eliminación del punto de conexión de VPC de Amazon

Si administra el agente de seguridad manualmente, es posible que haya creado un punto de conexión de Amazon VPC manualmente. Después de desinstalar el agente de seguridad para todos los recursos supervisados en la cuenta, podrá optar por eliminar este punto de conexión de VPC.

En la siguiente lista se presentan distintos casos en los que se puede utilizar una VPC compartida en lugar de no utilizarla.

- Sin una VPC compartida: Cuando ya no desee supervisar un recurso en una cuenta, considere la posibilidad de eliminar el punto de conexión de Amazon VPC.
- Cuando una cuenta de propietario de una VPC compartida elimina el recurso de la VPC compartida que aún se utilizaba, la cobertura de la Supervisión en tiempo de ejecución (y,

cuando corresponda, de la Supervisión en tiempo de ejecución de EKS) para los recursos de la cuenta de propietario de la VPC compartida y de la cuenta participante podría pasar a estar en mal estado. Para obtener información sobre el estado de la cobertura, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para eliminar un punto de conexión de VPC, consulte [Eliminar un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

Para eliminar el grupo de seguridad

- Sin una VPC compartida: cuando ya no desee supervisar un tipo de recurso en una cuenta, considere la opción de eliminar el grupo de seguridad asociado a la Amazon VPC.
- Con una VPC compartida: cuando la cuenta de propietario de la VPC compartida elimina el grupo de seguridad, cualquier cuenta de participante que actualmente utilice el grupo de seguridad asociado a la VPC compartida, el estado de cobertura de la Supervisión en tiempo de ejecución para los recursos de la cuenta de propietario de la VPC compartida y la cuenta de participante podrían quedar en mal estado. Para obtener más información, consulte [Revisar las estadísticas de la cobertura en tiempo de ejecución y resolución de problemas](#).

Para obtener información sobre los pasos, consulte [Eliminar un grupo de seguridad de Amazon EC2](#) en la Guía del usuario de Amazon EC2.

Para eliminar el agente GuardDuty de seguridad de un clúster de EKS

Para eliminar del clúster de EKS el agente de seguridad que ya no desea supervisar, consulte [Eliminar del clúster un complemento de Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Al eliminar el agente del complemento de EKS, no se elimina el espacio de nombres amazon-guardduty del clúster de EKS. Para eliminar el espacio de nombres amazon-guardduty, consulte [Deleting a namespace](#).

Para eliminar el espacio de nombres **amazon-guardduty** (clúster de EKS)

Al desactivar la configuración automatizada del agente, no se elimina automáticamente del clúster de EKS el espacio de nombres amazon-guardduty. Para eliminar el espacio de nombres amazon-guardduty, consulte [Deleting a namespace](#).

# GuardDuty Protección contra malware para EC2

La protección contra malware para EC2 ayuda a detectar la posible presencia de malware mediante el análisis de los [volúmenes de Amazon Elastic Block Store \(Amazon EBS\)](#) que se asocian a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) y a las cargas de trabajo de contenedores que se ejecutan en Amazon EC2. La protección contra malware para EC2 ofrece opciones de análisis en las que puede decidir si desea incluir o excluir instancias específicas de Amazon EC2 en el momento del análisis. También ofrece la opción de conservar en sus cuentas las instantáneas de los volúmenes de Amazon EBS adjuntos a las instancias de Amazon EC2 o a las cargas de trabajo de contenedores. GuardDuty Las instantáneas se retienen solo cuando se encuentra malware y se generan resultados de la protección contra malware para EC2.

La protección contra malware para EC2 se diseñó de forma que no afecte al rendimiento de los recursos. Para obtener información sobre cómo funciona Malware Protection for EC2 en Internet, consulte. GuardDuty [¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?](#) Para obtener información sobre la disponibilidad de Malware Protection para EC2 en diferentes versiones Regiones de AWS, consulte. [Regiones y puntos de conexión](#)

## Notas

Malware Protection for EC2 es compatible con análisis de malware en instancias administradas para modo automático de Amazon EKS. Para obtener más información, consulte el [soporte de instancias gestionadas en Guardduty](#).

Malware Protection for EC2 no admite escaneos de malware para AWS Fargate cargas de trabajo que se ejecuten con Amazon EKS o Amazon ECS.

Para obtener más información sobre estas características de Amazon EKS, consulte [¿Qué es Amazon EKS?](#) en la Guía del usuario de Amazon EKS.

## Temas

- [Comparación entre el escaneo de GuardDuty-initiated malware y el escaneo de On-demand malware](#)
- [¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?](#)
- [Volúmenes de Amazon EBS compatibles con el análisis de malware](#)
- [Configure la retención de instantáneas y la cobertura de análisis de EC2](#)



- [GuardDuty-initiated análisis de malware](#)
- [On-demand escanea el malware GuardDuty](#)
- [Supervisión de los estados y resultados de los análisis en Malware Protection for EC2](#)
- [GuardDuty cuentas de servicio de Región de AWS](#)
- [Cuotas en la protección contra malware de EC2](#)

## Comparación entre el escaneo de GuardDuty-initiated malware y el escaneo de On-demand malware

Malware Protection for EC2 ofrece dos tipos de análisis para detectar actividades potencialmente maliciosas en sus instancias de Amazon EC2 y cargas de trabajo de contenedores GuardDuty-initiated : análisis de malware y análisis de malware On-demand . En la siguiente tabla, se muestra la comparación entre ambos tipos de análisis.

| Factor                     | GuardDuty-initiated análisis de malware                                                                                                                                                                                                                                                                                                                                                                                                                                        | On-demand análisis de malware                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cómo se invoca el análisis | Tras activar el análisis de GuardDuty-initiated malware, siempre que se GuardDuty genere un hallazgo que indique la posible presencia de malware en una instancia de Amazon EC2 o en la carga de trabajo de un contenedor, GuardDuty se inicia automáticamente un análisis de malware sin agentes en los volúmenes de Amazon EBS adjuntos al recurso potencialmente afectado. Para obtener más información, consulte <a href="#">GuardDuty-initiated análisis de malware</a> . | Puede iniciar un análisis de On-demand software malicioso proporcionando el nombre de recurso de Amazon (ARN) de su instancia de Amazon EC2. Puede iniciar un análisis de On-demand malware incluso cuando no se haya GuardDuty encontrado o nada relacionado con su recurso. Para obtener más información, consulte <a href="#">On-demand escanea el malware GuardDuty</a> . |

| Factor                                          | GuardDuty-initiated análisis de malware                                                                                                                                                                                                                                                                                                                                                                                                                                                             | On-demand análisis de malware                                                                                                                            |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se necesita configuración                       | Para utilizar el análisis de GuardDuty-initiated malware, debes habilitarlo en tu cuenta. Para administrar varias cuentas mediante un AWS Organizations método basado en invitaciones, consulte <a href="#">Habilitar la detección de GuardDuty-initiated malware en entornos con varias cuentas</a> . Para habilitar el análisis de GuardDuty-initiated malware en su propia cuenta, consulte <a href="#">Habilitar el análisis de GuardDuty-initiated malware para una cuenta independiente</a> . | Tu cuenta debe estar GuardDuty habilitada. Para utilizar el análisis de On-demand malware, no es necesaria ninguna configuración a nivel de función.     |
| Tiempo de espera para iniciar un nuevo análisis | Cada vez que se GuardDuty genera uno de ellos <a href="#">Hallazgos que invocan un análisis de GuardDuty-initiated malware</a> , un análisis de malware se inicia automáticamente solo una vez cada 24 horas.                                                                                                                                                                                                                                                                                       | Puede iniciar un análisis de On-demand malware en el mismo recurso en cualquier momento después de 1 hora desde la hora de inicio del análisis anterior. |

| Factor                                                                | GuardDuty-initiated análisis de malware                                                                                                                                                                                                                                                                                                                                                                                             | On-demand análisis de malware                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disponibilidad del periodo de prueba gratuito de 30 días <sup>1</sup> | <p>Cuando actives la detección de GuardDuty-initiated malware por primera vez en tu cuenta, podrás utilizar un período de prueba gratuito de 30 días.</p> <p>Para obtener más información, consulte <a href="#">Prueba gratuita de 30 días en GuardDuty-initiated Malware Scan</a>.</p>                                                                                                                                             | No existe un período de prueba gratuito para detectar On-demand malware en GuardDuty cuentas nuevas o existentes.                                                                                                              |
| Opciones de análisis <sup>2</sup>                                     | <p>Tras configurar el análisis de GuardDuty-initiated malware, Malware Protection for EC2 ofrece la opción de analizar u omitir recursos específicos de Amazon EC2 mediante etiquetas. La Protección contra malware para EC2 no iniciará un análisis automático de los recursos que decida excluir de este. Para obtener más información, consulte <a href="#">Opciones de análisis con etiquetas definidas por el usuario</a>.</p> | <p>Dado que usted proporciona el ARN del recurso para iniciar manualmente un análisis de malware bajo demanda, el uso de <a href="#">Opciones de análisis con etiquetas definidas por el usuario</a> no resulta aplicable.</p> |

<sup>1</sup>\*Incurrirá en costos de uso al crear y retener las instantáneas de los volúmenes de EBS. Para obtener más información sobre cómo configurar la cuenta para retener instantáneas, consulte [Retención de instantáneas](#).

<sup>2</sup> Tanto el análisis de GuardDuty-initiated malware como el análisis de On-demand malware admiten el uso de una etiqueta global para excluir los recursos de Amazon EC2 de los análisis de malware. Para obtener más información, consulte [Etiqueta GuardDutyExcluded global](#).

## ¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?

En esta sección se explica cómo Malware Protection for EC2, que incluye tanto el escaneo de GuardDuty-initiated malware como el escaneo de On-demand malware, escanea los volúmenes de Amazon EBS asociados a sus instancias de Amazon EC2 y cargas de trabajo de contenedores. Antes de continuar, tenga en cuenta las siguientes personalizaciones:

- **Opciones de análisis:** la Protección contra malware para EC2 ofrece la posibilidad de especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis. Solo el análisis de GuardDuty-initiated malware admite opciones de análisis con etiquetas definidas por el usuario. Tanto el escaneo de GuardDuty-initiated malware como el escaneo de On-demand malware admiten la GuardDutyExcluded etiqueta global. Para obtener más información, consulte [Opciones de análisis con etiquetas definidas por el usuario](#).
- **Retención de instantáneas:** Malware Protection for EC2 ofrece una opción para conservar las instantáneas de los volúmenes de Amazon EBS en su cuenta. AWS Por defecto, esta opción está desactivada. Puede optar por conservar las instantáneas tanto para los escaneos de malware GuardDuty iniciados como para los que se encuentren bajo demanda. Para obtener más información, consulte [Retención de instantáneas](#).

Cuando se GuardDuty genere una o más [Hallazgos que invocan un análisis de GuardDuty-initiated malware](#), esta actividad será motivo GuardDuty para iniciar un análisis de malware. Si sus opciones de escaneo no excluyen esta instancia, entonces GuardDuty iniciará el escaneo.

Para iniciar un análisis de On-demand malware en los volúmenes de Amazon EBS asociados a una instancia de Amazon EC2, proporcione el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2.

Como respuesta al inicio de un análisis de malware bajo demanda o un análisis automático de GuardDuty-initiated malware, GuardDuty crea instantáneas de los volúmenes de EBS pertinentes adjuntos al recurso potencialmente afectado y las comparte con el. [GuardDuty cuenta de servicio](#) Cuando GuardDuty crea una instantánea de sus volúmenes de EBS, añade una etiqueta predeterminada llamada. GuardDutyScanId Esta etiqueta ayuda a acceder GuardDuty a la

instantánea. Asegúrese de no quitar esta etiqueta. A partir de estas instantáneas, GuardDuty crea una réplica cifrada del volumen EBS en la cuenta de servicio.

Una vez finalizado el escaneo, GuardDuty elimina las réplicas cifradas de los volúmenes de EBS y las instantáneas de los volúmenes de EBS. La configuración de retención de instantáneas está desactivada de manera predeterminada. Sin embargo, las instantáneas se conservan si el [bloqueo de instantáneas de Amazon EBS](#) está habilitado para ellas, independientemente de los resultados y la configuración del escaneo. GuardDuty no puede modificar la configuración de bloqueo de instantáneas de Amazon EBS.

En la siguiente lista se describe el comportamiento de retención de las instantáneas, independientemente del bloqueo de instantáneas de EBS:

La retención de instantáneas está activada:

- Cuando encuentra malware, GuardDuty conserva las instantáneas en su. Cuenta de AWS
- Cuando no se encuentra ningún malware, GuardDuty no conserva las instantáneas a menos que estén bloqueadas.

La retención de instantáneas está desactivada (de manera predeterminada):

- Tanto si se encuentra malware como si no, las instantáneas no se retienen.
- GuardDuty no puede eliminar las instantáneas de Amazon EBS bloqueadas.

GuardDuty conservará cada volumen de réplica de EBS en la cuenta de servicio durante un máximo de 55 horas. Si se produce una interrupción del servicio o un fallo en una réplica de un volumen de EBS y en su análisis de software malicioso, GuardDuty se conservará dicho volumen de EBS durante un máximo de siete días. El período extendido de retención del volumen sirve para clasificar y solucionar la interrupción o el fallo. GuardDuty Malware Protection for EC2 eliminará las réplicas de los volúmenes de EBS de la cuenta de servicio una vez que se haya solucionado la interrupción o el fallo, o una vez transcurrido el período de retención prolongado.

Para obtener información sobre la metodología de detección de GuardDuty malware y los motores de análisis que utiliza, consulte. [GuardDuty motor de escaneo de detección de malware](#)

## Volúmenes de Amazon EBS compatibles con el análisis de malware

En todos los Regiones de AWS lugares GuardDuty compatibles con la función Malware Protection for EC2, puede escanear los volúmenes de Amazon EBS cifrados o sin cifrar. Puede tener volúmenes

de Amazon EBS cifrados con una [Clave administrada de AWS](#) o [una clave administrada por el cliente](#). Actualmente, algunas de las regiones en las que la protección contra malware para EC2 se encuentra disponible admiten ambas formas de cifrar los volúmenes de Amazon EBS, mientras que otras solo admiten la clave administrada por el cliente. Para obtener información acerca de las regiones de admitidas, consulte [GuardDuty cuentas de servicio de Región de AWS](#). Para obtener información sobre las regiones en las que GuardDuty está disponible pero la protección contra malware para EC2 no está disponible, consulte. [Region-specific disponibilidad de funciones](#)

La siguiente lista describe la clave que se GuardDuty utiliza independientemente de que los volúmenes de Amazon EBS estén cifrados o no:

- Los volúmenes de Amazon EBS que no están cifrados o cifrados con Clave administrada de AWS: GuardDuty utilizan su propia clave para cifrar las réplicas de los volúmenes de Amazon EBS.

Si la región no admite el análisis de volúmenes de Amazon EBS cifrados con el [cifrado de Amazon EBS de forma predeterminada](#), deberá modificar la clave predeterminada de modo que sea una clave administrada por el cliente. Esto ayudará a GuardDuty acceder a estos volúmenes de EBS. Al modificar la clave, incluso los futuros volúmenes de EBS se crearán con la clave actualizada para que GuardDuty puedan soportar los escaneos de malware. Para conocer los pasos a seguir para modificar la clave predeterminada, consulte [Modificar el valor predeterminado AWS KMS ID clave de un volumen de Amazon EBS](#) en la siguiente sección.

- Volúmenes de Amazon EBS cifrados con una clave administrada por el cliente: GuardDuty utilizan la misma clave para cifrar el volumen de EBS de réplica. Para obtener información sobre las políticas relacionadas con el AWS KMS cifrado compatibles, consulte. [Service-linked permisos de rol para Malware Protection for EC2](#)

## Modificar el valor predeterminado AWS KMS ID clave de un volumen de Amazon EBS

Si utiliza la opción Crear un volumen de Amazon EBS mediante el [cifrado de Amazon EBS](#) y no especifica el ID de AWS KMS clave, el volumen de Amazon EBS se cifra con una [clave de cifrado predeterminada](#). Al habilitar el cifrado de forma predeterminada, Amazon EBS cifrará automáticamente los nuevos volúmenes e instantáneas por medio de la clave de KMS predeterminada para el cifrado de Amazon EBS.

Puede modificar la clave de cifrado predeterminada y utilizar una clave administrada por el cliente para el cifrado de Amazon EBS. Esto ayudará a GuardDuty acceder a estos volúmenes de Amazon

EBS. Para modificar la ID de clave predeterminada de EBS, agregue el siguiente permiso necesario a su política de IAM: `ec2:modifyEbsDefaultKmsKeyId`. Cualquier volumen de Amazon EBS recién creado que elija cifrar, pero no especifique un ID de clave de KMS asociada, utilizará el ID de clave predeterminada. Utilice uno de los siguientes métodos para actualizar el ID de clave predeterminada de EBS:

### Modificación de la ID de clave de KMS predeterminada de un volumen de Amazon EBS

Realice una de las siguientes acciones:

- Uso de una API: puede utilizar la [ModifyEbsDefaultKmsKeyId](#) API. Para obtener información sobre cómo puede ver el estado de cifrado del volumen, consulte [Crear volumen de Amazon EBS](#).
- Uso del AWS CLI comando: el siguiente ejemplo modifica el ID de clave de KMS predeterminado que cifrará los volúmenes de Amazon EBS si no proporciona un ID de clave de KMS. Asegúrese de sustituir la región por la Región de AWS de su ID de clave KM.

```
aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-id AKIAIOSFODNN7EXAMPLE
```

El comando anterior generará un resultado similar al siguiente:

```
{
  "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
}
```

Para obtener más información, consulte [modify-ebs-default-kms-key-id](#).

## Configure la retención de instantáneas y la cobertura de análisis de EC2

En esta sección, se explica cómo personalizar las opciones de análisis de malware para las instancias de Amazon EC2. Estas personalizaciones se aplican tanto a los escaneos de On-demand malware como a los iniciados por GuardDuty. Se puede hacer lo siguiente:

- Habilitar la retención de instantáneas: si se habilita antes de un escaneo, GuardDuty retendrá la instantánea de Amazon EBS que GuardDuty se detectó como maliciosa.

- Elija qué instancias de Amazon EC2 desea analizar: utilice etiquetas para incluir o excluir instancias de Amazon EC2 específicas de los análisis de malware.

## Retención de instantáneas

GuardDuty le ofrece la opción de conservar las instantáneas de sus volúmenes de EBS en su cuenta. AWS La configuración de retención de instantáneas está desactivada de manera predeterminada. Las instantáneas solo se retendrán si ha activado esta configuración antes de que se inicie el análisis.

Cuando se inicia el escaneo, GuardDuty genera las réplicas de los volúmenes de EBS en función de las instantáneas de los volúmenes de EBS. Cuando se complete el análisis y se haya activado la configuración de conservación de instantáneas en su cuenta, las instantáneas de sus volúmenes de EBS solo se retendrán cuando se detecte malware y se genere [Tipos de resultados de la protección contra malware para EC2](#). Si no se encuentra ningún malware, borra GuardDuty automáticamente las instantáneas de los volúmenes de EBS, independientemente de la configuración de las instantáneas, a menos que se haya activado el [bloqueo de instantáneas de Amazon EBS](#) en las instantáneas creadas.

## Costo de uso de instantáneas

Durante el análisis de malware, a medida que se GuardDuty crean las instantáneas de los volúmenes de Amazon EBS, hay un coste de uso asociado a este paso. Si activa la configuración de retención de instantáneas en su cuenta, cuando se detecte malware y se conserven las instantáneas, incurrirá en costos de uso por el mismo. Para obtener información sobre el costo de las instantáneas y su retención, consulte [Precios de Amazon EBS](#).

Como cuenta de GuardDuty administrador delegado, solo usted puede realizar esta actualización en nombre de las cuentas de los miembros de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija su método de acceso preferido para activar la configuración de retención de instantáneas.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>



2. En el panel de navegación, en Planes de protección, elija Protección contra malware para EC2.
3. Elija Configuración general en la sección inferior de la consola. Para retener las instantáneas, active Retención de instantáneas.

## API/CLI

Ejecute [UpdateMalwareScanSettings](#) para actualizar la configuración actual de retención de instantáneas.

Como alternativa, puede ejecutar el siguiente AWS CLI comando para conservar automáticamente las instantáneas cuando GuardDuty Malware Protection for EC2 genere hallazgos.

Asegúrese de sustituirlo por *detector-id* el suyo válido. `detectorId`

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

Si desea desactivar la retención de instantáneas, sustituya `RETENTION_WITH_FINDING` por `NO_RETENTION`.

## Opciones de análisis con etiquetas definidas por el usuario

Al utilizar el análisis de GuardDuty-initiated malware, también puede especificar etiquetas para incluir o excluir las instancias de Amazon EC2 y los volúmenes de Amazon EBS del proceso de análisis y detección de amenazas. Puede personalizar cada análisis de GuardDuty-initiated malware editando las etiquetas de la lista de etiquetas de inclusión o exclusión. Cada lista puede incluir hasta 50 etiquetas.

Si aún no tiene etiquetas definidas por el usuario asociadas a los recursos de EC2, consulte [Etiquetar los recursos de Amazon EC2](#) en la Guía del usuario de Amazon EC2.

 Note

On-demand el análisis de malware no admite opciones de análisis con etiquetas definidas por el usuario. Es compatible con [Etiqueta GuardDutyExcluded global](#).

## Exclusión de las instancias de EC2 del análisis de malware

Si desea excluir cualquier instancia de Amazon EC2 o volumen de Amazon EBS durante el proceso de digitalización, puede configurar la GuardDutyExcluded etiqueta true para cualquier instancia de Amazon EC2 o volumen de Amazon EBS y no la escaneará. GuardDuty Para obtener más información acerca de las etiquetas de GuardDutyExcluded, consulte [Service-linked permisos de rol para Malware Protection for EC2](#). También puede agregar una etiqueta de instancia de Amazon EC2 a una lista de exclusión. Si agrega varias etiquetas a la lista de exclusión de etiquetas, cualquier instancia de Amazon EC2 que contenga al menos una de estas etiquetas se excluirá del proceso de análisis de malware.

Como cuenta de GuardDuty administrador delegado, solo usted puede realizar esta actualización en nombre de las cuentas de los miembros de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de Amazon EC2 a una lista de exclusión.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
3. Amplíe la sección de Inclusion/Exclusion etiquetas. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de exclusión y, a continuación, elija Confirmar.
5. Especifique el par **Key-Value** de la etiqueta que desee excluir. Es opcional proporcionar el **Value**. Después de agregar todas las etiquetas, elija Guardar.

 Important

Las claves y los valores de las etiquetas distinguen mayúsculas de minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

Si no se proporciona un valor para una clave y la instancia de EC2 está etiquetada con la clave especificada, esta instancia de EC2 se excluirá del proceso de análisis de GuardDuty-initiated software malicioso, independientemente del valor asignado a la etiqueta.

## API/CLI

Se ejecuta [UpdateMalwareScanSettings](#) excluyendo una instancia EC2 o una carga de trabajo de contenedor del proceso de escaneo.

El siguiente comando de AWS CLI ejemplo agrega una nueva etiqueta a la lista de etiquetas de exclusión. Sustituya el *detector-id* de ejemplo por su propio detectorId válido.

MapEquals es una lista de pares Key-Value.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Exclude": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

 Important

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

## Inclusión de las instancias de EC2 en el análisis de malware

Si desea analizar una instancia de EC2, agregue su etiqueta a la lista de inclusión. Al agregar una etiqueta a una lista de inclusión de etiquetas, las instancias de EC2 que no contengan ninguna de las etiquetas agregadas se omiten del análisis de malware. Si agrega varias etiquetas a la lista de inclusión de etiquetas, se incluirá en el análisis de malware una instancia de EC2 que contenga al menos una de esas etiquetas. A veces, es posible que se omita una instancia de EC2 durante el proceso de análisis por otros motivos. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

Como cuenta de GuardDuty administrador delegado, solo usted puede realizar esta actualización en nombre de las cuentas de los miembros de la organización. Sin embargo, si una cuenta de miembro se [administra mediante el método de invitación](#), esta podrá realizar este cambio por su cuenta. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para agregar una etiqueta asociada a una instancia de EC2 a una lista de inclusión.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
3. Amplíe la sección de Inclusion/Exclusion etiquetas. Elija Add tags (Añadir etiquetas).
4. Elija Etiquetas de inclusión y, a continuación, elija Confirmar.
5. Elija Agregar nueva etiqueta de inclusión y especifique el par de **Key** y **Value** de la etiqueta que desee incluir. Es opcional proporcionar el **Value**.

Una vez que haya agregado todas las etiquetas de inclusión, elija Guardar.

Si no se proporciona un valor para una clave y se etiqueta una instancia de EC2 con la clave especificada, la instancia de EC2 se incluirá en el proceso de análisis de protección contra malware para EC2, independientemente del valor asignado a la etiqueta.

### API/CLI

- Ejecútelo [UpdateMalwareScanSettings](#) para incluir una instancia EC2 o una carga de trabajo de contenedor en el proceso de digitalización.

El siguiente comando de AWS CLI ejemplo agrega una nueva etiqueta a la lista de etiquetas de inclusión. Asegúrese de sustituir el ejemplo *detector-id* por el suyo `validoDetectorId`. Sustituya el ejemplo *TestKey* y *TestValue* por el Value par Key y de la etiqueta asociada a su recurso de EC2.

MapEquals es una lista de pares Key-Value.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectorsAPI](#).

```
aws guardduty update-malware-scan-settings --detector-id 60b8777933648562554d637e0e4bb3b2 --scan-resource-criteria '{"Include": {"EC2_INSTANCE_TAG" : {"MapEquals": [{"Key": "TestKeyWithValue", "Value": "TestValue" }, {"Key": "TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation "RETENTION_WITH_FINDING"
```

#### Important

Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Restricciones de etiquetado](#) en la Guía del usuario de Amazon EC2.

#### Note

La detección de una nueva etiqueta puede tardar GuardDuty hasta 5 minutos.

En cualquier momento, puede elegir entre etiquetas de inclusión o etiquetas de exclusión, pero no ambas. Si quiere cambiar de una etiqueta a otra, selecciónela en el menú desplegable cuando agregue nuevas etiquetas y confirme su selección. Esta acción borra todas las etiquetas actuales.

## Etiqueta **GuardDutyExcluded** global

GuardDuty utiliza una clave de etiqueta global `GuardDutyExcluded`, que puede añadir a sus recursos de Amazon EC2 y establecer el valor de la etiqueta. `true` Este recurso de Amazon EC2 que tiene este par de clave y valor de etiqueta se excluirá del análisis de malware. Ambos tipos de

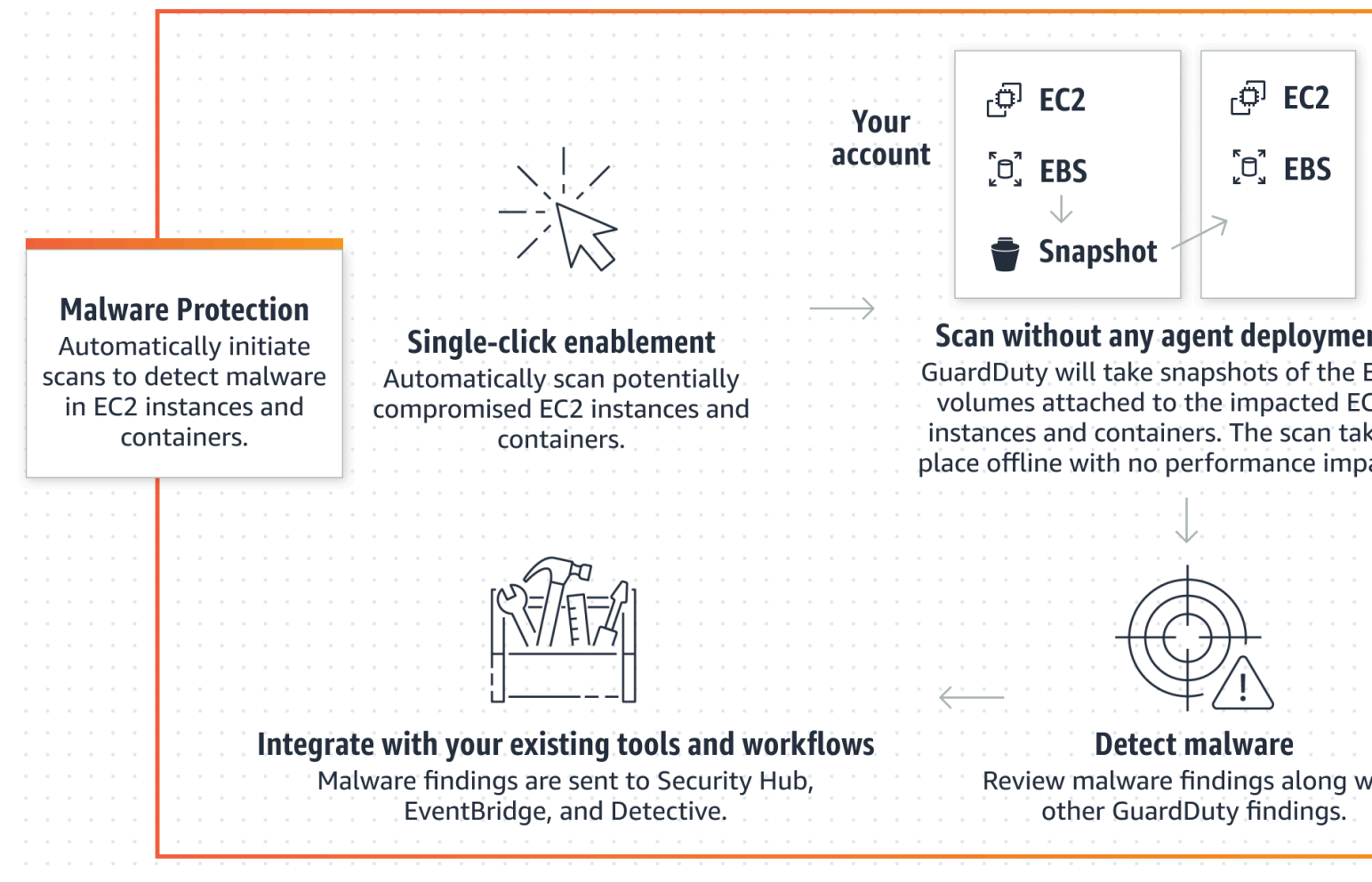
análisis (análisis de GuardDuty-initiated malware y análisis de On-demand malware) admiten la etiqueta global. Si inicia un análisis de malware bajo demanda en Amazon EC2, se generará un ID de análisis. Sin embargo, se omitirá el análisis con un motivo EXCLUDED\_BY\_SCAN\_SETTINGS. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

## GuardDuty-initiated análisis de malware

Con el análisis de GuardDuty-initiated malware activado, cada vez que se GuardDuty genere [Hallazgos que invocan un análisis de GuardDuty-initiated malware](#), se iniciará un análisis de malware sin agentes en los volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntos al recurso de Amazon EC2 potencialmente afectado. Antes de que se inicie un análisis, debe preparar la cuenta para cualquier personalización. Las opciones de análisis permiten agregar etiquetas de inclusión para los recursos que desea analizar y etiquetas de exclusión para los recursos que desea omitir durante el proceso de análisis. Al iniciar un análisis automático, siempre se tendrán en cuenta sus opciones de análisis. GuardDuty también admite un par globalGuardDutyExcluded: true etiqueta, clave y valor. Cuando añada esta etiqueta global a un recurso de Amazon EC2, GuardDuty iniciará el escaneo y, a continuación, lo omitirá. También puede optar por activar la configuración de retención de instantáneas para retener las instantáneas de los volúmenes de EBS en los que se detectó potencialmente malware. Para obtener más información sobre las opciones de análisis, la etiqueta de exclusión global y la configuración de instantáneas, consulte [Configure la retención de instantáneas y la cobertura de análisis de EC2](#).

Cuando GuardDuty genere varios resultados para el mismo recurso de Amazon EC2, solo GuardDuty podrá iniciar un análisis cuando hayan transcurrido 24 horas desde el último análisis de GuardDuty-initiated malware. Para obtener información sobre cómo se analizan los volúmenes de Amazon EBS adjuntos a la instancia o carga de trabajo de contenedor de Amazon EC2, consulte [¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?](#).

En la siguiente imagen se describe cómo funciona el análisis de GuardDuty-initiated malware.



Para obtener información sobre la metodología de detección de GuardDuty malware y los motores de análisis que utiliza, consulte [GuardDuty motor de escaneo de detección de malware](#)

Cuando se encuentra malware, se GuardDuty genera [Tipos de resultados de la protección contra malware para EC2](#). Si GuardDuty no se detecta la presencia de malware en el mismo recurso, no se realizará ningún análisis de GuardDuty-initiated malware. También puedes iniciar un análisis de On-demand malware en el mismo recurso. Para obtener más información, consulte [On-demand escanea el malware GuardDuty](#).

## Prueba gratuita de 30 días en GuardDuty-initiated Malware Scan

Puedes optar por activar o desactivar la detección de GuardDuty-initiated malware de una Cuenta de AWS forma compatible Región de AWS en cualquier momento. Si tiene una organización, cada cuenta de miembro tiene su propia prueba gratuita de 30 días.

Para entender cómo funciona la prueba gratuita de 30 días, considere las siguientes situaciones:

- Cuando lo GuardDuty habilitas por primera vez ( GuardDuty cuenta nueva), también se habilita la detección de GuardDuty-initiated malware y se incluye en la prueba gratuita de 30 días asociada al GuardDuty servicio.
- Una GuardDuty cuenta existente puede habilitar la detección de GuardDuty-initiated malware por primera vez con una prueba gratuita de 30 días. Cuando se habilita esta característica en una región diferente por primera vez, obtendrá una prueba gratuita de 30 días en esa región.
- Si ya utilizaba Malware Protection for EC2 y Región de AWS anteriormente este plan de protección se dividía en dos tipos de análisis: el análisis de GuardDuty-initiated malware y el análisis de On-demand malware, puede seguir utilizando el análisis de GuardDuty-initiated malware con el mismo modelo de precios y al mismo tiempo. Región de AWS Si habilita la detección de GuardDuty-initiated malware por primera vez en una nueva región, su cuenta dispondrá de una prueba gratuita de 30 días.

 Note

Aunque se encuentre en un periodo de prueba gratuito de 30 días, se aplica el costo de uso estándar para la creación de las instantáneas de volúmenes de Amazon EBS y su retención. Para obtener más información, consulte [Precios de Amazon EBS](#).

## Habilitar la detección de GuardDuty-initiated malware en entornos con varias cuentas

En un entorno con varias cuentas, solo las cuentas de GuardDuty administrador pueden habilitar la detección de GuardDuty-initiated malware en nombre de las cuentas de sus miembros. Además, una cuenta de administrador que gestione las cuentas de los miembros con AWS Organizations soporte técnico puede optar por activar automáticamente la detección de GuardDuty-initiated malware en todas las cuentas nuevas y existentes de la organización. Para obtener más información, consulte [Administrar GuardDuty cuentas con AWS Organizations](#).

## Establecer un acceso confiable para permitir la detección de GuardDuty-initiated malware

Si la cuenta de administrador GuardDuty delegado no es la misma que la cuenta de administración de su organización, la cuenta de administración debe habilitar la detección de GuardDuty-initiated malware en su organización. De esta forma, la cuenta de administrador delegado puede crear las



cuentas de [Service-linked permisos de rol para Malware Protection for EC2](#) los miembros mediante las que se administran. AWS Organizations

 Note

Antes de designar una cuenta de GuardDuty administrador delegado, consulte.

[Recomendaciones y consideraciones](#)

Elija el método de acceso que prefiera para permitir que la cuenta de GuardDuty administrador delegado pueda detectar las cuentas de los miembros de la organización mediante GuardDuty-initiated software malicioso.

## Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Para iniciar sesión, utilice la cuenta de administración de su AWS Organizations organización.

2. a. Si no ha designado una cuenta de GuardDuty administrador delegado, entonces:

En la página de configuración, en la sección Cuenta de GuardDuty administrador delegado, introduzca los 12 dígitos **account ID** que desee designar para administrar la GuardDuty política en su organización. Elija Delegar.

- b. i. Si ya ha designado una cuenta de GuardDuty administrador delegado diferente de la cuenta de administración, haga lo siguiente:

En la página Configuración, en Administrador delegado, active la configuración Permisos. Esta acción permitirá a la cuenta de GuardDuty administrador delegado adjuntar los permisos pertinentes a las cuentas de los miembros y permitir la detección de GuardDuty-initiated malware en estas cuentas de los miembros.

- ii. Si ya has designado una cuenta de GuardDuty administrador delegado que sea igual a la cuenta de administración, puedes activar directamente la detección de GuardDuty-initiated malware en las cuentas de los miembros. Para obtener más información, consulte [Auto-enable GuardDuty-initiated escanea todas las cuentas de los miembros con malware](#).

 Tip

Si la cuenta de GuardDuty administrador delegado es diferente de tu cuenta de administración, debes proporcionar permisos a la cuenta de GuardDuty administrador delegado para permitir la detección de GuardDuty-initiated malware en las cuentas de los miembros.

3. Si quieres permitir que la cuenta de GuardDuty administrador delegado habilite la detección de GuardDuty-initiated malware para detectar cuentas de miembros en otras regiones, cambia la tuya Región de AWS y repite los pasos anteriores.

## API/CLI

1. Con sus credenciales de la cuenta de administración, ejecute el siguiente comando:

```
aws organizations enable-aws-service-access --service-principal malware-protection.guardduty.amazonaws.com
```

2. (Opcional) Para habilitar la detección de GuardDuty-initiated malware en la cuenta de administración que no sea una cuenta de administrador delegado, la cuenta de administración la creará primero de [Service-linked permisos de rol para Malware Protection for EC2](#) forma explícita en su cuenta y, a continuación, habilitará la detección de GuardDuty-initiated malware desde la cuenta de administrador delegado, de forma similar a la de cualquier otra cuenta de miembro.

```
aws iam create-service-linked-role --aws-service-name malware-protection.guardduty.amazonaws.com
```

3. Ha designado la cuenta de GuardDuty administrador delegado en la cuenta actualmente seleccionada. Región de AWS Si ha designado una cuenta como cuenta de GuardDuty administrador delegado en una región, esa cuenta debe ser su cuenta de GuardDuty administrador delegado en todas las demás regiones. Repita el paso anterior para el resto de las regiones.

## Configurar el análisis de GuardDuty-initiated malware para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para activar o desactivar la detección de GuardDuty-initiated malware en una cuenta de GuardDuty administrador delegado.

### Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija Malware Protection for EC2.
3. En la página Protección contra malware para EC2, seleccione Editar junto al análisis de GuardDuty-initiated malware.
4. Realice una de las siguientes acciones:

#### Utilización Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
- Seleccione Save.

#### Utilización Configure las cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.
- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Save.

### API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como EBS\_MALWARE\_PROTECTION y status como ENABLED.

Puede activar la detección de GuardDuty-initiated malware ejecutando el siguiente AWS CLI comando. Asegúrese de utilizar una cuenta de GuardDuty administrador delegado válida *detector ID*.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /  
    --account-ids 555555555555 /  
    --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Auto-enable GuardDuty-initiated escanea todas las cuentas de los miembros con malware

Elija su método de acceso preferido para habilitar la función de escaneo de GuardDuty-initiated malware en todas las cuentas de los miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

## Console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

Uso de Malware Protection for EC2 page

1. En el panel de navegación, elija Malware Protection for EC2.
2. En la página Protección contra malware para EC2, seleccione Editar en la sección de análisis de GuardDuty-initiated malware.
3. Elija Habilitar para todas las cuentas. Esta acción permite detectar automáticamente el GuardDuty-initiated malware de las cuentas existentes y nuevas de la organización.
4. Seleccione Save.

### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

## Uso de Cuentas page

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de activación automática, selecciona Activar para todas las cuentas objeto de análisis de GuardDuty-initiated malware.
4. En la página Protección contra malware para EC2, seleccione Editar en la sección de análisis de GuardDuty-initiated malware.
5. Elija Habilitar para todas las cuentas. Esta acción permite detectar automáticamente el GuardDuty-initiated malware de las cuentas existentes y nuevas de la organización.
6. Seleccione Save.

### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

## Uso de Cuentas page

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de activación automática, selecciona Activar para todas las cuentas objeto de análisis de GuardDuty-initiated malware.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilita de forma selectiva el análisis de GuardDuty-initiated malware para las cuentas de los miembros](#).

## API/CLI

- Para activar de forma selectiva la detección de GuardDuty-initiated malware en las cuentas de sus miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia *detector ID*.
- En el siguiente ejemplo, se muestra cómo se puede activar la detección de GuardDuty-initiated malware en una cuenta de un solo miembro. Para deshabilitar una cuenta de miembro, sustituya ENABLED por DISABLED.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features ' [{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"} ] '
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilita el análisis de GuardDuty-initiated malware para todas las cuentas de miembros activas existentes

Elige el método de acceso que prefieras para activar el análisis de GuardDuty-initiated malware de todas las cuentas de miembros activos existentes en la organización.

Para configurar el análisis de GuardDuty-initiated malware para todas las cuentas de miembros activas existentes

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija Malware Protection for EC2.
3. En Malware Protection for EC2, puede ver el estado actual de la configuración del análisis de GuardDuty-initiated malware. En la sección Cuentas de miembros activas, seleccione Acciones.

4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Seleccione Save.

Auto-enable GuardDuty-initiated análisis de malware para detectar nuevas cuentas de miembros

Las cuentas de los miembros recién agregadas deben habilitarse GuardDuty antes de seleccionar la configuración del análisis de GuardDuty-initiated malware. Las cuentas de los miembros gestionadas mediante invitación pueden configurar manualmente la detección de GuardDuty-initiated malware para sus cuentas. Para obtener más información, consulte [Step 3 - Accept an invitation](#).

Elija el método de acceso que prefiera para activar la detección de GuardDuty-initiated malware en busca de nuevas cuentas que se unan a su organización.

## Console

La cuenta de GuardDuty administrador delegado puede habilitar la detección de GuardDuty-initiated malware para detectar nuevas cuentas de miembros en una organización mediante la página Protección contra malware para EC2 o la página Cuentas.

Para habilitar automáticamente el análisis de GuardDuty-initiated malware para nuevas cuentas de miembros

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:
  - Utilizar la página Malware Protection for EC2:
    1. En el panel de navegación, elija Malware Protection for EC2.
    2. En la página Protección contra malware para EC2, seleccione Editar en el análisis de GuardDuty-initiated malware.
    3. Elija Configurar cuentas manualmente.
    4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se incorpore a su organización, se habilite automáticamente el análisis de GuardDuty-initiated malware para esa cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.

## 5. Seleccione Save.

- Mediante la página Cuentas:
  1. En el panel de navegación, elija Cuentas.
  2. En la página Cuentas, seleccione Auto-enable las preferencias.
  3. En la ventana Administrar preferencias de activación automática, selecciona Habilitar cuentas nuevas bajo análisis de GuardDuty-initiated malware.
  4. Seleccione Save.

## API/CLI

- Para activar o desactivar la detección de GuardDuty-initiated malware en las cuentas de nuevos miembros, invoca la operación de la [UpdateOrganizationConfiguration](#) API con la tuya propia. *detector ID*
- En el siguiente ejemplo, se muestra cómo se puede activar la detección de GuardDuty-initiated malware en una cuenta de un solo miembro. Para deshabilitar esta característica, consulte [Habilita de forma selectiva el análisis de GuardDuty-initiated malware para las cuentas de los miembros](#). Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name": "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

- Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.



Habilita de forma selectiva el análisis de GuardDuty-initiated malware para las cuentas de los miembros

Elija el método de acceso que prefiera para configurar el análisis de GuardDuty-initiated malware de las cuentas de los miembros de forma selectiva.

## Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija Cuentas.
3. En la página de cuentas, consulta la columna de análisis de GuardDuty-initiated malware para ver el estado de tu cuenta de miembro.
4. Seleccione la cuenta para la que desee configurar el análisis de GuardDuty-initiated malware. Puede seleccionar varias cuentas de manera simultánea.
5. En el menú Editar planes de protección, elija la opción adecuada para el análisis de GuardDuty-initiated malware.

## API/CLI

Para activar o desactivar de forma selectiva el análisis de GuardDuty-initiated malware en las cuentas de sus miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia. *detector ID*

En el siguiente ejemplo, se muestra cómo se puede activar la detección de GuardDuty-initiated malware en una cuenta de un solo miembro.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
"Status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Para activar de forma selectiva el análisis de GuardDuty-initiated malware en tus cuentas de miembros, ejecuta la operación de la [updateMemberDetectors](#) API con la tuya propia. *detector ID* En el siguiente ejemplo, se muestra cómo se puede activar la detección de GuardDuty-initiated malware en una cuenta de un solo miembro.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

Habilita el análisis de GuardDuty-initiated malware para detectar las cuentas existentes en la organización gestionadas mediante invitación

La función vinculada al servicio (SLR) de protección contra GuardDuty malware para EC2 debe crearse en las cuentas de los miembros. La cuenta de administrador no puede habilitar la función de detección de GuardDuty-initiated malware en las cuentas de los miembros que no estén administradas por. AWS Organizations

Actualmente, puedes realizar los siguientes pasos a través de la GuardDuty consola <https://console.aws.amazon.com/guardduty/> para activar la detección de GuardDuty-initiated malware en las cuentas de los miembros existentes.

## Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta de administrador.

2. En el panel de navegación, elija Cuentas.
3. Seleccione la cuenta de miembro para la que desea activar el análisis de GuardDuty-initiated malware. Puede seleccionar varias cuentas de manera simultánea.

4. Elija Acciones.
5. Seleccione Desasociar miembro.
6. En su cuenta de miembro, seleccione Protección contra malware en Planes de protección, en el panel de navegación.
7. Selecciona Activar el análisis de GuardDuty-initiated malware. GuardDuty creará una cámara réflex para la cuenta del miembro. Para obtener más información sobre los SLR, consulte [Service-linked permisos de rol para Malware Protection for EC2](#).
8. En la cuenta de administrador, elija Cuentas en el panel de navegación.
9. Elija la cuenta de miembro que debe volver a agregarse a la organización.
10. Seleccione Acciones y Agregar miembro.

## API/CLI

1. Utilice la cuenta de administrador para ejecutar la [DisassociateMembers](#) API en las cuentas de los miembros que deseen habilitar la detección de GuardDuty-initiated malware.
2. Utilice su cuenta de miembro para invocar y [UpdateDetector](#) activar el análisis de GuardDuty-initiated malware.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
--data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
{"EbsVolumes":true}}}'
```

3. Utilice la cuenta de administrador para ejecutar la API [CreateMembers](#) y volver a agregar al miembro a la organización.

## Habilitar el análisis de GuardDuty-initiated malware para una cuenta independiente

Una cuenta independiente es la que toma la decisión de habilitar o deshabilitar un plan de protección Cuenta de AWS en un plan específico. Región de AWS

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la detección de GuardDuty-initiated malware en entornos con varias cuentas](#).

Después de activar el análisis de GuardDuty-initiated malware, GuardDuty iniciará un análisis de malware del volumen de Amazon EBS adjunto a la instancia de Amazon EC2 que estaba involucrada en un. GuardDuty Para obtener una lista de los resultados que inician el análisis de malware, consulte [Hallazgos que invocan un análisis de GuardDuty-initiated malware](#).

Elija el método de acceso que prefiera para configurar el análisis de GuardDuty-initiated malware para una cuenta independiente.

### Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
3. El panel Protección contra malware para EC2 muestra el estado actual del análisis de GuardDuty-initiated malware de su cuenta. Seleccione Activar para activar el análisis de GuardDuty-initiated malware en esta cuenta.
4. Elija Guardar para confirmar la opción seleccionada.

### API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID de detector regional propio y transmita el objeto dataSources con EbsVolumes establecido en true.

También puede activar el análisis de GuardDuty-initiated malware AWS CLI ejecutando el siguiente AWS CLI comando. Asegúrese de usar su propia validez *detector ID*.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

## Hallazgos que invocan un análisis de GuardDuty-initiated malware

Cuando GuardDuty detecte un comportamiento sospechoso que sea indicativo de malware en una instancia de Amazon EC2 o una carga de trabajo de contenedor que se esté ejecutando en una instancia de Amazon EC2 GuardDuty, generará un hallazgo. Si este hallazgo generado pertenece a la siguiente lista de GuardDuty hallazgos, GuardDuty se iniciará automáticamente un análisis de malware en los volúmenes de Amazon EBS adjuntos a la instancia de Amazon EC2 implicada en el hallazgo. Tras el escaneo, si GuardDuty detecta malware, también generará uno o más. [Tipos de resultados de la protección contra malware para EC2](#)

Si se genera alguno de los siguientes GuardDuty hallazgos en su cuenta, GuardDuty se iniciará automáticamente un análisis de malware en el volumen de Amazon EBS de la instancia de Amazon EC2 potencialmente comprometida.

- [Backdoor:EC2/C&CAActivity.B](#)
- [Backdoor:EC2/C&CAActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)

- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#) (solo salientes)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#) (solo salientes)
- [UnauthorizedAccess:EC2/SSHBruteForce](#) (solo salientes)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [Execution:Runtime/NewLibraryLoaded](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/CryptoMinerExecuted](#)

- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)

## On-demand escanea el malware GuardDuty

On-demand el análisis de malware le ayuda a detectar la presencia de malware en los volúmenes de Amazon Elastic Block Store (Amazon EBS) conectados a sus instancias de Amazon EC2. Sin necesidad de configuración, puede proporcionar el nombre de recurso de Amazon (ARN) de la instancia de Amazon EC2 que desee analizar para iniciar un análisis de malware bajo demanda. Puede iniciar un análisis de malware bajo demanda a través de la GuardDuty consola o la API. Antes de iniciar un análisis de malware bajo demanda, puede establecer la configuración de [Retención de instantáneas](#) que prefiera. Los siguientes escenarios pueden ayudarle a identificar cuándo utilizar este tipo de análisis de On-demand malware GuardDuty:

- Desea detectar la presencia de malware en sus instancias de Amazon EC2 sin activar el análisis de GuardDuty-initiated malware.
- Ha activado el análisis de GuardDuty-initiated malware y se ha activado un análisis automáticamente. Después de seguir la corrección recomendada para el tipo de resultado generado de Malware Protection for EC2, si desea iniciar un análisis en el mismo recurso, podrá

iniciar un análisis de malware bajo demanda una vez transcurrida 1 hora desde la hora de inicio del análisis anterior.

On-demand el análisis de malware no requiere que hayan transcurrido 24 horas desde el momento en que se inició el análisis de malware anterior. Debería haber transcurrido una hora antes de iniciar un análisis de On-demand malware en el mismo recurso. Para evitar la duplicación de un análisis de malware en la misma instancia de EC2, consulte [Re-scanning instancia de Amazon EC2 previamente escaneada](#).

#### Note

On-demand El análisis de malware no está incluido en el período de prueba gratuito de 30 días con. GuardDuty El costo de uso se aplica al volumen total de Amazon EBS analizado por cada análisis de malware. Para obtener más información, consulta los [GuardDuty precios de Amazon](#). Para obtener información sobre el costo de crear las instantáneas del volumen de Amazon EBS y su retención, consulte [Precios de Amazon EBS](#).

## Cómo funciona el análisis de On-demand malware

Con el análisis de On-demand malware, puede iniciar una solicitud de análisis de software malicioso para su instancia de Amazon EC2 incluso cuando esté en uso. Tras iniciar un análisis de On-demand malware, GuardDuty crea instantáneas de los volúmenes de Amazon EBS adjuntos a la instancia de Amazon EC2 cuyo nombre de recurso de Amazon (ARN) se proporcionó para el análisis. A continuación, GuardDuty comparte estas instantáneas con. [GuardDuty cuenta de servicio](#) GuardDuty crea réplicas de volúmenes EBS cifrados a partir de esas instantáneas de la GuardDuty cuenta de servicio. Para obtener más información sobre cómo se analizan los volúmenes de Amazon EBS, consulte [¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?](#).

#### Note

GuardDuty crea las instantáneas de los datos que ya se han escrito en los volúmenes de Amazon EBS en el momento en que se inicia un análisis de malware. On-demand

Si encuentra malware y ha activado la configuración de retención de instantáneas, las instantáneas del volumen de EBS se conservan automáticamente en su archivo. Cuenta de AWS On-demand



el análisis de malware genera el. [Tipos de resultados de la protección contra malware para EC2](#)  
Si no se encuentra ningún malware, las instantáneas de sus volúmenes de EBS se eliminarán, independientemente de la configuración de retención de instantáneas.

GuardDuty utiliza una clave de etiqueta global `GuardDutyExcluded`, que puede añadir a sus recursos de Amazon EC2 y establecer el valor de la etiqueta. `true` Este recurso de Amazon EC2 que tiene este par de clave y valor de etiqueta se excluirá del análisis de malware. Ambos tipos de análisis (análisis de GuardDuty-initiated malware y análisis de On-demand malware) admiten la etiqueta global. Si inicia un análisis de malware bajo demanda en Amazon EC2, se generará un ID de análisis. Sin embargo, se omitirá el análisis con un motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

## Iniciar el análisis de On-demand malware en GuardDuty

En esta sección se proporciona una lista de requisitos previos antes de iniciar un análisis de malware bajo demanda y los pasos para iniciar el análisis en un recurso por primera vez.

Como cuenta de GuardDuty administrador, puede iniciar un análisis de malware bajo demanda en nombre de las cuentas de los miembros activos que tengan configurados los siguientes requisitos previos en sus cuentas. Las cuentas independientes y las cuentas de miembros activos también GuardDuty pueden iniciar un análisis de malware bajo demanda para sus propias instancias de Amazon EC2.

### Requisitos previos

Antes de iniciar un análisis de On-demand software malicioso, su cuenta debe cumplir los siguientes requisitos previos:

- GuardDuty debe estar habilitada en el Regiones de AWS lugar en el que desee iniciar el análisis de malware bajo demanda.
- Asegúrese de que el [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) esté asociado al usuario de IAM o rol de IAM. Necesitará la clave de acceso y la clave secreta asociadas al usuario de IAM o rol de IAM.
- Como cuenta de GuardDuty administrador delegado, tiene la opción de iniciar un análisis de malware bajo demanda en nombre de una cuenta de miembro activa.
- Antes de iniciar un análisis de malware bajo demanda, asegúrese de que no se ha iniciado ningún análisis en el mismo recurso en la última hora; de lo contrario, se eliminará el duplicado.

Para obtener más información, consulte [Re-scanning instancia de Amazon EC2 previamente escaneada](#).

- Si es una cuenta de miembro que no tiene el [Service-linked permisos de rol para Malware Protection for EC2](#), al iniciar un análisis de malware bajo demanda para una instancia de Amazon EC2 que pertenezca a la cuenta, se creará automáticamente el rol vinculado al servicio para Malware Protection for EC2.

 Important

Asegúrese de que nadie elimine los [permisos del rol vinculado al servicio para Malware Protection for EC2](#) cuando el análisis de malware aún esté en curso. Este análisis de malware puede iniciarse GuardDuty o iniciarse bajo demanda. Eliminar el rol vinculado al servicio impedirá que el análisis se complete correctamente y que se obtenga una conclusión definitiva del análisis.

## Inicie el análisis de On-demand malware

Puede iniciar un análisis de malware bajo demanda en su cuenta a través de GuardDuty la consola o utilizando AWS CLI. Deberá proporcionar el nombre de recurso de Amazon (ARN) de Amazon EC2 para el que desea iniciar el análisis. Los pasos detallados se indican en la consola y en la AWS CLI API/instrucciones de la siguiente sección.

Elija el método de acceso que prefiera para iniciar un análisis de malware bajo demanda.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. Inicie el análisis mediante una de las siguientes opciones:
  - a. Utilizar la página Malware Protection for EC2:
    - i. En el panel de navegación, en Planes de protección, elija Malware Protection for EC2.
    - ii. En la página Malware Protection for EC2, proporcione el ARN de la instancia de Amazon EC2<sup>1</sup> para la que desea iniciar el análisis.
  - b. Mediante la página Análisis de malware:

- i. En el panel de navegación, elija Análisis de malware.
- ii. Elija Iniciar análisis bajo demanda y proporcione el ARN de la instancia de Amazon EC2<sup>1</sup> para la que desea iniciar el análisis.
- iii. Si se ha vuelto a hacer el análisis, seleccione una ID de instancia de Amazon EC2 en la página Análisis de malware.

Amplíe el menú desplegable Iniciar el escaneo bajo demanda y elija la instancia Rescan seleccionada.

3. Después de iniciar correctamente un análisis con cualquiera de los métodos, se genera una ID de análisis. Puede utilizar este ID de análisis para hacer un seguimiento del progreso del análisis. Para obtener más información, consulte [Supervisión de los estados y resultados de los análisis de malware](#).

## API/CLI

[StartMalwareScan](#) invoque que acepte la <sup>instancia</sup> 1 resourceArn de Amazon EC2 para la que desea iniciar un análisis de malware bajo demanda.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f"
```

Tras iniciar correctamente un análisis, `StartMalwareScan` devuelve un `scanId`. Invoque el [DescribeMalwareScans](#) monitor para comprobar el progreso del análisis iniciado.

<sup>1</sup>Para obtener información sobre el formato del ARN de su instancia de Amazon EC2, consulte [Nombre de recurso de Amazon \(ARN\)](#). Para las instancias de Amazon EC2, puede utilizar el siguiente formato de ARN de ejemplo sustituyendo los valores de la partición, la región, la ID de Cuenta de AWS y la ID de la instancia de Amazon EC2. Para obtener información sobre la longitud del ID de instancia, consulte [ID de recursos](#).

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

## AWS Organizations política de control de servicios: acceso denegado

Al utilizar las [políticas de control de servicios \(SCP\)](#) de AWS Organizations, la cuenta de GuardDuty administrador delegado puede restringir los permisos y denegar acciones, como iniciar un análisis de malware bajo demanda para detectar una instancia de Amazon EC2 propiedad de sus cuentas.

Como cuenta de GuardDuty miembro, al iniciar un análisis de malware bajo demanda para sus instancias de Amazon EC2, es posible que reciba un error. Puede conectarse con la cuenta de administración para saber por qué se ha configurado una SCP para su cuenta de miembro. Para más información, consulte [Efectos de las SCP en los permisos](#).

## Re-scanning instancia de Amazon EC2 previamente escaneada

Tanto si el análisis se GuardDuty-initiated realiza bajo demanda como si se inicia bajo demanda, puede iniciar un nuevo análisis de malware bajo demanda en la misma instancia de Amazon EC2 una hora después de la hora de inicio del análisis de malware anterior. Si el nuevo análisis de malware se inicia en el plazo de 1 hora desde el inicio del análisis de malware anterior, la solicitud producirá el siguiente error y no se generará ningún ID de análisis para esta solicitud.

A scan was started on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.

Los pasos para volver a analizar la instancia son los mismos que para iniciar un análisis de malware bajo demanda por primera vez. Para obtener más información sobre los pasos, consulte [Inicie el análisis de On-demand malware](#).

Para hacer un seguimiento del estado de los análisis de malware, consulte [Supervisión de los estados y resultados de los análisis en Malware Protection for EC2](#).

## Supervisión de los estados y resultados de los análisis en Malware Protection for EC2

Tras iniciar un análisis de malware en una instancia de Amazon EC2, GuardDuty proporciona automáticamente los campos de estado y resultado. Puede supervisar el estado durante las transiciones y ver si se ha detectado malware. En la siguiente tabla se muestran los valores posibles asociados al análisis de malware.

## Valores potenciales de

Running, Completed , Skipped o Failed

Clean o Infected

GuardDuty initiated o On demand

\*El resultado del análisis solo se rellena cuando el estado del análisis pasa a ser Completed. El resultado del análisis Infected significa que GuardDuty se detectó la presencia de malware.

Los resultados de cada análisis de malware tienen un periodo de retención de 90 días. Elija el método de acceso que prefiera para realizar un seguimiento del estado de su análisis de malware.

## Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Análisis de malware en EC2.
3. Puede filtrar los análisis de malware según las siguientes Propiedades disponibles en la barra de criterios de filtro.
  - ID de análisis: identificador único asociado al análisis de malware de EC2.
  - ID de cuenta: Cuenta de AWS ID donde se inició el análisis de malware.
  - ARN de instancia de EC2: nombre de recurso de Amazon (ARN) asociado a la instancia de Amazon EC2 asociada al análisis.
  - Estado del análisis: el estado del análisis del volumen de EBS, como en ejecución, omitido y completado
  - Tipo de análisis: indica si se trata de un análisis de On-demand malware o de un análisis de GuardDuty-initiated malware.

## API/CLI

- Una vez que el análisis de malware obtenga un resultado, utilícelo [DescribeMalwareScans](#) para filtrar los escaneos de malware en función de EC2\_INSTANCE\_ARN, SCAN\_ID, ACCOUNT\_ID, SCAN\_TYPE, GUARDDUTY\_FINDING\_ID, SCAN\_STATUS, y SCAN\_START\_TIME.

Los criterios de GUARDDUTY\_FINDING\_ID filtrado están disponibles cuando SCAN\_TYPE se GuardDuty inicia.

- Puede cambiar el ejemplo *filter-criteria* en el siguiente comando. Actualmente, puede filtrar de una CriterionKey a la vez. Las opciones de CriterionKey son EC2\_INSTANCE\_ARN, SCAN\_ID, ACCOUNT\_ID, SCAN\_TYPE, GUARDDUTY\_FINDING\_ID, SCAN\_STATUS y SCAN\_START\_TIME.

Puede cambiar el *max-results* (hasta 50) y el *sort-criteria*. El AttributeName es obligatorio y debe ser scanStartTime.

En el siguiente ejemplo, los valores de *red* son marcadores de posición. Sustitúyalos por los valores adecuados para la cuenta. Por ejemplo, sustituya el ejemplo por detector-id *60b8777933648562554d637e0e4bb3b2* el suyo válido detector-id. Si usa el mismo que CriterionKey se muestra a continuación, asegúrese de reemplazar el ejemplo por EqualsValue el suyo válido AWS *scan-id*.

```
aws guardduty describe-malware-scans --detector-id 60b8777933648562554d637e0e4bb3b2 --max-results 1 --sort-criteria '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

- La respuesta de este comando muestra un resultado como máximo con detalles sobre el recurso afectado y los resultados de malware (si está Infected).

## GuardDuty cuentas de servicio de Región de AWS

Cuando se crea una instantánea y se comparte con una cuenta de GuardDuty servicio, se crea un nuevo evento en tus CloudTrail registros. Este evento especifica la snapshotId and userId (cuenta GuardDuty de servicio correspondiente Región de AWS). Para obtener más información, consulte [¿Cómo GuardDuty escanea los volúmenes de EBS para detectar malware?](#).

El siguiente ejemplo es un fragmento de un CloudTrail evento que muestra el cuerpo de la solicitud: `ModifySnapshotAttribute`

```
"requestParameters": {
  "snapshotId": "snap-1234567890abcdef0",
  "createVolumePermission": {
    "add": {
      "items": [
        {
          "userId": "111122223333"
        }
      ]
    }
  },
  "attributeType": "CREATE_VOLUME_PERMISSION"
}
```

En la siguiente tabla se muestran las cuentas GuardDuty de servicio de cada región. `userId`Es la cuenta GuardDuty de servicio y depende de la región seleccionada.

| Región de AWS                          | Código de región | GuardDuty ID de cuenta de servicio ( <code>userId</code> ) |
|----------------------------------------|------------------|------------------------------------------------------------|
| Este de EE. UU. (Norte de Virginia)    | us-east-1        | 652050842985                                               |
| Este de EE. UU. (Ohio)                 | us-east-2        | 178123968615                                               |
| Oeste de EE. UU. (Norte de California) | us-west-1        | 669213148797                                               |
| Oeste de EE. UU. (Oregón)              | us-west-2        | 447226417196                                               |
| Asia-Pacífico (Mumbai)                 | ap-south-1       | 913179291432                                               |
| Asia-Pacífico (Osaka)                  | ap-northeast-3   | 089661699081                                               |
| Asia-Pacífico (Seúl)                   | ap-northeast-2   | 039163547507                                               |
| Asia-Pacífico (Tokio)                  | ap-northeast-1   | 874749492622                                               |

| Región de AWS                       | Código de región | GuardDuty ID de cuenta de servicio ( <b>userId</b> ) |
|-------------------------------------|------------------|------------------------------------------------------|
| Asia-Pacífico (Singapur)            | ap-southeast-1   | 247460962669                                         |
| Asia-Pacífico (Sídney)              | ap-southeast-2   | 124839743349                                         |
| Canadá (centro)                     | ca-central-1     | 175877067165                                         |
| Oeste de Canadá (Calgary)           | ca-west-1        | 894794104037                                         |
| Europa (Fráncfort)                  | eu-central-1     | 002294850712                                         |
| Europa (Irlanda)                    | eu-west-1        | 283769539786                                         |
| Europa (Londres)                    | eu-west-2        | 310125036783                                         |
| Europa (París)                      | eu-west-3        | 866607715269                                         |
| Europa (Estocolmo)                  | eu-north-1       | 693780578038                                         |
| China (Pekín)                       | cn-north-1       | 448721096076                                         |
| China (Ningxia)                     | cn-northwest-1   | 480864352451                                         |
| América del Sur (São Paulo)         | sa-east-1        | 546914126324                                         |
| Asia-Pacífico (Hyderabad) (Opt-in)  | ap-south-2       | 682251015962                                         |
| Asia-Pacífico (Melbourne) (Opt-in)  | ap-southeast-4   | 353488359550                                         |
| Asia Pacífico (Malasia) Opt-in ()   | ap-southeast-5   | 009160069308                                         |
| Asia Pacífico (Tailandia) Opt-in () | ap-southeast-7   | 94137711582                                          |



| Región de AWS                      | Código de región | GuardDuty ID de cuenta de servicio ( <b>userId</b> ) |
|------------------------------------|------------------|------------------------------------------------------|
| Europa (España) (Opt-in)           | eu-south-2       | 936182149045                                         |
| Europa (Zúrich) (Opt-in)           | eu-central-2     | 867642063380                                         |
| Israel (Tel Aviv) (Opt-in)         | il-central-1     | 619233833001                                         |
| Europa (Milán) (Opt-in)            | eu-south-1       | 977238331021                                         |
| Asia Pacífico (Hong Kong) (Opt-in) | ap-east-1        | 249472122084                                         |
| Medio Oriente (Baréin) (Opt-in)    | me-south-1       | 404001805210                                         |
| África (Ciudad del Cabo) (Opt-in)  | af-south-1       | 957664736811                                         |
| Asia-Pacífico (Yakarta) (Opt-in)   | ap-southeast-3   | 452118225523                                         |
| Medio Oriente (EAU) (Opt-in)       | me-central-1     | 828603743433                                         |
| México (Central) (Opt-in)          | mx-central-1     | 557690616787                                         |
| Asia-Pacífico (Taipéi)             | ap-east-2        | 863518437308                                         |
| Asia-Pacífico (Nueva Zelanda)      | ap-southeast-6   | 686255982852                                         |
| AWS GovCloud (US-East)             | us-gov-east-1    | 226283551151                                         |
| AWS GovCloud (US-West)             | us-gov-west-1    | 226300430612                                         |

## Cuotas en la protección contra malware de EC2

En esta sección se incluyen las cuotas asociadas al uso de Malware Protection for EC2. Para conocer las cuotas asociadas a, consulte. GuardDuty [GuardDuty cuotas](#)

En la siguiente tabla se indica la disponibilidad predeterminada de diversos recursos cuando se utiliza Malware Protection for EC2.

| Alcance                                                               | Predeterminado | Comentarios                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Extracción y análisis de datos en un documento comprimido o archivado | 5              | El número máximo de niveles anidados permitidos en un documento archivado.                                                                                                                                                                                                                                                                                             |
| Número de documentos dentro de un documento archivado                 | 1 000          | El número máximo de archivos que se pueden analizar dentro de un archivo. Este recuento es la suma del número de documentos extraídos del archivo y el número de documentos extraídos de todos los archivos anidados.                                                                                                                                                  |
| Número de amenazas                                                    | 32             | El número máximo de amenazas que puede ver en el panel de resultados. GuardDuty Es posible que Malware Protection for EC2 haya detectado más nombres de amenazas. Si el número de nombres de amenazas detectadas es superior al valor predeterminado, puede ver los detalles del JSON seleccionando el identificador de búsqueda situado debajo del nombre de búsqueda |

| Alcance                                     | Predeterminado | Comentarios                                                                                                                                                                                                                                                                                |
|---------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             |                | en el panel de detalles de la GuardDuty consola.                                                                                                                                                                                                                                           |
| Número de archivos por amenaza detectada    | 5              | El número máximo de archivos identificados por amenaza detectada. Por ejemplo, si GuardDuty detecta 10 archivos asociados a una sola amenaza, la amenaza mostrará un máximo de 5 archivos.                                                                                                 |
| Volúmenes de EBS por análisis por instancia | 11             | El número máximo de volúmenes de EBS que GuardDuty se pueden escanear por instancia de EC2. Si hay más de 11 volúmenes de EBS que deben escanearse, GuardDuty Malware Protection for EC2 los ordena <code>deviceName</code> alfabéticamente y selecciona los primeros 11 volúmenes de EBS. |

| Alcance                                   | Predeterminado                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Comentarios                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño del volumen de EBS                 | 2048 GB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Asociado a una carga de trabajo de instancia y contenedor de Amazon EC2, GuardDuty Malware Protection for EC2 puede escanear cada volumen de Amazon EBS que tenga un tamaño máximo de 2048 GB. Esta cuota se aplica a todos los países en los que Región de AWS esté disponible el soporte de Malware Protection para EC2. |
| Tipos de sistemas de archivos compatibles | <p>GuardDuty Malware Protection for EC2 puede analizar los siguientes tipos de sistemas de archivos:</p> <ul style="list-style-type: none"> <li>• Sistema de archivos de nueva tecnología (NTFS)</li> <li>• Sistema de archivos X (XFS)</li> <li>• Sistema de archivos de segunda extensión (ext2)</li> <li>• Sistema de archivos de cuarta extensión (ext4)</li> <li>• Sistema de archivos con tabla de asignación de archivos (FAT)</li> <li>• Sistema de archivos con tabla de asignación de archivos virtuales (VFAT)</li> </ul> | N/A.                                                                                                                                                                                                                                                                                                                       |

| Alcance                                                               | Predeterminado | Comentarios                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Etiquetas de opciones de análisis                                     | 50             | El máximo número de etiquetas de recursos que puede agregar para personalizar la configuración de las opciones de análisis de malware. Para obtener más información, consulte <a href="#">Opciones de análisis con etiquetas definidas por el usuario</a> .                                                        |
| Periodo de conservación de resultados                                 | 90             | El número máximo de días que GuardDuty retiene un hallazgo. Para obtener la información más reciente, consulte <a href="#">GuardDuty Cuotas de Amazon</a> .                                                                                                                                                        |
| Periodo de retención de análisis de malware                           | 90             | El número máximo de días que GuardDuty Malware Protection for EC2 conserva el historial de un análisis. Para obtener más información acerca de la visualización de análisis de malware recientes, consulte <a href="#">Supervisión de los estados y resultados de los análisis en Malware Protection for EC2</a> . |
| Transacciones por segundo (TPS) para On-demand el análisis de malware | 1              | El número de solicitudes de análisis de On-demand malware que se pueden iniciar por segundo en cada región.                                                                                                                                                                                                        |

| Alcance                                               | Predeterminado | Comentarios                                                                                                                       |
|-------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Límite de ráfaga para el escaneo de On-demand malware | 1              | El número de solicitudes simultáneas de análisis de On-demand malware y malware que se pueden iniciar por segundo en cada región. |

# GuardDuty Protección contra malware para S3

La protección contra malware para S3 ayuda a detectar la posible presencia de malware mediante el análisis de los objetos recién cargados en el bucket seleccionado de Amazon Simple Storage Service (Amazon S3). Cuando se carga un objeto de S3 o una nueva versión de un objeto de S3 existente en el depósito seleccionado, GuardDuty se inicia automáticamente un análisis de malware.

## [Protección contra malware para S3: descripción general y demostración](#)

### Dos enfoques para habilitar la protección contra malware para S3

Puede activar la protección contra malware para S3 si Cuenta de AWS habilita el GuardDuty servicio y utiliza Malware Protection for S3 como parte de la GuardDuty experiencia general, o si quiere utilizar la función Malware Protection for S3 por sí sola sin activar el GuardDuty servicio. Si habilita la protección contra malware para S3 por sí sola, la GuardDuty documentación indica que utiliza la protección contra malware para S3 como una función independiente.

Consideraciones para utilizar la protección contra malware para S3 de forma independiente

- GuardDuty consideraciones de seguridad: el identificador del detector es un identificador único que se asocia a tu cuenta en una región. Al activar GuardDuty una o más regiones de

una cuenta, se crea automáticamente un identificador de detector para esa cuenta en cada región en la que se active GuardDuty. Para obtener más información, consulte Detector en el documento [Conceptos y términos clave en Amazon GuardDuty](#).

Al habilitar la protección contra malware para S3 de forma independiente en una cuenta, dicha cuenta no tendrá un ID de detector asociado. Esto afecta a GuardDuty las funciones que puedan estar disponibles para usted. Por ejemplo, cuando un análisis de software malicioso realizado en S3 detecta la presencia de malware, no se generará ningún GuardDuty dato en el suyo, Cuenta de AWS ya que todos los GuardDuty resultados están asociados a un identificador de detector.

- Comprobar si el objeto escaneado es malicioso: de forma predeterminada, GuardDuty publica los resultados del análisis de malware en el bus de EventBridge eventos de Amazon predeterminado y en un espacio de CloudWatch nombres de Amazon. Si habilita el etiquetado al habilitar la protección contra malware para S3 para un bucket, el objeto de S3 analizado recibe una etiqueta que menciona la conclusión del análisis. Para obtener más información acerca del etiquetado, consulte [Etiquetado opcional de objetos en función del resultado del análisis](#).

### Consideraciones generales para habilitar la protección contra malware para S3

Si utiliza Malware Protection for S3 de forma independiente o como parte de la experiencia, se deben tener en cuenta las GuardDuty siguientes consideraciones generales:

- Puede habilitar la protección contra malware para S3 para un bucket de Amazon S3 que pertenezca a una cuenta propia. Como cuenta de GuardDuty administrador delegado, no puede habilitar esta función en un bucket de Amazon S3 que pertenezca a una cuenta de miembro.
- Puede habilitar esta función en los buckets de S3 que pertenecen a la misma región que está actualmente seleccionada en la GuardDuty consola. GuardDuty no admite la activación de esta función en los buckets S3 que se encuentran entre regiones.
- Como cuenta de GuardDuty administrador delegado, recibirá una EventBridge notificación de Amazon cada vez que se produzca un cambio en un bucket [Consulta y lectura del estado del bucket protegido](#) de S3 que una de las cuentas de los miembros de su organización haya configurado para esta función.

### Contenido

- [Precios y costo de uso de la protección contra malware para S3](#)
- [¿Cómo funciona la protección contra malware para S3?](#)



- [Capacidades de la protección contra malware para S3](#)
- [\(Opcional\) Comience a utilizar GuardDuty Malware Protection para S3 de forma independiente \(solo en la consola\)](#)
- [Configurar la protección contra malware para S3 para el bucket](#)
- [Pasos a seguir tras habilitar la protección contra malware para S3](#)
- [On-demand Escaneo de malware S3 en GuardDuty](#)
- [Utilizar el control de acceso basado en etiquetas \(TBAC\) con la protección contra malware para S3](#)
- [Consulta y lectura del estado del bucket protegido](#)
- [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#)
- [Resolución de problemas](#)
- [Editar el plan de protección contra malware para un bucket protegido](#)
- [Desactivar la protección contra malware para S3 para un bucket protegido](#)
- [Compatibilidad con las características de Amazon S3](#)
- [Cuotas en la protección contra malware para S3](#)

## Precios y costo de uso de la protección contra malware para S3

Los precios de Malware Protection para S3 funcionan de manera diferente a los de otros planes de protección GuardDuty. Si bien la mayoría de los planes de GuardDuty protección incluyen una versión de prueba gratuita de 30 días, Malware Protection for S3 incluye una capa gratuita. AWS Para obtener información sobre GuardDuty los precios, consulte [Precios en GuardDuty](#).

En la siguiente lista se indican los precios asociados al uso de la protección contra malware para S3.

### Nivel gratuito (costo de escaneo)

Cada una Cuenta de AWS recibe un nivel gratuito que incluye el uso hasta un límite específico por mes para cada región. Cada una Cuenta de AWS recibe un nivel mensual gratuito de uso de hasta 1000 solicitudes y 1 GB de datos escaneados. Si el uso supera el límite especificado, comenzará a incurrir en el costo de uso correspondiente al límite superado. Para obtener información completa sobre los precios, consulte los [precios GuardDuty de los planes de protección](#).

 Important

On-demand el escaneo no está incluido en la capa gratuita.

Para obtener información sobre el costo de uso después de habilitar la protección contra malware para S3, consulte [Revisar el costo de uso de la protección contra malware para S3](#).

### Costo de uso del etiquetado de objetos de S3

Al habilitar la protección contra malware para S3, es opcional habilitar el etiquetado para los objetos de S3 analizados. Si decide habilitar el etiquetado de objetos de S3, existe un coste de uso asociado. Para obtener más información sobre los costos, consulte la pestaña [Administración e información](#) en la página de precios de Amazon S3.

El coste de uso del etiquetado de objetos de S3 no está incluido en la capa gratuita.

### API de Amazon S3: costo de uso de GET y PUT

Se incurrirá en costes de uso cuando GuardDuty ejecute las API de Amazon S3 en función de la función de IAM. Por ejemplo, tras asumir la función de IAM, GuardDuty ejecuta la `PutObject` API para añadir el objeto de prueba al bucket seleccionado. Esto ayuda a GuardDuty evaluar el estado de activación de la función.

Para obtener información sobre los precios de las llamadas a la API de S3 en su página Región de AWS, consulte [Solicitudes y recuperaciones de datos en la pestaña Almacenamiento y solicitudes](#) de la página de precios de Amazon S3.

## Revisar el costo de uso de la protección contra malware para S3

Su cuenta comienza a incurrir en costes de uso cuando utiliza Malware Protection para S3 más allá del límite específico establecido en la capa gratuita. Para obtener información sobre la capa gratuita, consulte [Precios y costo de uso de la protección contra malware para S3](#). Tenga en cuenta que la capa gratuita no se aplica al escaneo de objetos bajo demanda de Malware Protection for S3.

La GuardDuty consola no permite revisar el costo de uso de Malware Protection para S3.

Para ver el costo de uso, navegue hasta Cost Explorer en la <https://console.aws.amazon.com/costmanagement/> consola. Para obtener información sobre la Cuenta de AWS facturación, consulte la [Guía AWS Billing del usuario](#).

Para obtener información sobre el costo de uso estimado en GuardDuty, consulte [Monitorear el uso y estimar los costos](#).

## ¿Cómo funciona la protección contra malware para S3?

En esta sección se describen los componentes de la protección contra malware para S3, cómo funciona después de habilitarla para un bucket de S3 y cómo puede revisar el estado y el producto del análisis de malware.

### Descripción general de

Puede activar Malware Protection for S3 para un bucket de Amazon S3 que le pertenezca Cuenta de AWS. GuardDuty ofrece la flexibilidad necesaria para habilitar esta función en todo su depósito o limitar el alcance del análisis de malware a [prefijos de objetos](#) específicos, en el que se GuardDuty analiza cada objeto cargado que comience con uno de los prefijos seleccionados. Puede agregar hasta 5 prefijos. Cuando se habilita la característica para un bucket de S3, ese bucket se denomina bucket protegido.

### Permisos de roles de IAM

La protección contra malware para S3 utiliza una función de IAM que le permite GuardDuty realizar las acciones de análisis de malware en su nombre. Estas acciones incluyen recibir una notificación de los objetos recién cargados en el bucket seleccionado, analizar dichos objetos y, opcionalmente, agregar etiquetas a los objetos analizados. Este es un requisito previo para configurar el bucket de S3 con esta característica.

Tiene la opción de actualizar un rol de IAM existente o crear un nuevo rol para este propósito. Al habilitar la protección contra malware para S3 para más de un bucket, podrá actualizar el rol de IAM existente de modo que incluya el nombre del otro bucket, según sea necesario. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).

### Etiquetado opcional de objetos en función del resultado del análisis

Al habilitar la protección contra malware para S3 para el bucket, es posible seguir un paso opcional para habilitar el etiquetado de los objetos de S3 analizados. El rol de IAM ya incluye el permiso para agregar etiquetas al objeto después del análisis. Sin embargo, solo GuardDuty añadirá etiquetas cuando habilite esta opción en el momento de la configuración.

Debe habilitar esta opción antes de que se cargue un objeto. Una vez finalizado el escaneo, GuardDuty agrega una etiqueta predefinida al objeto S3 escaneado con el siguiente par clave-valor:

GuardDutyMalwareScanStatus:*Potential scan result*

Los posibles valores de la etiqueta del producto del análisis son NO\_THREATS\_FOUND, THREATS\_FOUND, UNSUPPORTED, ACCESS\_DENIED y FAILED. Para obtener más información acerca de estos valores, consulte [the section called “Estado potencial de análisis de objeto de S3 y estado del producto”](#).

Habilitar el etiquetado es una de las formas de conocer el producto del análisis del objeto de S3. Además, puede utilizar estas etiquetas para agregar una política de recursos de S3 de control de acceso basado en etiquetas (TBAC), de modo que pueda tomar medidas respecto a los objetos potencialmente maliciosos. Para obtener más información, consulte [Agregar TBAC en el recurso del bucket de S3](#).

Recomendamos que habilite el etiquetado en el momento de configurar la protección contra malware para S3 para el bucket. Si habilita el etiquetado después de cargar un objeto y, posiblemente, se inicie el escaneo, no GuardDuty podrá añadir etiquetas al objeto escaneado. Para obtener información sobre el costo asociado al etiquetado de objetos de S3, consulte [Precios y costo de uso de la protección contra malware para S3](#).

## Proceso posterior a la habilitación de la protección contra malware para S3 para un bucket

Tras habilitar la protección contra malware para S3, se creará un recurso del plan de protección contra malware exclusivo para el bucket de S3 seleccionado. Este recurso está asociado a un ID de plan de protección contra malware, que es un identificador único para el recurso protegido. Al usar uno de los permisos de IAM, crea GuardDuty y administra una regla EventBridge administrada con el nombre de. D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3\*

## Cómo GuardDuty gestiona sus datos: barreras para la protección de datos

Malware Protection for S3 escucha las EventBridge notificaciones de Amazon. Cuando se carga un objeto en el depósito seleccionado o en uno de los prefijos, GuardDuty descarga ese objeto del depósito de S3 mediante un [AWS PrivateLink](#), a continuación, lo lee, descifra y escanea en un entorno aislado de la misma región. El entorno de análisis se ejecuta en una nube privada virtual (VPC) bloqueada sin acceso a Internet. La VPC está conectada a un grupo de reglas de firewall de DNS que permite la comunicación solo con los dominios que son propietarios de la lista de

permitidos. AWS Durante el análisis, almacena GuardDuty temporalmente el objeto S3 descargado en el entorno de análisis cifrado con las claves [AWS Key Management Service \(AWS KMS\)](#).

#### Note

De forma predeterminada, todas las API de Amazon S3 enumeradas en el [tipo de evento de objeto creado](#) en la Guía del usuario de Amazon S3, iniciarán el análisis de protección contra malware para S3.

Estos tipos de eventos incluyen [PutObject](#), el [objeto POST](#) y [CompleteMultipartUpload](#).  
[CopyObject](#)

Para obtener información sobre la metodología de detección de GuardDuty malware y los motores de análisis que utiliza, consulte [GuardDuty motor de escaneo de detección de malware](#).

Una vez finalizado el análisis de software malicioso, GuardDuty procesa los metadatos del análisis con el estado del análisis y, a continuación, elimina la copia descargada del objeto.

GuardDuty limpia el entorno de escaneo cada vez antes de que comience un nuevo escaneo. GuardDuty utiliza una autorización condicionada para el acceso del operador al entorno de digitalización, y todas las solicitudes de acceso se revisan, aprueban y auditan.

## Revisar el estado y el producto del análisis de objetos del S3

GuardDuty publica el evento resultante del escaneo de objetos de S3 en el bus de eventos EventBridge predeterminado de Amazon. GuardDuty también envía a Amazon las métricas de escaneo, como el número de objetos escaneados y los bytes escaneados CloudWatch. Si has activado el etiquetado, GuardDuty añadirá la etiqueta predefinida GuardDutyMalwareScanStatus y un posible resultado del escaneo como valor de la etiqueta.

#### Important

GuardDuty se envía al menos una vez, lo que significa que puede recibir varios resultados de escaneo del mismo objeto. Le recomendamos que diseñe sus aplicaciones para gestionar los resultados duplicados. Solo se le facturará una vez por cada objeto analizado.

Para obtener más información, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).

## Revisar los resultados generados

La revisión de los resultados dependerá de si utiliza o no Malware Protection for S3 con GuardDuty. Considere los siguientes escenarios:

Uso de la protección contra malware para S3 cuando el GuardDuty servicio está activado (ID del detector)

Si el análisis de malware detecta un archivo potencialmente malicioso en un objeto S3, GuardDuty generará un hallazgo asociado. Puede ver los detalles del resultado y seguir los pasos recomendados para remediarlo potencialmente. En función de la [frecuencia de las búsquedas de exportación, las conclusiones](#) generadas se exportan a un bucket de S3 y a un bus de EventBridge eventos.

Para obtener información sobre el tipo de resultado que se generará, consulte [Tipo de resultado de la protección contra malware para S3](#).

Utilizar la protección contra malware para S3 como una característica independiente (sin ID de detector)

GuardDuty no podrá generar resultados porque no hay un ID de detector asociado. Para conocer el estado del análisis de malware con objetos S3, puede ver el resultado del análisis que GuardDuty se publica automáticamente en su bus de eventos predeterminado. También puede ver las CloudWatch métricas para evaluar la cantidad de objetos y bytes que se GuardDuty intentaron escanear. Puede configurar CloudWatch alarmas para recibir notificaciones sobre los resultados del escaneo. Si ha habilitado el etiquetado de objetos de S3, también podrá ver el estado del análisis de malware si comprueba en el objeto de S3 la clave de la etiqueta GuardDutyMalwareScanStatus y el valor de la etiqueta del producto del análisis.

Para obtener información sobre el estado y el producto del análisis de objetos de S3, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).

## Capacidades de la protección contra malware para S3

La siguiente lista ofrece una descripción general de lo que puede esperar o realizar después de habilitar la protección contra malware para S3 en el bucket:

- Elija qué analizar: analice los archivos a medida que se cargan en todos los prefijos o en prefijos específicos (hasta 5) asociados al bucket de S3 seleccionado.

- Análisis automáticos de los objetos cargados: una vez que actives Malware Protection for S3 para un bucket, se GuardDuty iniciará automáticamente un análisis para detectar el posible malware en un objeto recién cargado.
- On-demand escaneos: puede iniciar escaneos de objetos existentes o volver a escanear objetos escaneados anteriormente. Para obtener más información, consulte [On-demand Escaneo de malware S3 en GuardDuty](#).
- Actívela a través de la consola, mediante API/AWS CLI o CloudFormation: elija el método que prefiera para activar la protección contra malware para S3.

Puede habilitar la protección contra malware para S3 por medio de plataformas de infraestructura como código (IaC), como Terraform. Para obtener más información, consulte [Recurso: aws\\_guarddduty\\_malware\\_protection\\_plan](#).

- Formatos de archivo compatibles, cuotas de la protección contra malware para S3 y características de Amazon S3: la protección contra malware para S3 es compatible con todos los formatos de archivo que se pueden cargar en un bucket de S3. Si el archivo cargado está protegido con contraseña y GuardDuty es capaz de detectar la presencia de una protección por contraseña para el tipo de archivo cargado, GuardDuty intentará escanear el contenido original con contraseñas comunes. Si la contraseña falla, se omitirá el escaneo. GuardDuty no puede detectar la presencia de protección por contraseña en todos los formatos de archivo. Si no GuardDuty puede detectar la presencia de una protección con contraseña, GuardDuty seguirá escaneando el contenido cifrado.

Para obtener información sobre las cuotas relacionadas con el tamaño de los objetos, el nivel máximo de profundidad del archivo y otros detalles, consulte [Cuotas en la protección contra malware para S3](#).

Para obtener información sobre si una característica de Amazon S3 es compatible, consulte [Compatibilidad con las características de Amazon S3](#).

- Admite el etiquetado de objetos S3 escaneados: si lo [Etiquetado opcional de objetos en función del resultado del análisis](#) habilitas, después de cada análisis de malware, GuardDuty se añadirá una etiqueta que indica el estado del escaneo. Puede utilizar esta etiqueta para configurar el control de acceso basado en etiquetas (TBAC) para los objetos de S3. Por ejemplo, puede restringir el acceso a los objetos de S3 indicados como maliciosos y cuyo valor de etiqueta sea THREATS\_FOUND.
- EventBridge Notificaciones de Amazon: GuardDuty envía eventos a Amazon EventBridge cuando el estado de los recursos del plan de protección contra malware cambia o cuando se completa un análisis de malware del objeto S3. Estos eventos se envían al bus de eventos predeterminado.

Puede usar EventBridge estos eventos para escribir reglas que tomen medidas, como monitorear cuándo ocurren estos eventos. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

- CloudWatch métricas: consulta CloudWatch las métricas para activar las alarmas en determinados estados de detección de malware. Para obtener más información, consulte [Métricas de estado del escaneo de objetos de S3 en CloudWatch](#).

## (Opcional) Comience a utilizar GuardDuty Malware Protection para S3 de forma independiente (solo en la consola)

Utilice este paso opcional si quiere empezar a utilizar la opción de detección de amenazas de Malware Protection for S3, independientemente del GuardDuty estado en el que se encuentre Cuenta de AWS.

Si también quieres utilizar otros planes de protección dedicados GuardDuty, debes empezar con el GuardDuty servicio de Amazon. Para obtener información sobre los planes de GuardDuty protección, consulte [Características de GuardDuty](#). Si ya lo ha activado GuardDuty en su cuenta, puede omitir este paso y continuar con él [Configurar la protección contra malware para S3 para el bucket](#).

Pasos para comenzar a utilizar la detección de amenazas de la protección contra malware para S3 únicamente

1. Inicia sesión en Consola de administración de AWS y abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Seleccione Protección contra GuardDuty malware únicamente para S3. Esto ayuda a detectar si un archivo recién cargado en el bucket de Amazon Simple Storage Service (Amazon S3) potencialmente contiene malware.



## Try threat detection with GuardDuty

☐ Amazon GuardDuty - all features

Experience threat detection capabilities in your AWS environment.

☒ GuardDuty Malware Protection for S3 only

Detect malicious file upload to your Amazon S3 buckets. You don't need to enable Amazon GuardDuty.

**Get started**

3. Elija Comenzar. Ahora puede continuar con los pasos que se indican en [Configurar la protección contra malware para S3 para el bucket](#).

## Configurar la protección contra malware para S3 para el bucket

Para que la protección contra malware para S3 analice y (opcionalmente) agregue etiquetas a los objetos de S3, puede utilizar roles de servicio que tengan los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre el uso de roles de servicio para habilitar la protección contra malware para S3, consulte [Acceso a servicios](#). Esta función es diferente de la función [vinculada al servicio GuardDuty Malware Protection](#).

Si prefiere utilizar funciones de IAM, puede adjuntar una función de IAM que incluya los permisos necesarios para escanear y (opcionalmente) añadir etiquetas a sus objetos de S3. GuardDuty a continuación, asume esta función de IAM para realizar estas acciones en su nombre. Necesitará este nombre de rol de IAM a la hora de habilitar este plan de protección para el bucket de Amazon S3.

Si utiliza roles de IAM, cada vez que desee proteger un bucket de Amazon S3, deberá seguir los dos pasos que se indican en esta sección.

Para habilitar la protección contra malware para S3, necesitará detalles, como el nombre del bucket de S3, los prefijos de objetos si desea centrar la protección en prefijos específicos y el nombre del rol de IAM con los permisos necesarios.

Los pasos siguen siendo los mismos tanto si empieza a utilizar Malware Protection para S3 de forma independiente como si lo habilita como parte del GuardDuty servicio.

## Temas

1. [Crear o actualizar la política del rol de IAM](#)
2. [Habilitar la protección contra malware para S3 para el bucket](#)
3. [Solución de problemas de errores de permisos de roles de IAM](#)

## Habilitar la protección contra malware para S3 para el bucket

En esta sección se indican los pasos detallados que se deben seguir para habilitar la protección contra malware para S3 en un bucket de una cuenta propia. Revise las siguientes consideraciones antes de continuar:

- Cuando habilita este plan de protección mediante la GuardDuty consola, incluye el paso para crear un nuevo rol o usar un rol existente en la sección Acceso al servicio.
- Cuando habilita este plan de protección mediante la GuardDuty API o la CLI, debe hacerlo [Crear o actualizar la política del rol de IAM](#) antes de continuar.
- Independientemente de cómo habilite este plan de protección, debe tener lo el [Permisos para crear un recurso de plan de protección contra malware](#) requerido.

## Pensar la limitación de los buckets de Amazon S3

La limitación de S3 podría limitar la velocidad a la que se pueden transferir datos hacia o desde sus buckets de Amazon S3. Esto podría retrasar los análisis de malware de los objetos recién cargados.

Si espera que sus buckets de S3 reciban grandes volúmenes de solicitudes de GET y PUT, considere implementar medidas para evitar que se limiten. Para obtener información sobre cómo hacerlo, consulte [Evitar la limitación de Amazon S3](#) en la Guía del usuario de Amazon Athena.

## Permisos para crear un recurso de plan de protección contra malware

Al habilitar Malware Protection for S3 para un bucket de Amazon S3, GuardDuty crea un recurso del plan de protección contra malware que actúa como identificador del plan de protección del bucket. Si aún no utiliza el [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#), debe agregar los siguientes permisos para crear este recurso:

- `guardDuty:CreateMalwareProtectionPlan`
- `iam:PassRole`

Puedes usar el siguiente ejemplo de política personalizada y sustituirlo por los valores adecuados para tu cuenta: *placeholder values*

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/role-name",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "malware-protection-  
plan.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateMalwareProtectionPlan"
      ],
      "Resource": "*"
    }
  ]
}
```

## Habilitar la protección contra malware para S3 mediante GuardDuty la consola

En las siguientes secciones se proporciona un recorrido paso a paso, tal como se verá en la GuardDuty consola.

Para habilitar la protección contra malware para S3 mediante la consola GuardDuty

Ingresa los detalles del bucket de S3

Siga los pasos que se indican a continuación para proporcionar los detalles del bucket de Amazon S3:

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee activar la protección contra malware para S3.
3. En el panel de navegación, elija Protección contra malware para S3.
4. En la sección Depósitos protegidos, seleccione Activar para activar la protección contra malware para S3 en un depósito de S3 que le Cuenta de AWS pertenezca.
5. En Ingresar detalles del bucket de S3, ingrese el nombre del bucket de Amazon S3. O bien, seleccione Examinar S3 para seleccionar un bucket de S3.

El compartimento Región de AWS de S3 y el lugar en el que Cuenta de AWS se habilita la protección contra malware para S3 deben ser iguales. Por ejemplo, si la cuenta pertenece a la región us-east-1, la región del bucket de Amazon S3 también debe ser us-east-1.

6. En Prefijo, puede seleccionar Todos los objetos del bucket de S3 u Objetos que comiencen con un prefijo específico.
  - Seleccione Todos los objetos del depósito de S3 cuando desee y GuardDuty podrá escanear todos los objetos recién cargados del depósito seleccionado.
  - Seleccione Objetos que comienzan con un prefijo específico cuando desee analizar los objetos recién cargados que pertenezcan a un prefijo específico. Esta opción sirve para focalizar el alcance del análisis de malware únicamente en los prefijos de objetos seleccionados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos en la Consola de Amazon S3 mediante carpetas](#) en la Guía del usuario de Amazon S3.

Elija Agregar prefijo e ingrese el prefijo. Puede agregar hasta cinco prefijos.

## Habilite el etiquetado para los objetos analizados

Se trata de un paso opcional. Si activas la opción de etiquetado antes de que un objeto se cargue en tu depósito, después de completar el escaneo, GuardDuty añadirá una etiqueta predefinida con la clave `GuardDutyMalwareScanStatus` y el valor como resultado del escaneo. Para utilizar la protección contra malware para S3 de forma óptima, recomendamos habilitar la opción de agregar etiquetas a los objetos de S3 una vez finalizado el análisis. Se aplica el costo estándar de etiquetado de objetos de S3. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

### ¿Por qué debería habilitar el etiquetado?

- Habilitar el etiquetado es una de las formas de conocer el resultado del análisis de malware. Para obtener información sobre el resultado de un análisis de malware de S3, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).
- Configure la política de control de acceso basado en etiquetas (TBAC) en el bucket de S3 que contiene el objeto potencialmente malicioso. Para obtener información sobre las consideraciones y la forma de aplicar el control de acceso basado en etiquetas (TBAC), consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\) con la protección contra malware para S3](#).

### Consideraciones GuardDuty para añadir una etiqueta a su objeto de S3:

- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto. Para obtener más información, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Si las 10 etiquetas ya están en uso, no GuardDuty se puede añadir la etiqueta predefinida al objeto escaneado. GuardDuty también publica el resultado del escaneo en el bus de EventBridge eventos predeterminado. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

- Si la función de IAM seleccionada no incluye el permiso para GuardDuty etiquetar el objeto de S3, ni siquiera con el etiquetado activado en el depósito protegido, no GuardDuty podrá añadir una etiqueta a este objeto de S3 escaneado. Para obtener más información sobre el permiso de rol de IAM necesario para el etiquetado, consulte [Crear o actualizar la política del rol de IAM](#).

GuardDuty también publica el resultado del escaneo en el bus de EventBridge eventos predeterminado. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

Para seleccionar una opción en Etiquetar objetos analizados

- Cuando desee añadir etiquetas GuardDuty a los objetos S3 escaneados, seleccione Etiquetar objetos.
- Si no desea añadir etiquetas GuardDuty a los objetos S3 escaneados, seleccione No etiquetar objetos.

## Acceso a los servicios

Siga los pasos que se indican a continuación para elegir un rol de servicio existente o crear un nuevo rol de servicio que cuente con los permisos necesarios para realizar acciones de análisis de malware en su nombre. Entre esas acciones se incluye el análisis de objetos de S3 recién cargados y (opcionalmente) la adición de etiquetas a esos objetos. Para obtener información sobre los permisos que tendrá el rol, consulte [Crear o actualizar la política del rol de IAM](#).

En la sección Acceso al servicio, puede realizar una de las siguientes acciones:

1. Crear y utilizar un nuevo rol de servicio: puede utilizar la opción de crear un nuevo rol de servicio que cuente con los permisos necesarios para realizar el análisis de malware.

En el nombre del rol, puede elegir usar el nombre relleno previamente GuardDuty o introducir un nombre significativo de su elección para identificar el rol. Por ejemplo, GuardDutyS3MalwareScanRole. El nombre del rol debe tener entre 1 y 64 caracteres. Los caracteres válidos son los caracteres a-z A-Z, 0-9 y '+', '@', '-' y '\_'.

2. Utilizar un rol de servicio existente: puede elegir un rol de servicio existente de la lista Nombre del rol de servicio.
  - a. En Plantilla de política puede ver la política que corresponde al bucket de S3. Asegúrese de que ha ingresado o seleccionado un bucket de S3 en la sección de detalles Ingrese el bucket de S3.
  - b. En Nombre de rol de servicio, elija un rol de servicio de la lista de roles de servicio.

Puede realizar cambios en la política en función de sus necesidades. Para obtener más información sobre cómo crear o actualizar un rol de IAM, consulte [Crear o actualizar una política de rol de IAM](#).

Si tiene problemas con los permisos de los roles de IAM, consulte [Solución de problemas de errores de permisos de roles de IAM](#).

(Opcional) Etiquetar el ID del plan de protección contra malware

Este es un paso opcional que ayuda a agregar etiquetas al recurso del plan de protección contra malware que se creará para el recurso de bucket de S3.

Cada etiqueta consta de dos partes: una clave de etiqueta y un valor de etiqueta opcional. [Para obtener más información sobre el etiquetado y sus ventajas, consulte Recursos de etiquetado. AWS](#)

Para agregar etiquetas al recurso del plan de protección contra malware

1. Ingrese la Clave y un Valor opcional para la etiqueta. Tanto la clave como el valor de la etiqueta distinguen entre mayúsculas y minúsculas. Para obtener información sobre los nombres de clave y valor de etiqueta, consulte [Límites y requisitos al asignar nombres a las etiquetas](#).
2. Para agregar más etiquetas al recurso del plan de protección contra malware, seleccione Agregar nueva etiqueta y repita el paso anterior. Puede agregar hasta 50 etiquetas a cada recurso de .
3. Seleccione Habilitar.

Habilitar la protección contra malware para S3 mediante API/CLI

En esta sección se incluyen los pasos que debe seguir para activar la protección contra malware para S3 mediante programación en su AWS entorno. Para esto se requiere el nombre de recurso de Amazon (ARN) del rol de IAM que creó en este paso: [Crear o actualizar la política del rol de IAM](#).

Para habilitar la protección contra malware para S3 mediante programación mediante API/CLI

- Por medio de la API

Ejecute [CreateMalwareProtectionPlan](#) para habilitar la protección contra malware para S3 en un bucket que pertenezca a su propia cuenta.

- Mediante el uso de AWS CLI

En función de cómo desee activar la protección contra malware para S3, en la siguiente lista se proporcionan AWS CLI ejemplos de comandos para un caso de uso específico. Cuando

ejecute estos comandos, sustituya el *placeholder examples shown in red*, por los valores adecuados para su cuenta.

### AWS CLI comandos de ejemplo

- Utilice el siguiente AWS CLI comando para activar la protección contra malware para S3 en un depósito sin etiquetar los objetos de S3 escaneados:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"}
```

- Utilice el siguiente AWS CLI comando para activar la protección contra malware para S3 en un depósito con prefijos de objetos específicos y sin etiquetar los objetos de S3 escaneados:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::111122223333:role/role-name" --protected-resource '{"S3Bucket":
{"BucketName": "amzn-s3-demo-bucket1", "ObjectPrefixes": ["Object1", "Object1"]}}'
```

- Utilice el siguiente AWS CLI comando para activar la protección contra malware para S3 en un depósito con el etiquetado de objetos escaneados de S3 activado:

```
aws guardduty create-malware-protection-plan --role
"arn:aws:iam::111122223333:role/role-name" --protected-resource
"S3Bucket"={"BucketName"="amzn-s3-demo-bucket1"} --actions
"Tagging"={"Status"="ENABLED"}
```

Después de ejecutar estos comandos correctamente, se generará un ID único de plan de protección contra malware. Para realizar acciones, como actualizar o desactivar el plan de protección del bucket, necesitará este ID de plan de protección contra malware.

Si tiene problemas con los permisos de los roles de IAM, consulte [Solución de problemas de errores de permisos de roles de IAM](#).

## Crear o actualizar la política del rol de IAM

Para que la protección contra malware para S3 analice y (opcionalmente) agregue etiquetas a los objetos de S3, puede utilizar roles de servicio que tengan los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre el uso de roles



de servicio para habilitar la protección contra malware para S3, consulte [Acceso a servicios](#). Esta función es diferente de la función [vinculada al servicio GuardDuty Malware Protection](#).

Si prefiere utilizar roles de IAM, puede asociar un rol de IAM que incluya los permisos necesarios para analizar y (opcionalmente) agregar etiquetas a los objetos de S3. Debe crear un rol de IAM o actualizar un rol existente para incluir estos permisos. Dado que estos permisos son necesarios para cada bucket de Amazon S3 para el que habilite la protección contra malware para S3, deberá seguir este paso para cada bucket de Amazon S3 que desee proteger.

En la siguiente lista se explica cómo determinados permisos ayudan a GuardDuty realizar el análisis de malware en tu nombre:

- Permita que Amazon EventBridge Actions cree y gestione la regla EventBridge gestionada para que Malware Protection for S3 pueda escuchar sus notificaciones de objetos de S3.

Para obtener más información, consulta [las reglas EventBridge gestionadas por Amazon](#) en la Guía del EventBridge usuario de Amazon.

- Permita que Amazon S3 y EventBridge Actions envíen notificaciones EventBridge para todos los eventos de este bucket

Para obtener más información, consulte [Habilitar Amazon EventBridge](#) en la Guía del usuario de Amazon S3.

- Permita que las acciones de Amazon S3 accedan al objeto de S3 cargado y agreguen una etiqueta predefinida, GuardDutyMalwareScanStatus, al objeto de S3 analizado. Al utilizar un prefijo de objeto, agregue una condición `s3:prefix` únicamente en los prefijos de destino. Esto GuardDuty impide el acceso a todos los objetos de S3 del bucket.
- Permita que las acciones clave del KMS accedan al objeto antes de escanear y colocar un objeto de prueba en los depósitos con el SSE-KMS cifrado DSSE-KMS y el soporte.

#### Note

Este paso es necesario cada vez que habilite la protección contra malware para S3 para un bucket en la cuenta. Si ya cuenta con un rol de IAM existente, puede actualizar su política de forma que incluya los detalles de otro recurso de bucket de Amazon S3. El tema [Agregar permisos de política de IAM](#) proporciona un ejemplo de cómo hacerlo.

Utilice las siguientes políticas para crear o actualizar un rol de IAM.

## Políticas

- [Agregar permisos de política de IAM](#)
- [Agregar la política de relación de confianza](#)

## Agregar permisos de política de IAM

Puede optar por actualizar la política en línea de un rol de IAM existente o crear un nuevo rol de IAM. Para obtener información sobre los pasos, consulte [Crear un rol de IAM](#) o [Modificar una política de permisos de rol](#) en la Guía del usuario de IAM.

Agregue la siguiente plantilla de permisos al rol de IAM que prefiera. Sustituya los siguientes valores de marcador de posición por los valores apropiados asociados a la cuenta:

- Para *amzn-s3-demo-bucket*, sustitúyalo por el nombre de tu bucket de Amazon S3.

Para utilizar el mismo rol de IAM para más de un recurso de bucket de S3, actualice una política existente como se muestra en el siguiente ejemplo:

```
...  
...  
"Resource": [  
    "arn:aws:s3:::amzn-s3-demo-bucket/*",  
    "arn:aws:s3:::amzn-s3-demo-bucket2/*"  
],  
...  
...
```

Asegúrese de agregar una coma (,) antes de agregar un nuevo ARN asociado al bucket de S3. Repita este paso siempre que haga referencia a un Resource de bucket de S3 en la plantilla de política.

- Para *111122223333*, sustitúyalo por tu Cuenta de AWS ID.
- Para *us-east-1*, sustitúyalo por tu Región de AWS.
- Sustituya *APKAEIBAERJR2EXAMPLE* por el identificador de clave administrada por el cliente. Si su depósito de S3 está cifrado mediante una AWS KMS clave, añadimos los permisos correspondientes si elige la opción [Crear un nuevo rol](#) al configurar la protección contra malware para su depósito.

```
"Resource": "arn:aws:kms:us-east-1:111122223333:key/*"
```

## Plantilla de la política del rol de IAM

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",
    "Effect": "Allow",
    "Action": [
      "events:PutRule",
      "events>DeleteRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ],
    "Condition": {
      "StringLike": {
        "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGuardDutyToMonitorEventBridgeManagedRule",
    "Effect": "Allow",
    "Action": [
      "events:DescribeRule",
      "events:ListTargetsByRule"
    ],
    "Resource": [
      "arn:aws:events:us-east-1:111122223333:rule/DO-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
    ]
  }
],
}
```

```

    {
      "Sid": "AllowPostScanTag",
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "AllowEnableS3EventBridgeEvents",
      "Effect": "Allow",
      "Action": [
        "s3:PutBucketNotification",
        "s3:GetBucketNotification"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "AllowPutValidationObject",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
      ]
    },
    {
      "Sid": "AllowCheckBucketOwnership",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}

```

```

    },
    {
      "Sid": "AllowMalwareScan",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "AllowDecryptForMalwareScan",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/APKAEIBAERJR2EXAMPLE",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "s3.us-east-1.amazonaws.com"
        }
      }
    }
  ]
}

```

## Agregar la política de relación de confianza

Asocie la siguiente política de confianza al rol de IAM. Para obtener más información sobre los pasos, consulte [Modificar una política de confianza del rol](#).

### JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```
    "Effect": "Allow",
    "Principal": {
      "Service": "malware-protection-plan.guardduty.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
```

## Solución de problemas de errores de permisos de roles de IAM

Al habilitar Malware Protection para S3, GuardDuty comprueba si su función de servicio de IAM tiene los permisos necesarios para validar la propiedad del bucket de Amazon S3. Si estos permisos faltan o están mal configurados, es posible que reciba el siguiente mensaje:

```
"message": "The request was rejected because provided IAM role does not have the
  required permissions to validate S3 bucket ownership."
"type": "InvalidInputException"
```

Los siguientes escenarios pueden ayudarlo a solucionar este error:

### Faltan permisos para el rol de IAM

- El rol de IAM debe tener los permisos necesarios para permitir la protección contra malware para que S3 asuma el rol.
- GuardDuty valida la propiedad del bucket con el "s3:ListBucket" permiso. Debe estar presente en el rol de IAM que se utiliza.

Para obtener información acerca de los permisos, consulte [Crear o actualizar la política del rol de IAM](#).

### Disponibilidad del rol de IAM

- Al crear un nuevo rol de IAM, espere unos minutos para que los cambios alcancen una coherencia final antes de activar la protección contra malware para S3. Si intenta activar el plan de protección inmediatamente después de crear el rol, la validación podría fallar.
- En el caso de las implementaciones de Infrastructure as Code (IaC), GuardDuty recomienda declarar una dependencia de los recursos para garantizar que la función de IAM alcance una coherencia definitiva.

[Para ver ejemplos de plantillas sobre cómo hacerlo, consulta el repositorio. GuardDuty GitHub](#)

## Cross-region habilitación

Asegúrese de que su bucket de Amazon S3 esté en la misma región en la que está habilitando Malware Protection for S3 GuardDuty.

## Pasos a seguir tras habilitar la protección contra malware para S3

En esta sección se indican los pasos que puede seguir tras habilitar la protección contra malware para S3 para un bucket. Los siguientes pasos se presentan en un orden que facilita avanzar en las próximas etapas:

A seguir después de habilitar la protección contra malware para S3 para el bucket

1. Agregue la política de recursos de control de acceso basado en etiquetas (TBAC): al habilitar el etiquetado, antes de cargar un objeto en el bucket seleccionado, asegúrese de agregar la política TBAC al recurso del bucket de S3. Para obtener más información, consulte [Agregar TBAC en el recurso del bucket de S3](#).
2. Supervise el estado del plan de protección contra malware: supervise la columna Estado para cada bucket protegido. Para obtener información sobre los posibles estados y su significado, consulte [Consulta y lectura del estado del bucket protegido](#).
3. Inicie un escaneo seleccionando una de las siguientes opciones:
  - Cargar un objeto:
    1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
    2. Cargue un archivo en el bucket de S3 o en el prefijo de objeto para el que habilitó esta característica. Para conocer los pasos para cargar un archivo, consulte [Cargar un objeto en el bucket](#) en la Guía del usuario de Amazon S3.
  - Inicie un análisis bajo demanda: [On-demand Escaneo de malware S3 en GuardDuty](#)
4. Supervise el estado del análisis del objeto de S3 y el producto del análisis: este paso incluye información sobre cómo comprobar el estado del análisis de malware del objeto de S3.

| Habilitado GuardDuty tanto como la protección contra malware para S3                                                                                      | Habilitada únicamente la protección contra malware para S3                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Cuando GuardDuty está habilitada, puede generar el <a href="#">Tipo de resultado de la protección</a></li> </ul> | Puede comprobar potencialmente el producto del análisis de objetos de S3 por medio de |

| Habilitado GuardDuty tanto como la protección contra malware para S3                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Habilitada únicamente la protección contra malware para S3                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><a href="#">n contra malware para S3</a> símbolo para indicar la presencia de malware en el objeto S3 escaneado.</p> <ul style="list-style-type: none"> <li>Puede comprobar potencialmente el producto del análisis de objetos de S3 por medio de una o más opciones en <a href="#">Supervisión de los análisis de objetos de S3 en la protección contra malware para S3</a>. Estas incluyen el uso de Amazon EventBridge, CloudWatch las métricas del plan de protección contra malware y el etiquetado de los objetos escaneados.</li> </ul> | <p>una o más opciones en <a href="#">Supervisión de los análisis de objetos de S3 en la protección contra malware para S3</a>. Estas incluyen el uso de Amazon EventBridge, CloudWatch las métricas del plan de protección contra malware y el etiquetado de los objetos escaneados.</p> |

## On-demand Escaneo de malware S3 en GuardDuty

GuardDuty Malware Protection for S3 monitorea continuamente las nuevas subidas a S3. En el caso de los objetos que existían antes de activar la protección, o para volver a escanear los objetos previamente escaneados, puede iniciar un análisis de malware de S3 bajo demanda una vez que haya activado el plan de protección contra GuardDuty malware para su depósito.

On-demand La detección de malware utiliza la función de IAM del plan de protección contra malware para acceder a los objetos y aplicar la configuración. El análisis anulará cualquier prefijo configurado en el plan de protección contra malware para el paquete.

### Note

La cuota de protección contra malware para S3 se aplica al análisis de malware bajo demanda. Para obtener más información, consulte [Cuotas en la protección contra malware para S3](#).

Para obtener más información sobre los precios, consulte [Precios y costo de uso de la protección contra malware para S3](#).



## Requisitos previos

Antes de iniciar un análisis de software malicioso bajo demanda, su cuenta debe cumplir los siguientes requisitos previos:

- La protección contra malware para S3 está habilitada en el depósito de destino. Para obtener más información, consulte [Configurar la protección contra malware para S3 para el bucket](#).
- La [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) política se adjunta al usuario de IAM o al rol de IAM que invoca la API.

## Inicie un análisis de malware bajo demanda

Utilice la operación [SendObjectMalwareScan](#) API, que requiere la ruta del objeto S3 como entrada.

### API/CLI

Puede escanear la última versión del objeto o especificar una versión concreta para escanearlo.

Para escanear una versión específica de un objeto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket":  
  "amzn-s3-demo-bucket", "Key": "APKAEIBAERJR2EXAMPLE", "VersionId":  
  "d41d8cd98f00b204e9800998eEXAMPLE"}'
```

Para escanear la versión más reciente de un objeto:

```
aws guardduty send-object-malware-scan --s3-object '{"Bucket": "amzn-s3-demo-  
bucket", "Key": "APKAEIBAERJR2EXAMPLE"}'
```

### Important

Una llamada a la API correcta confirma que se ha aceptado la solicitud de escaneo. Sin embargo, es importante supervisar los resultados del escaneo para garantizar que se complete correctamente e identificar cualquier problema, como errores al acceder al objeto. Para obtener más información, consulte [Supervisión de los análisis de objetos de S3 en la protección contra malware para S3](#).

# Utilizar el control de acceso basado en etiquetas (TBAC) con la protección contra malware para S3

Al habilitar la protección contra malware para S3 para el bucket, podrá optar por habilitar el etiquetado. Tras intentar escanear un objeto S3 recién cargado en el depósito seleccionado, GuardDuty añade una etiqueta al objeto escaneado para indicar el estado del análisis de malware. Habilitar el etiquetado conlleva un costo de uso directo. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).

GuardDuty utiliza una etiqueta predefinida con la clave como `GuardDutyMalwareScanStatus` y el valor como uno de los estados de detección de malware. Para obtener información sobre estos valores, consulte [the section called “Estado potencial de análisis de objeto de S3 y estado del producto”](#).

Consideraciones GuardDuty para añadir una etiqueta a su objeto S3:

- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto. Para obtener más información, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Si las 10 etiquetas ya están en uso, no GuardDuty se puede añadir la etiqueta predefinida al objeto escaneado. GuardDuty también publica el resultado del escaneo en el bus de EventBridge eventos predeterminado. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

- Si la función de IAM seleccionada no incluye el permiso para GuardDuty etiquetar el objeto de S3, ni siquiera con el etiquetado activado en el depósito protegido, no GuardDuty podrá añadir una etiqueta a este objeto de S3 escaneado. Para obtener más información sobre el permiso de rol de IAM necesario para el etiquetado, consulte [Crear o actualizar la política del rol de IAM](#).

GuardDuty también publica el resultado del escaneo en el bus de EventBridge eventos predeterminado. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

## Agregar TBAC en el recurso del bucket de S3

Puede utilizar las políticas de recursos de bucket de S3 para administrar el control de acceso basado en etiquetas (TBAC) para los objetos de S3. Puede proporcionar acceso a usuarios específicos

para acceder y leer el objeto de S3. Si tiene una organización que se creó mediante el uso AWS Organizations, debe garantizar que nadie pueda modificar las etiquetas añadidas por ella GuardDuty. Para obtener más información, consulte [Impedir que las etiquetas sean modificadas salvo por las entidades principales autorizadas](#) en la Guía del usuario de AWS Organizations . El ejemplo utilizado en el tema vinculado menciona ec2. Cuando utilice este ejemplo, *ec2* sustitúyalo por s3.

En la siguiente lista se explica lo que puede hacer mediante TBAC:

- Impida que todos los usuarios, excepto la entidad principal del servicio de protección contra malware para S3, lean los objetos de S3 que aún no estén etiquetados con el siguiente par de clave y valor de etiqueta:

GuardDutyMalwareScanStatus:*Potential key value*

- Solo se GuardDuty permite añadir la clave de etiqueta GuardDutyMalwareScanStatus con un valor como resultado del escaneo a un objeto S3 escaneado. La siguiente plantilla de política puede autorizar a determinados usuarios con acceso a anular potencialmente el par de clave y valor de la etiqueta.

Ejemplo de política de recursos del bucket de S3:

Sustituya los siguientes valores de marcador en la política de ejemplo:

- *IAM-role-name*- Indique en su bucket la función de IAM que utilizó para configurar la protección contra malware para S3.
- *555555555555*- Proporcione la información Cuenta de AWS asociada al depósito protegido.
- *amzn-s3-demo-bucket*- Proporcione el nombre del depósito protegido.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "NoReadUnlessClean",
    "Effect": "Deny",
    "NotPrincipal": {
      "AWS": [
        "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
```

```

        "arn:aws:iam::555555555555:role/IAM-role-name"
    ],
    },
    "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
        "StringNotEquals": {
            "s3:ExistingObjectTag/GuardDutyMalwareScanStatus":
"NO_THREATS_FOUND"
        }
    },
    {
        "Sid": "OnlyGuardDutyCanTagScanStatus",
        "Effect": "Deny",
        "NotPrincipal": {
            "AWS": [
                "arn:aws:sts::555555555555:assumed-role/IAM-role-name/
GuardDutyMalwareProtection",
                "arn:aws:iam::555555555555:role/IAM-role-name"
            ]
        },
        "Action": "s3:PutObjectTagging",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "s3:RequestObjectTagKeys": "GuardDutyMalwareScanStatus"
            }
        }
    }
]
}

```

Podrá obtener más información sobre el etiquetado del recurso S3 en [Etiquetado y políticas de control de acceso](#).

## Consulta y lectura del estado del bucket protegido

Después de habilitar la protección contra malware para S3 para un bucket, el estado indica si la característica está configurada y funciona según lo esperado. Este estado está asociado a un identificador (ID) único del plan de protección contra malware. GuardDuty crea este ID en el momento de activar la función.

Utilice el siguiente procedimiento para ver el estado del bucket protegido:

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Protección contra malware para S3.
3. En la tabla Buckets protegidos, consulte la columna Estado correspondiente a su bucket de S3.

En la siguiente tabla se indican y describen los valores del estado asociados al recurso del plan de protección contra malware. Si entiendes qué significan estos estados para tu depósito protegido, podrás asegurarte de que se GuardDuty inicia un análisis automático de malware cuando se carga un objeto.

| Status                   | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activo                   | <p>El bucket de S3 se ha configurado correctamente con la protección contra malware para S3.</p> <p>Cuando el estado es Activo, los cambios en el rol de IAM (eliminación o modificación de permisos) no actualizarán el estado a Advertencia ni Error. Recomendamos supervisar el estado del análisis de forma continua mediante cualquiera de los métodos descritos en <a href="#">Supervisión de los análisis de objetos de S3</a>.</p> |
| Advertencia <sup>*</sup> | <p>La protección contra malware para S3 se diseñó de modo que no se vea afectada cuando aparezca una advertencia. Cuando GuardDuty detecte un nuevo objeto de S3, iniciará un análisis de malware. Después de iniciar el análisis correctamente, es posible que el valor de la columna Estado tarde unos minutos en</p>                                                                                                                    |

| Status             | Description (Descripción)                                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | cambiar a Activo. Recibirá una EventBridge notificación cuando se actualice el valor de la columna de estado.                                            |
| Error <sup>*</sup> | El bucket no está protegido. No se completará ninguno de los análisis de malware asociados a este bucket S3. Puede haber una o más causas raíz posibles. |

\* Para obtener información sobre posibles problemas y los pasos correspondientes para resolverlos, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

## Supervisión de los análisis de objetos de S3 en la protección contra malware para S3

Al utilizar Malware Protection para S3 con un ID de GuardDuty detector, si su objeto de Amazon S3 es potencialmente malicioso, GuardDuty se generará [Tipo de resultado de la protección contra malware para S3](#). Con la GuardDuty consola y las API, puede ver los resultados generados. Para obtener información para comprender este tipo de resultado, consulte [Detalles de los resultados](#).

Si se utiliza Malware Protection para S3 sin activarla GuardDuty (sin ID de detector), aunque el objeto escaneado de Amazon S3 sea potencialmente malicioso, no GuardDuty se detectará nada.

### Contenido

- [Estado potencial de análisis de objeto de S3 y estado del producto](#)
- [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#)
- [Supervisión de los escaneos de objetos de S3 con etiquetas GuardDuty gestionadas](#)
- [Métricas de estado del escaneo de objetos de S3 en CloudWatch](#)

## Estado potencial de análisis de objeto de S3 y estado del producto

Esta sección explica los valores potenciales del estado de análisis de objetos de S3 y los valores del producto del análisis.

Un estado de análisis de objeto de S3 indica el estado del análisis de malware, como completado, omitido o fallido.

Un estado del producto del análisis de malware de objeto de S3 indica el producto del análisis basado en el valor del estado del análisis. Cada valor del estado del producto del análisis de malware se asigna a un estado de análisis.

La siguiente lista proporciona los valores potenciales del producto del análisis de objetos de S3. Si ha habilitado el etiquetado, puede supervisar el producto del análisis mediante [Utilizar etiquetas de objetos de S3](#). Después del análisis, el valor de la etiqueta tendrá uno de los siguientes valores del producto del análisis.

Valores potenciales del estado del producto del análisis de malware de objetos de S3.

- NO\_THREATS\_FOUND— no GuardDuty detectó ninguna amenaza potencial asociada al objeto escaneado.
- THREATS\_FOUND— GuardDuty detectó una amenaza potencial asociada al objeto escaneado.
- UNSUPPORTED: hay algunas razones por las que la protección contra malware para S3 omitirá un análisis. Por ejemplo, archivos protegidos con contraseña, archivos con tasas de compresión extremadamente altas, [Protección contra malware para las cuotas de S3](#) y la incompatibilidad con determinadas características de Amazon S3. Para obtener más información, consulte [Capacidades de la protección contra malware para S3](#).
- ACCESS\_DENIED— no GuardDuty puede acceder a este objeto para escanearlo. Compruebe los permisos de rol de IAM asociados a este bucket. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).

Si ha habilitado el etiquetado de objetos de S3 posterior al análisis, consulte [Solucionar errores en el etiquetado posterior al análisis de objetos de S3](#).

- FAILED— no GuardDuty se puede realizar un análisis de malware en este objeto debido a un error interno.

La siguiente lista proporciona los valores potenciales del estado de análisis de objetos de S3 y su asignación al producto del análisis de objetos de S3.

Valores potenciales del estado de análisis de objetos de S3.

- Completado: el análisis se completó correctamente e indica si el objeto S3 tiene malware. En este caso, el valor potencial del producto del análisis de objetos de S3 podría ser THREATS\_FOUND o NO\_THREATS\_FOUND.

- **Omitido:** GuardDuty omite un análisis de malware cuando el análisis de este objeto de S3 no es compatible con Malware Protection for S3 o GuardDuty no tiene acceso al objeto de S3 cargado en el depósito seleccionado.

En este caso, el valor potencial del producto del análisis de objetos de S3 podría ser `UNSUPPORTED` o `ACCESS_DENIED`.

GuardDuty también omitirá el análisis si se elimina la función de IAM requerida.

- **Fallo:** similar al valor del resultado del escaneo de objetos `S3FAILED`, este estado de escaneo significa que no GuardDuty se pudo realizar un escaneo de malware en el objeto S3 debido a un error interno.

Cuando el estado del escaneo es `SKIPPED`, la EventBridge notificación del resultado del escaneo de objetos de S3 incluye un `statusReasons` campo dentro de `scanResultDetails`. Este campo es una lista de cadenas que proporciona el motivo específico por el que se omitió el escaneo. En la siguiente tabla se describen los `statusReasons` valores posibles.

| Motivo del estado                        | Estado del resultado del escaneo | Description (Descripción)                                                                                                                                                                                                                                                  |
|------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>UNAUTHORIZED_TO_GET_OBJECT</code>  | <code>ACCESS_DENIED</code>       | Malware Protection for S3 no tiene permiso para leer el objeto S3 o el objeto S3 no existe. Compruebe que la función de IAM asociada al bucket protegido tenga los permisos necesarios y que cualquier AWS KMS política de bucket permita que la función descifre objetos. |
| <code>UNAUTHORIZED_TO_ASSUME_ROLE</code> | <code>ACCESS_DENIED</code>       | Malware Protection for S3 no puede asumir la función de IAM configurada para el depósito protegido. Compruebe que la política de confianza del rol permita que Malware Protection for S3 asuma el rol.                                                                     |
| <code>SSE_C_ENCRYPTED_OBJECT</code>      | <code>ACCESS_DENIED</code>       | El objeto S3 se cifra con una clave de cifrado proporcionada por el cliente (SSE-C). GuardDuty no puede acceder a los objetos                                                                                                                                              |



| Motivo del estado              | Estado del resultado del escaneo | Description (Descripción)                                                                                                                                                                                         |
|--------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                |                                  | cifrados con. SSE-C Para obtener más información, consulte <a href="#">Compatibilidad con las características de Amazon S3</a> .                                                                                  |
| OBJECT_E_TAG_CHANGED           | ACCESS_DENIED                    | La ETag del objeto S3 cambió entre el momento en que se inició el escaneo y el momento en que se GuardDuty intentó leer el objeto. Se escaneará la siguiente carga o la nueva versión.                            |
| BUCKET_NOT_FOUND               | ACCESS_DENIED                    | El depósito S3 asociado al escaneo ya no existe.                                                                                                                                                                  |
| UNSUPPORTED_STORAGE_CLASS      | UNSUPPORTED                      | El objeto S3 utiliza una clase de almacenamiento que no es compatible con Malware Protection for S3. Para obtener más información, consulte <a href="#">Compatibilidad con las características de Amazon S3</a> . |
| OBJECT_SIZE_LIMIT_EXCEEDED     | UNSUPPORTED                      | El tamaño del objeto S3 supera el límite máximo de tamaño de archivo de Malware Protection for S3. Para obtener más información, consulte <a href="#">Protección contra malware para las cuotas de S3</a> .       |
| PASSWORD_PROTECTED             | UNSUPPORTED                      | El objeto está protegido por contraseña.                                                                                                                                                                          |
| EXTRACTED_FILE_LIMIT_EXCEEDED  | UNSUPPORTED                      | El archivo contiene más archivos que el límite máximo permitido. Para obtener más información, consulte <a href="#">Protección contra malware para las cuotas de S3</a> .                                         |
| EXTRACTED_LEVEL_LIMIT_EXCEEDED | UNSUPPORTED                      | El archivo supera la profundidad de anidación máxima permitida.                                                                                                                                                   |

| Motivo del estado               | Estado del resultado del escaneo | Description (Descripción)                                                                                                                                                                                |
|---------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EXTRACTED_BYTE_LIMIT_EXCEEDED   | UNSUPPORTED                      | El contenido del archivo extraído supera el tamaño máximo de bytes permitido. Para obtener más información, consulte <a href="#">Protección contra malware para las cuotas de S3</a> .                   |
| EXTRACTION_RATIO_LIMIT_EXCEEDED | UNSUPPORTED                      | El archivo tiene una relación de compresión extremadamente alta que supera el límite permitido. Para obtener más información, consulte <a href="#">Protección contra malware para las cuotas de S3</a> . |

## Supervisión de escaneos de objetos de S3 con Amazon EventBridge

Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones Software-as-a-Service (SaaS) y AWS servicios, y dirige esos datos a destinos como Lambda. Esto le permite monitorear los eventos que ocurren en los servicios y crear arquitecturas basadas en eventos. Para obtener más información, consulta la [Guía del EventBridge usuario de Amazon](#).

Como cuenta propietaria de un bucket de S3 protegido con Malware Protection for S3, GuardDuty publica EventBridge las notificaciones en el bus de eventos predeterminado en los siguientes escenarios:

- Cambios en el estado de los recursos del plan de protección contra malware para cualquiera de los buckets protegidos. Para obtener información sobre los diversos estados, consulte [Consulta y lectura del estado del bucket protegido](#).

Para configurar la regla Amazon EventBridge (EventBridge) para el estado del recurso, consulte [Estado del recurso del plan de protección contra malware](#).

- El resultado del escaneo de objetos de S3 se publica en el bus de EventBridge eventos predeterminado.

El campo `s3Throttled` indica si hubo o no un retraso en la carga o recuperación de almacenamiento desde Amazon S3. El valor `true` indica que hubo un retraso, y `false` indica que no hubo retraso.

Si `s3Throttled` es `true` para el producto del análisis, Amazon S3 recomienda configurar los prefijos de manera que ayuden a reducir las transacciones por segundo (TPS) para cada prefijo. Para obtener más información, consulte [Patrones de diseño de prácticas recomendadas: optimización del rendimiento de Amazon S3](#) en la Guía del usuario de Amazon S3.

Para configurar la regla Amazon EventBridge (EventBridge) para los resultados del escaneo de objetos de S3, consulte [Producto del análisis del objeto S3](#).

- Se produce un evento de error en la etiqueta posterior al análisis debido a las siguientes razones:
  - El rol de IAM no tiene los permisos necesarios para etiquetar el objeto.

La [Agregar permisos de política de IAM](#) plantilla incluye el permiso para GuardDuty etiquetar un objeto.

- El recurso del bucket o el objeto especificado en el rol de IAM ya no existe.
- El objeto de S3 asociado ya ha alcanzado el límite máximo de etiquetas. Para obtener más información sobre el límite de etiquetas, consulte [Categorizar el almacenamiento mediante etiquetas](#) en la Guía del usuario de Amazon S3.

Para configurar la regla Amazon EventBridge (EventBridge) para los eventos de error de etiquetas posteriores al escaneo, consulte [Post-scan etiqueta los eventos de error](#).

## Configura reglas EventBridge

Puede configurar EventBridge reglas en su cuenta para enviar a otra Servicio de AWS persona el estado del recurso, los eventos de error de etiquetas posteriores al escaneo o el resultado del escaneo de objetos de S3. Como cuenta de GuardDuty administrador delegado, recibirá la notificación del estado de los recursos del plan de protección contra malware cuando se produzca un cambio en el estado.

Se aplicará el EventBridge precio estándar. Para obtener más información, consulta los [EventBridge precios de Amazon](#).

Todos los valores que aparecen en el ejemplo *red* son marcadores de posición. Estos valores cambiarán según los valores de la cuenta y según se detecte o no malware.

## Temas

- [Estado del recurso del plan de protección contra malware](#)
- [Producto del análisis del objeto S3](#)
- [Post-scan etiqueta los eventos de error](#)

### Estado del recurso del plan de protección contra malware

Puede crear un patrón de EventBridge eventos en función de los siguientes escenarios:

### Valores potenciales de **detail-type**

- "GuardDuty Malware Protection Resource Status Active"
- "GuardDuty Malware Protection Resource Status Warning"
- "GuardDuty Malware Protection Resource Status Error"

### Patrón del evento

```
{
  "detail-type": ["potential detail-type"],
  "source": ["aws.guarddduty"]
}
```

### Ejemplo de esquema de notificaciones para **GuardDuty Malware Protection Resource Status Active**:

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status Active",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guarddduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
```

```

        "bucketName": "amzn-s3-demo-bucket"
      },
      "resourceStatus": "ACTIVE"
    }
  }
}

```

### Ejemplo de esquema de notificaciones para **GuardDuty Malware Protection Resource Status Warning**:

```

{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "GuardDuty Malware Protection Resource Status warning",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-02-28T01:01:01Z",
    "s3BucketDetails": {
      "bucketName": "amzn-s3-demo-bucket"
    },
    "resourceStatus": "WARNING",
    "statusReasons": [
      {
        "code": "INSUFFICIENT_TEST_OBJECT_PERMISSIONS"
      }
    ]
  }
}

```

### Ejemplo de esquema de notificaciones para **GuardDuty Malware Protection Resource Status Error**:

```

{
  "version": "0",
  "id": "fc7a35b7-83bd-3c1f-ecfa-1b8de9e7f7d2",
  "detail-type": "GuardDuty Malware Protection Resource Status Error",
  "source": "aws.guardduty",

```

```

"account": "111122223333",
"time": "2017-12-22T18:43:48Z",
"region": "us-east-1",
"resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
"detail": {
  "schemaVersion": "1.0",
  "eventTime": "2024-02-28T01:01:01Z",
  "s3BucketDetails": {
    "bucketName": "amzn-s3-demo-bucket"
  },
  "resourceStatus": "ERROR",
  "statusReasons": [
    {
      "code": "EVENTBRIDGE_MANAGED_EVENTS_DELIVERY_DISABLED"
    }
  ]
}
}

```

Según el motivo de resourceStatus ERROR, se completará el valor statusReasons.

Para obtener información sobre los pasos de solución de problemas para las siguientes advertencias y errores, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

Producto del análisis del objeto S3

```

{
  "detail-type": ["GuardDuty Malware Protection Object Scan Result"],
  "source": ["aws.guardduty"]
}

```

Cuando scanStatus está SKIPPED, scanResultDetails incluye un statusReasons campo que indica el motivo específico por el que se omitió el escaneo. Para obtener información sobre los valores posibles, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

Ejemplo de esquema de notificaciones para **NO\_THREATS\_FOUND**:

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",

```

```

"source": "aws.guardduty",
"account": "111122223333",
"time": "2024-02-28T01:01:01Z",
"region": "us-east-1",
"resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
"detail": {
  "schemaVersion": "1.0",
  "scanStatus": "COMPLETED",
  "resourceType": "S3_OBJECT",
  "s3objectDetails": {
    "bucketName": "amzn-s3-demo-bucket",
    "objectKey": "APKAEIBAERJR2EXAMPLE",
    "eTag": "ASIAI44QH8DHBEXAMPLE",
    "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
    "s3Throttled": false
  },
  "scanResultDetails": {
    "scanResultStatus": "NO_THREATS_FOUND",
    "threats": null,
    "statusReasons": null
  }
}
}

```

### Ejemplo de esquema de notificaciones para **THREATS\_FOUND**:

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0171419",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {
      "bucketName": "amzn-s3-demo-bucket",

```

```

      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "THREATS_FOUND",
      "threats": [
        {
          "name": "EICAR-Test-File (not a virus)"
        }
      ],
      "statusReasons": null
    }
  }
}

```

#### Note

El campo `scanResultDetails.Threats` contiene solo una amenaza. De forma predeterminada, el análisis de protección contra malware para S3 indica la primera amenaza detectada. Después de esto, el `scanStatus` se establece en `COMPLETED`.

Esquema de notificaciones de ejemplo para el estado del producto del análisis **UNSUPPORTED** (Omitido):

```

{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "S3_OBJECT",
    "s3objectDetails": {

```



```

        "bucketName": "amzn-s3-demo-bucket",
        "objectKey": "APKAEIBAERJR2EXAMPLE",
        "eTag": "ASIAI44QH8DHBEXAMPLE",
        "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
        "s3Throttled": false
    },
    "scanResultDetails": {
        "scanResultStatus": "UNSUPPORTED",
        "threats": null,
        "statusReasons": ["PASSWORD_PROTECTED"]
    }
}
}

```

Esquema de notificaciones de ejemplo para el estado del producto del análisis **ACCESS\_DENIED** (Omitido):

```

{
    "version": "0",
    "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
    "detail-type": "GuardDuty Malware Protection Object Scan Result",
    "source": "aws.guardduty",
    "account": "111122223333",
    "time": "2024-02-28T01:01:01Z",
    "region": "us-east-1",
    "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/b4c7f464ab3a4EXAMPLE"],
    "detail": {
        "schemaVersion": "1.0",
        "scanStatus": "SKIPPED",
        "resourceType": "S3_OBJECT",
        "s3ObjectDetails": {
            "bucketName": "amzn-s3-demo-bucket",
            "objectKey": "APKAEIBAERJR2EXAMPLE",
            "eTag": "ASIAI44QH8DHBEXAMPLE",
            "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
            "s3Throttled": false
        },
        "scanResultDetails": {
            "scanResultStatus": "ACCESS_DENIED",
            "threats": null,
            "statusReasons": ["SSE_C_ENCRYPTED_OBJECT"]
        }
    }
}

```

```
}
}
```

Esquema de notificaciones de ejemplo para el estado del producto del análisis **FAILED**:

```
{
  "version": "0",
  "id": "72c7d362-737a-6dce-fc78-9e27a0EXAMPLE",
  "detail-type": "GuardDuty Malware Protection Object Scan Result",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2024-02-28T01:01:01Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guardduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "FAILED",
    "resourceType": "S3_OBJECT",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "APKAEIBAERJR2EXAMPLE",
      "eTag": "ASIAI44QH8DHBEXAMPLE",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "scanResultDetails": {
      "scanResultStatus": "FAILED",
      "threats": null,
      "statusReasons": null
    }
  }
}
```

Post-scan etiqueta los eventos de error

Patrón del evento:

```
{
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guarddduty"
}
```

Ejemplo de esquema de notificaciones para **ACCESS\_DENIED**:

```
{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guarddduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
    "eventTime": "2024-06-10T16:16:08Z",
    "s3ObjectDetails": {
      "bucketName": "amzn-s3-demo-bucket",
      "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
      "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
      "versionId": "d41d8cd98f00b204e9800998eEXAMPLE",
      "s3Throttled": false
    },
    "postScanActions": [{
      "actionType": "TAGGING",
      "failureReason": "ACCESS_DENIED"
    }]
  }
}
```

Ejemplo de esquema de notificaciones para **MAX\_TAG\_LIMIT\_EXCEEDED**:

```
{
  "version": "0",
  "id": "746acd83-d75c-5b84-91d2-dad5f13ba0d7",
  "detail-type": "GuardDuty Malware Protection Post Scan Action Failed",
  "source": "aws.guarddduty",
  "account": "111122223333",
  "time": "2024-06-10T16:16:08Z",
  "region": "us-east-1",
  "resources": ["arn:aws:guarddduty:us-east-1:111122223333:malware-protection-plan/
b4c7f464ab3a4EXAMPLE"],
  "detail": {
    "schemaVersion": "1.0",
```

```
"eventTime": "2024-06-10T16:16:08Z",
"s3objectDetails": {
  "bucketName": "amzn-s3-demo-bucket",
  "objectKey": "2024-03-10-16-16-00-7D723DE8DBE9Y2E0",
  "eTag": "0e9eeec810ad8b61d69112c15c2a5hb6",
  "versionId" : "d41d8cd98f00b204e9800998eEXAMPLE",
  "s3Throttled": false
},
"postScanActions": [{
  "actionType": "TAGGING",
  "failureReason": "MAX_TAG_LIMIT_EXCEEDED"
}]
}
```

Para solucionar estos motivos de error, consulte [Solucionar errores en el etiquetado posterior al análisis de objetos de S3](#).

## Supervisión de los escaneos de objetos de S3 con etiquetas GuardDuty gestionadas

Utilice la opción de habilitar el etiquetado para GuardDuty poder añadir etiquetas a su objeto de Amazon S3 después de completar el análisis de malware.

### Consideraciones para habilitar el etiquetado

- Al GuardDuty etiquetar sus objetos de S3, hay un costo de uso asociado. Para obtener más información, consulte [Precios y costo de uso de la protección contra malware para S3](#).
- Debe conservar los permisos de etiquetado necesarios para su función de IAM preferida asociada a este segmento; de lo contrario, no GuardDuty podrá añadir etiquetas a los objetos escaneados. El rol de IAM ya incluye los permisos para agregar etiquetas a los objetos de S3 analizados. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).
- De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto de S3. Para obtener más información, consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\)](#).

Después de habilitar el etiquetado para un bucket de S3 o prefijos específicos, cualquier objeto nuevo cargado que sea analizado tendrá una etiqueta asociada en el siguiente formato de par de clave y valor:

GuardDutyMalwareScanStatus:*Scan-Result-Status*

Para obtener información sobre los posibles valores de las etiquetas, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

## Solucionar problemas de errores de etiquetas posteriores al análisis de objetos de S3 en la protección contra malware para S3

Esta sección solo se aplica si ha [Habilite el etiquetado para los objetos analizados](#) en el bucket protegido.

Al GuardDuty intentar añadir una etiqueta al objeto de S3 escaneado, la acción de etiquetar puede provocar un error. Las posibles razones por las que esto puede ocurrir en el bucket son `ACCESS_DENIED` y `MAX_TAG_LIMIT_EXCEEDED`. Utilice los siguientes temas para comprender las posibles razones de estos errores en el etiquetado posterior al análisis y para solucionarlos.

### `ACCESS_DENIED`

La siguiente lista proporciona posibles razones que pueden causar este problema:

- Falta el permiso para la función de IAM utilizada para este bucket de S3 protegido.  
AllowPostScanTag Verificar que el rol de IAM asociado utilice esta política de bucket. Para obtener más información, consulte [Crear o actualizar la política del rol de IAM](#).
- La política de bucket de S3 protegido no permite añadir etiquetas GuardDuty a este objeto.
- El objeto de S3 analizado ya no existe.

### `MAX_TAG_LIMIT_EXCEEDED`

De forma predeterminada, puede asociar hasta 10 etiquetas a un objeto de S3. Para obtener más información, consulte la sección Consideraciones sobre GuardDuty cómo añadir una etiqueta a un objeto [Habilite el etiquetado para los objetos analizados](#) de S3.

## Métricas de estado del escaneo de objetos de S3 en CloudWatch

Puede monitorizar el GuardDuty uso CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se retienen durante 15 meses, lo que le permite acceder a información histórica y obtener una mejor perspectiva sobre el rendimiento de la protección contra malware para S3. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Las CloudWatch métricas de Malware Protection for S3 están disponibles a nivel de recursos. Puede consultar estas métricas por cada recurso protegido de manera independiente. Las métricas se informan en el espacio de nombres AWS/GuardDuty/MalwareProtection. Puede configurar alarmas en recursos específicos para supervisar la postura de seguridad.

#### Métricas del estado del análisis de malware

| Métrica            | Descripción                                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CompletedScanCount | <p>Cantidad de análisis de malware de objetos S3 que se completaron en un periodo determinado.</p> <p>Dimensiones válidas:</p> <ul style="list-style-type: none"><li>Malware Protection Plan Id</li></ul> <p>Resource Name</p> <p>Unidades: recuento</p>                            |
| FailedScanCount    | <p>Cantidad de análisis de objetos de S3 maliciosos en los que se produjo un error en un intervalo de tiempo determinado.</p> <p>Dimensiones válidas:</p> <ul style="list-style-type: none"><li>Malware Protection Plan Id</li></ul> <p>Resource Name</p> <p>Unidades: recuento</p> |
| SkippedScanCount   | <p>Cantidad de análisis de malware de objetos de S3 que se omitieron en un periodo determinado.</p> <p>Dimensiones válidas:</p> <ul style="list-style-type: none"><li>Malware Protection Plan Id</li></ul>                                                                          |

Resource Name

Skipped Reason

Valores potenciales de

- Unsupported
- MissingPermissions

Unidades: recuento

## Métricas de productos de análisis de malware

InfectedScanCount

La cantidad de análisis de malware en objetos de S3 que detectaron objetos potencialmente maliciosos en un periodo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

CompletedScanBytes

La cantidad de bytes de objetos de S3 analizados en un período de tiempo determinado.

Dimensiones válidas:

- Malware Protection Plan Id

Resource Name

Unidades: recuento

 Note

De forma predeterminada, las estadísticas de las CloudWatch métricas son AVG.

Las siguientes dimensiones son compatibles con las métricas de protección contra malware para S3.

| Dimensión                  | Descripción                                                                                                                                                                                         |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Malware Protection Plan Id | El identificador único que se asocia al recurso del plan de protección contra malware que se GuardDuty crea para el recurso protegido.                                                              |
| Resource Name              | El nombre del recurso protegido.                                                                                                                                                                    |
| Skipped Reason             | La razón por la que se ha omitido un análisis de malware de objetos de S3.<br><br>Valores potenciales de <ul style="list-style-type: none"><li>• Unsupported</li><li>• MissingPermissions</li></ul> |

Para obtener información sobre cómo acceder a estas métricas y consultarlas, consulta [Cómo usar CloudWatch las métricas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

Para obtener información sobre la configuración de alarmas, consulta [Uso de CloudWatch alarmas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

## Resolución de problemas

### Contenido

- [Solución de problemas sobre el estado del plan de protección contra malware](#)
- [Solución de problemas de análisis de malware bajo demanda](#)



## Solución de problemas sobre el estado del plan de protección contra malware

Para cualquier depósito protegido, GuardDuty muestra el estado en función de la clasificación. Por ejemplo, si un depósito protegido tiene problemas en las categorías de error y advertencia, GuardDuty mostrará primero el problema asociado al estado de error.

En la siguiente lista aparecen los errores y las advertencias para el estado del plan de protección contra malware.

### Errores

- [EventBridge la notificación está deshabilitada para este bucket de S3](#)
- [EventBridge Falta una regla gestionada para recibir los eventos del bucket de S3](#)
- [El bucket de S3 ya no existe](#)

### Advertencia

[No se pudo colocar el objeto de prueba](#)

### EventBridge la notificación está deshabilitada para este bucket de S3

El código de motivo de estado asociado es

EVENTBRIDGE\_MANAGED\_EVENTS\_DELIVERY\_DISABLED.

### Detalle del estado

GuardDuty EventBridge se utiliza para recibir una notificación cuando se carga un objeto nuevo en este depósito de S3. Este permiso falta en el rol de IAM.

### Pasos para solucionar el problema

Opción 1: agregue la siguiente instrucción de permiso al rol de IAM:

```
{
  "Sid": "AllowEnableS3EventBridgeEvents",
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketNotification",
    "s3:GetBucketNotification"
  ],
  "Resource": [
```

```
    "arn:aws:s3:::amzn-s3-demo-bucket"  
  ]  
}
```

Reemplace *amzn-s3-demo-bucket* por el nombre de su bucket de Amazon S3.

Opción 2: Habilitar la EventBridge notificación mediante la consola Amazon S3

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. En la página Buckets, en la pestaña Buckets de uso general, seleccione el nombre del bucket asociado a este error.
3. En esta página del bucket, elija la pestaña Propiedades.
4. En la EventBridge sección Amazon, selecciona Editar.
5. En la EventBridge página Editar Amazon, en Enviar notificación a Amazon EventBridge para todos los eventos de este grupo, selecciona Activado.
6. Seleccione Save changes (Guardar cambios).

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

## EventBridge Falta una regla gestionada para recibir los eventos del bucket de S3

El código de motivo de estado asociado es EVENTBRIDGE\_MANAGED\_RULE\_DISABLED.

### Detalle del estado

Faltan los permisos de la regla EventBridge administrada para administrar la configuración de la EventBridge regla.

### Pasos para solucionar el problema

Agregue la siguiente instrucción de permiso al rol de IAM:

```
{  
  "Sid": "AllowManagedRuleToSendS3EventsToGuardDuty",  
  "Effect": "Allow",  
  "Action": [  
    "events:PutRule",  
    "events>DeleteRule",  
    "events:PutTargets",
```

```
        "events:RemoveTargets"
      ],
      "Resource": [
        "arn:aws:events:*:*:rule/D0-NOT-DELETE-AmazonGuardDutyMalwareProtectionS3*"
      ],
      "Condition": {
        "StringEquals": {
          "events:ManagedBy": "malware-protection-plan.guardduty.amazonaws.com"
        }
      }
    }
  }
```

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

## El bucket de S3 ya no existe

El código de motivo de estado asociado es PROTECTED\_RESOURCE\_DELETED.

### Detalle del estado

Se eliminó este bucket de S3 de la cuenta y ya no existe.

### Paso para solucionar el problema

Si la eliminación del bucket de S3 no fue deliberada, puede crear un nuevo bucket desde la consola de Amazon S3.

Después de crear el bucket correctamente, habilite la protección contra malware para S3. Para ello, siga los pasos que se indican en la página [Configurar la protección contra malware para S3 para el bucket](#).

## No se pudo colocar el objeto de prueba

El código de motivo de estado asociado es INSUFFICIENT\_TEST\_OBJECT\_PERMISSIONS.

### Note

El permiso para agregar un objeto de prueba es opcional. La ausencia de este permiso en el rol de IAM no impide que la protección contra malware para S3 inicie el análisis de malware en los objetos recién cargados. Después de que se inicie correctamente un análisis,

el estado del plan de protección contra malware puede tardar unos minutos en cambiar de Advertencia a Activo.

Si el rol de IAM ya incluye este permiso, entonces esta advertencia indica una política de bucket de Amazon S3 restrictiva que no permite el acceso de IAM para colocar el objeto de prueba en este bucket de S3.

## Detalle del estado

Para validar la configuración del depósito seleccionado, GuardDuty coloca un objeto de prueba en el depósito.

## Pasos para solucionar el problema

Puede optar por actualizar el rol de IAM para incluir los permisos que faltan. Al rol de IAM seleccionado, añada los siguientes permisos para GuardDuty poder colocar el objeto de prueba en el recurso seleccionado:

```
{
  "Sid": "AllowPutValidationObject",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket/malware-protection-resource-validation-object"
  ]
}
```

Reemplace *amzn-s3-demo-bucket* por el nombre de su bucket de Amazon S3. Para obtener más información sobre los permisos de roles de IAM, consulte [Crear o actualizar la política del rol de IAM](#).

El valor de la columna Estado puede tardar unos minutos en cambiar a Activo.

## Solución de problemas de análisis de malware bajo demanda

No se ha podido iniciar un análisis.

Asegúrese de que la solicitud de escaneo contenga una entrada válida y de que el plan de protección contra malware esté habilitado para el depósito.

## Editar el plan de protección contra malware para un bucket protegido

Es posible que tenga que editar la política de permisos de IAM que prefiera, habilitar o desactivar el etiquetado del objeto de S3 analizado, o agregar o eliminar prefijos de objetos de S3. Por ejemplo, cuando habilitó la protección contra malware para S3 para el bucket, decidió no habilitar el etiquetado del objeto de S3 analizado con el resultado del análisis. Sin embargo, ahora quiere GuardDuty añadir la etiqueta predefinida y el resultado del escaneo como valor de la etiqueta.

Elija el método de acceso que prefiera para actualizar el plan de protección contra malware para el bucket de S3 protegido.

### Console

Para editar un plan de protección contra malware

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección contra malware para S3.
3. En Buckets protegidos, seleccione el bucket para el que desea editar la configuración existente.
4. Elija Edit (Edición de).
5. Actualice la configuración y los ajustes existentes para el bucket y confirme los cambios. Para obtener información sobre la descripción y los pasos de cada sección, consulte [Habilitar la protección contra malware para S3 para el bucket](#).

Supervise la columna Estado correspondiente a este bucket protegido. Si aparece como Advertencia o Error, consulte [Solución de problemas sobre el estado del plan de protección contra malware](#).

## API/CLI

Para editar el plan de protección contra malware mediante la API o AWS CLI

- Mediante la API

Ejecute la [UpdateMalwareProtectionPlan](#) API mediante el ID del plan de protección contra malware asociado a este recurso del plan.

Para recuperar el ID del plan de protección contra malware en una región específica, puede ejecutar la [ListMalwareProtectionPlans](#) API en esa región.

- Mediante el uso de AWS CLI

La siguiente lista proporciona AWS CLI ejemplos de comandos para actualizar el recurso del plan de protección contra malware. Necesitará el ID del plan de protección contra malware asociado al bucket de S3.

### AWS CLI ejemplos de comandos

- Utilice el siguiente AWS CLI comando para activar o desactivar el etiquetado del recurso del plan de protección contra malware asociado a su bucket de S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --actions "Tagging"={"Status"="ENABLED|DISABLED"}
```

- Utilice el siguiente AWS CLI comando para añadir un prefijo de objeto al recurso del plan de protección contra malware asociado a su bucket de S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=["amzn-s3-demo-1", "amzn-s3-demo-2"]}
```

Asegúrese de incluir los prefijos de objeto existentes en este comando; de lo contrario, los GuardDuty eliminará al editar el recurso del plan de protección contra malware.

- Utilice el siguiente AWS CLI comando para eliminar un prefijo de objeto del recurso del plan de protección contra malware asociado a su bucket de S3:

```
aws guardduty update-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE --protected-resource "S3Bucket"={"ObjectPrefixes"=[""]}
```

Si aún no tiene el ID del plan de protección contra malware para este recurso, puede ejecutar el siguiente AWS CLI comando y sustituirlo *us-east-1* por la región para la que desee incluir los ID del plan de protección contra malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

## Desactivar la protección contra malware para S3 para un bucket protegido

Al deshabilitar Malware Protection for S3 para un bucket protegido, GuardDuty elimina el ID del plan de Malware Protection asociado a ese bucket. GuardDuty dejará de iniciar un análisis de malware cuando se cargue un objeto nuevo en este depósito o en uno de los prefijos de objeto seleccionados.

Si lo ha activado GuardDuty y ahora quiere suspenderlo o desactivarlo GuardDuty, consulte [Suspender o deshabilitar GuardDuty](#). Como en Malware Protection for S3 no existe el concepto de identificador de detector, la desactivación o la suspensión GuardDuty no repercuten en el estado de un depósito protegido de tu cuenta. Puede continuar el uso de la característica de protección contra malware para S3 de forma independiente con el precio estándar asociado. Para obtener más información, consulte [Revisar el costo de uso de la protección contra malware para S3](#). Para dejar de utilizar la protección contra malware para S3, deberá desactivarla para todos los buckets protegidos en la cuenta. Si quieres seguir usando GuardDuty y deshabilitar solo Malware Protection for S3 para un bucket, los siguientes pasos no afectarán a la configuración del GuardDuty servicio ni a otros planes de protección que hayas habilitado.

Elija el método de acceso que prefiera para desactivar la protección contra malware para S3 en el bucket de S3 protegido.

### Console

Para deshabilitar la protección contra malware para S3 mediante GuardDuty la consola

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Protección contra malware para S3.
3. En Buckets protegidos, seleccione el bucket para el que desea desactivar la protección contra malware para S3.

Solo puede seleccionar un bucket protegido a la vez. Para desactivar la protección contra malware para S3 para más de un bucket, siga estos pasos de nuevo para otro bucket de S3.

4. Elija Desactivar para confirmar la selección.

## API/CLI

Para deshabilitar la protección contra malware para S3 mediante la API o AWS CLI

- Mediante la API

Ejecute la [DeleteMalwareProtectionPlan](#) API mediante el ID del plan de protección contra malware asociado a este recurso del plan.

Para recuperar el ID del plan de protección contra malware, puede ejecutar la [ListMalwareProtectionPlans](#) API.

- Mediante el uso de AWS CLI

Como alternativa, puede ejecutar el siguiente AWS CLI comando para deshabilitar la protección contra malware para S3 sustituyéndolo `4cc8bf26c4d75EXAMPLE` por el ID del plan de protección contra malware asociado a este depósito de S3:

```
aws guardduty delete-malware-protection-plan --malware-protection-plan-id 4cc8bf26c4d75EXAMPLE
```

Si aún no tiene el ID del plan de protección contra malware para este bucket de S3, puede ejecutar el siguiente AWS CLI comando y `us-east-1` sustituirlo por la región para la que desee incluir los ID del plan de protección contra malware.

```
aws guardduty list-malware-protection-plans --region us-east-1
```

## Compatibilidad con las características de Amazon S3

En la siguiente tabla se especifica si la protección contra malware para S3 es compatible o no con las características de Amazon S3 enumeradas.



| ¿Hay compatibilidad disponible? | Description (Descripción)                                               |
|---------------------------------|-------------------------------------------------------------------------|
| Sí                              | Los objetos de S3 se pueden recuperar sin restaurar de forma asíncrona. |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Condicional                     | <ul style="list-style-type: none"><li>• La compatibilidad con Intelligent Tiering está disponible para objetos de S3 en los niveles Frequent, Infrequent y Archive Instance Access.</li><li>• Los niveles de inscripción Archive y Deep Archive no son compatibles.</li><li>• Intelligent Tiering siempre crea un nuevo objeto en el nivel Frequent Access. Por lo tanto, se admite el análisis de objetos durante la creación.</li><li>• Las futuras funciones de Intelligent Tiering podrían iniciar los objetos en el nivel Archive. Por lo tanto, esto no se admite.</li></ul> |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------|
| No                              | GuardDuty solo admite depósitos de uso general para la protección contra malware de S3. |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                   |
|---------------------------------|-----------------------------------------------------------------------------|
| No                              | <p>Los objetos de S3 se deben restaurar antes de poder acceder a ellos.</p> |
| No                              | <p>La protección contra malware para S3 no se admite en Outposts.</p>       |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sí                              | <p>Todos los objetos de S3 cargados se analizan en busca de malware. Si ha cargado un objeto con la versión de archivo v1 e inmediatamente ha subido otra versión sustituida por la v2, GuardDuty escaneará las versiones v1 y v2 del archivo de objeto. Sin embargo, es posible que la hora de inicio del análisis no esté en el mismo orden.</p> |
| Sí                              | <p>Si el depósito de destino es un recurso protegido, GuardDuty escaneará todos los objetos de S3 y los replicará con los prefijos protegidos y supervisados.</p>                                                                                                                                                                                  |
| No                              | <p>No puede definir una regla de replicación basada en la etiqueta del producto del análisis. Amazon S3 no admite la replicación para etiquetas, excepto durante la creación.</p>                                                                                                                                                                  |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sí                              | <p>GuardDuty admite el escaneo de malware para detectar objetos de S3 cifrados con claves administradas y administradas por el cliente. Asegúrese de que el rol de IAM incluya el permiso para utilizar la clave. Para obtener más información, consulte <a href="#">Agregar permisos de política de IAM</a>.</p> |

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| No                              | La protección contra malware para S3 no admite el análisis de objetos de S3 cifrados con claves a las que no se puede acceder. |

No

Si los objetos de Amazon S3 se cifran mediante el Cliente de cifrado de Amazon S3, no quedarán expuestos a terceros, incluida AWS. Para obtener información sobre por qué no se admite esta opción, consulte [Proteger los datos mediante el cifrado del cliente](#).

 Note

CSE-KMS los objetos cifrados se reciben como un blob cifrado donde no se puede determinar el cifrado. Por lo tanto, los GuardDuty procesa a medida que se reciben y escanea el blob cifrado como un archivo normal. GuardDuty no devuelve el estado de UNSUPPORTED escaneo de dichos objetos, a menos que alguno de ellos lo [Cuotas en la protección contra malware para S3](#) supere.

| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sí                              | Los objetos bloqueados de S3 se bloquean según WORM (única escritura, múltiples lecturas). La protección contra malware para S3 puede acceder a los objetos y analizarlos.                                                                                                                                                                        |
| Sí                              | La protección contra malware para S3 puede analizar los buckets configurados con Pago por el solicitante. El solicitante pagará las llamadas a S3. Para obtener más información, consulte <a href="#">Uso de buckets de pagos por solicitante para transferencias de almacenamiento y uso</a> en la Guía del usuario de Amazon S3.                |
| Sí                              | Puede definir políticas de ciclo de vida basadas en la etiqueta del producto del análisis. Por ejemplo, eliminar automáticamente los objetos maliciosos. Para obtener más información sobre la configuración del ciclo de vida, consulte <a href="#">Administración del ciclo de vida del almacenamiento</a> en la Guía del usuario de Amazon S3. |



| ¿Hay compatibilidad disponible? | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sí                              | Puede definir políticas de recursos de bucket basadas en la etiqueta del producto del análisis de objetos de S3. Por ejemplo, impida el acceso a los objetos de S3 que aún no se hayan escaneado o a las amenazas GuardDuty detectadas. Para obtener más información, consulte <a href="#">Utilizar el control de acceso basado en etiquetas (TBAC) con la protección contra malware para S3</a> . |

## Cuotas en la protección contra malware para S3

En esta sección se proporcionan las cuotas predeterminadas, que también se conocen como límites. A menos que se especifique, cada cuota es Region-specific. Para ver las cuotas predeterminadas específicas para el uso del GuardDuty servicio básico, consulte [GuardDuty Cuotas de Amazon](#).

En las siguientes tablas se describen las cuotas múltiples que se aplicarán a la Cuenta de AWS.

| AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                                                                                                          |
|-----------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100 GB                            | No                 | <p>El tamaño máximo del objeto S3 que GuardDuty se intentará escanear en busca de malware.</p> <p>Aunque esta cuota no se puede ajustar, si necesitas escanear objetos más grandes, ponte en contacto con nosotros AWS Support para determinar</p> |

| AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   |                    | <p>si GuardDuty puedes aumentar la cuota para tu caso de uso.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 100 GB                            | No                 | <p>La cantidad máxima de datos que GuardDuty se pueden extraer y analizar de un archivo comprimido.</p> <p>GuardDuty omitirá los archivos archivados que se extraigan a más de 100 GB.</p> <div data-bbox="933 829 1507 1333"> <p> <b>Note</b></p> <p>Los archivos con una relación de compresión extremadamente alta entre el tamaño del archivo comprimido y el tamaño del contenido extraído pueden estar sujetos a límites incluso si el tamaño del contenido extraído está por debajo de esta cuota.</p> </div> |

| AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 000                            | No                 | <p>El número máximo de archivos que GuardDuty se pueden extraer y analizar en un archivo de almacenamiento. Si el archivo contiene más de 10 000 archivos, GuardDuty tendrá que omitir el archivo archivado.</p> <div>  <b>Note</b><br/>           Estos límites pueden aplicarse a los tipos de archivos compuestos, Los tipos de archivo incluyen, entre otros, mensajes de correo electrónico codificados con extensiones multipropósito de correo de Internet (MIME), archivos Python compilados (PYC), archivos de ayuda HTML compilados (CHM), todos los instaladores y documentos de OpenDocument formato (ODF).         </div> |
| 5                                 | No                 | <p>Los niveles máximos de archivos anidados que se pueden extraer. GuardDuty Si el archivo incluye archivos anidados por encima de este valor, los GuardDuty omitirá.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                 |
|-----------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 25                                | No                 | La cantidad máxima de buckets de S3 para los que puede habilitar la protección contra malware para S3. Este límite de cuota es por cuenta en cada región. |

# GuardDuty Protección contra malware para AWS Copia de seguridad

## Temas

- [Descripción general de](#)
- [¿Cómo funciona Malware Protection for Backup?](#)
- [GuardDuty Protección contra malware para Backup: permisos de rol de IAM](#)
- [\(Opcional\) Comience a utilizar Malware Protection for Backup Independent \(solo en consola\)](#)
- [Inicio de un On-Demand análisis en busca de Malware Protection for Backup](#)
- [Supervisión de los estados de los escaneos y de los resultados en Malware Protection for Backup](#)
- [Cuotas de protección contra malware para Backup](#)

## Descripción general de

Malware Protection for Backup le ayuda a detectar la posible presencia de malware en los datos de backup escaneando los recursos AWS protegidos por Backup, como las instantáneas de Amazon EBS, las AMI de Amazon EC2 y los puntos de recuperación de Amazon S3. Cuando AWS Backup crea o actualiza un recurso de copia de seguridad protegido, GuardDuty puede realizar un análisis de malware en esa copia de seguridad para ayudar a identificar el contenido potencialmente malicioso antes de restaurarlo en su entorno.

### Cómo utilizar Malware Protection for Backup

Puede utilizar esta función de dos modos, en función de si GuardDuty está habilitada en su cuenta:

#### 1. Uso de Malware Protection for Backup con GuardDuty activado

Cuando GuardDuty está activado en una región, AWS Backup integra Malware Protection con el flujo de GuardDuty trabajo de búsqueda. Los resultados del análisis de malware aparecen en GuardDuty los resultados, además de en Amazon EventBridge y Amazon CloudWatch.

#### 2. Uso de Malware Protection for Backup sin activar GuardDuty

Puede utilizar Malware Protection for Backup de forma independiente, sin activar el GuardDuty servicio completo. En este modo, los resultados del escaneo permanecen completamente disponibles a través de EventBridge y CloudWatch.

## Consideraciones para usar Malware Protection for Backup de forma independiente

Cuando se utiliza la función sin habilitarla GuardDuty:

- La configuración del plan de backup se gestiona íntegramente en AWS Backup.

GuardDuty no proporciona controles para seleccionar los planes de respaldo, los almacenes o los tipos de recursos. Toda la activación, la programación y la configuración de políticas permanecen en Backup AWS .

- GuardDuty los resultados no se generan.

Los hallazgos requieren un identificador de detector, que se crea solo cuando GuardDuty está activado. Cuando se utiliza Malware Protection de forma independiente, los resultados del análisis se obtienen exclusivamente a través de EventBridge eventos y CloudWatch métricas.

- Aún puede iniciar escaneos bajo demanda desde la GuardDuty consola.

Incluso cuando no GuardDuty está habilitada, la GuardDuty consola proporciona un flujo de trabajo para iniciar un análisis de malware bajo demanda en busca de los tipos de recursos de respaldo compatibles. Esto permite a los clientes utilizar una GuardDuty interfaz familiar sin necesidad de un GuardDuty servicio completo.

- Non-GuardDuty los clientes pueden acceder a los flujos de trabajo de inicio del escaneo.

Los puntos de entrada al escaneo bajo demanda están disponibles para todos los clientes que utilizan Malware Protection for Backup, independientemente de si existe un GuardDuty detector en la cuenta.

- El comportamiento y la cobertura del escaneo siguen siendo idénticos.

Ya sea GuardDuty que esté habilitada o no, la función escanea los mismos tipos AWS de recursos de Backup con el mismo motor de detección de malware. La única diferencia es dónde se publican los resultados.

Este modelo permite a los clientes adoptar el escaneo de malware para realizar copias de seguridad sin necesidad GuardDuty de funciones más amplias de detección de amenazas, al tiempo que

proporciona un GuardDuty-based flujo de trabajo opcional para iniciar y ver las operaciones de escaneo.

## Cómo funciona Malware Protection for Backup

Malware Protection for Backup puede analizar los siguientes recursos AWS protegidos por backup:

- Instantáneas de Amazon EBS
- AMI de Amazon EC2
- Puntos de recuperación Amazon S3 y [copias de seguridad continuas o recuperación puntual \(PITR\) de S3](#)
- [Bóvedas bloqueadas \(inmutables\) \(puntos de EBS/EC2 recuperación\) que utilizan AWS Backup Vault Lock en las regiones compatibles](#)

## Escaneo incremental

AWS Backup captura los cambios incrementales para muchos tipos de recursos. GuardDuty tiene la capacidad de escanear solo los bloques u objetos nuevos o modificados cuando se crea o actualiza una copia de seguridad, lo que mejora el rendimiento y reduce la sobrecarga de digitalización, al tiempo que logra una cobertura total con el tiempo.

## On-demand digitalización

Puede iniciar un análisis de cualquier recurso de backup compatible en cualquier momento, directamente desde AWS Backup o desde la GuardDuty consola. Los casos de uso más comunes incluyen verificar una copia de seguridad antes de restaurarla, volver a comprobar los datos antiguos después de que se publiquen nuevas firmas de amenazas o realizar análisis periódicos de conformidad.

### Note

- Malware Protection for Backup solo se puede activar para los recursos de respaldo de la misma región.
- GuardDuty escanea una copia de solo lectura de la copia de seguridad; no modifica el contenido de la copia de seguridad.
- El escaneo funciona tanto para bóvedas estándar como para bóvedas bloqueadas (inmutables).

# ¿Cómo funciona Malware Protection for Backup?

En esta sección se describen los componentes de Malware Protection for Backup, cómo funciona y cómo puede revisar el estado y el resultado del análisis de malware.

## Descripción general de

Malware Protection for Backup es una función que le ayuda a detectar la presencia de malware en las instantáneas de EBS, las imágenes de EC2 (AMI) y los puntos de recuperación que pertenecen a los tipos de recursos de EBS, EC2 y S3. Puede iniciar un análisis de software malicioso bajo demanda mediante la GuardDuty consola o la API. Para ello, asigne una función de IAM que proporcione los permisos necesarios para el análisis, además de uno o dos ARN de recursos, según la categoría de análisis. Existen dos categorías de análisis posibles: escaneos completos y escaneos incrementales.

## Escaneo completo y escaneo incremental

En un análisis completo, la API acepta el ARN de un recurso y analiza todos los archivos de ese recurso. Por otro lado, un análisis incremental toma dos ARN de recursos, ambos pertenecientes al mismo recurso, y analiza los archivos modificados que hay entre ellos. Como ejemplo, supongamos que tomamos una instantánea de un volumen de EBS. Llamémoslo snapshot-1. Si se realiza un escaneo completo de esta instantánea, GuardDuty escanea todos los archivos que contiene esta instantánea. Supongamos ahora que se han añadido algunos archivos al mismo volumen y que se ha tomado una nueva instantánea. Vamos a llamarla snapshot-2. Como solo han cambiado unos pocos archivos entre la snapshot-1 y la snapshot-2, se puede iniciar un análisis incremental con los ARN de recursos de estas dos instantáneas. En este caso, se hace referencia a snapshot-2 como el recurso y a snapshot-1 como el recurso. *target* base Verá que esta terminología se utiliza en el resto del documento. Este escaneo incremental escaneará los archivos modificados entre la snapshot-1 y la snapshot-2.

## Escaneo de malware (PITR) Point-in-Time-Recovery

Cuando se habilita desde AWS Backup, el escaneo de malware en busca de copias de seguridad continuas (PITR) se realiza de acuerdo con la frecuencia configurada en el plan de respaldo. Esto lo organiza el servicio AWS Backup. Por ejemplo, GuardDuty ejecutará el primer escaneo de t0 a t2, el siguiente escaneo de t2 a t4, el escaneo posterior de t4 a t6 y así sucesivamente. Cada uno de estos escaneos genera un identificador de escaneo que se puede consultar mediante la GetMalwareScan API para obtener el estado y el resultado del escaneo durante ese período de tiempo.



Como alternativa, también puedes escanear todo el recurso PITR desde la GuardDuty consola o mediante la GuardDuty StartMalwareScan API bajo demanda, introduciendo una marca de tiempo de finalización. Esto garantizará que se GuardDuty escanee todo el recurso desde el principio hasta la fecha de finalización.

#### Note

- No se pueden activar escaneos parciales o incrementales en el PITR desde GuardDuty
- La fecha de finalización de un análisis bajo demanda no puede ser anterior a (hora actual: 15 minutos).

## Volver a escanear archivos previamente infectados en un análisis incremental

Como parte de un análisis incremental, también GuardDuty volverá a analizar los archivos previamente infectados desde el análisis base durante un máximo de 365 días.

### Requisitos para un escaneo incremental

Se deben cumplir los siguientes requisitos GuardDuty para realizar un escaneo incremental. Si no se cumple alguno de estos requisitos, GuardDuty omitirá el escaneo.

- El recurso base debe escanearse en los últimos 365 días y el resultado del escaneo debe estar en COMPLETED o COMPLETED\_WITH\_ISSUES.
- El recurso base debe tener una fecha de creación anterior a la del recurso de destino.
- Los recursos base y de destino deben tener el mismo tipo de cifrado en el caso de las instantáneas.
- Los recursos base y de destino deben ser del mismo linaje.
  - En el caso de una instantánea de EBS y un punto de recuperación de EBS, esto significa que proceden del mismo volumen o de copias del mismo volumen, sin ningún cambio en el tipo de cifrado.
  - En el caso de un punto de recuperación de S3, los ARN de los recursos base y de destino deben crearse a partir del mismo depósito de S3 subyacente.
  - En el caso de las AMI, se comparan pares de instantáneas entre la AMI base y la de destino para identificar las instantáneas para un escaneo incremental. Cada par de instantáneas debe cumplir las condiciones mencionadas anteriormente. Se omitirá cualquier instantánea de la AMI de destino que no tenga una instantánea coincidente correspondiente en la AMI base.

## Re-scanning recursos de respaldo escaneados anteriormente

Puede iniciar un nuevo análisis de malware bajo demanda en el mismo recurso transcurridos 10 minutos desde la hora de inicio del análisis de malware anterior. Si el nuevo análisis de malware se inicia dentro de los 10 minutos siguientes al inicio del anterior, tu solicitud generará el siguiente error y no se generará ningún identificador de análisis para esta solicitud. Los pasos para volver a analizar la instancia son los mismos que para iniciar un análisis de malware bajo demanda por primera vez.

## Se requiere el rol de IAM para el escaneo

Debe asignar una función de IAM para iniciar un escaneo completo o incremental. Esta función proporciona los permisos necesarios para realizar las operaciones de escaneo. [GuardDuty Protección contra malware para Backup: permisos de rol de IAM](#) proporciona la lista exacta de los permisos necesarios, junto con la política de confianza pertinente necesaria para realizar el análisis.

## Revisión del estado y el resultado del análisis de los recursos

GuardDuty publica el evento resultante del escaneo en el bus de eventos EventBridge predeterminado de Amazon. GuardDuty se envía al menos una vez, lo que significa que puede recibir varios resultados de escaneo para el mismo objeto. Le recomendamos que diseñe sus aplicaciones para gestionar los resultados duplicados. Solo se le facturará una vez por cada objeto analizado.

Para obtener más información, consulte [Supervisión de los estados de los escaneos y de los resultados en Malware Protection for Backup](#).

## Revisar los resultados generados

La revisión de los resultados depende de si utiliza o no Malware Protection for Backup with GuardDuty. Considere los siguientes escenarios:

Uso de Malware Protection for Backup cuando el GuardDuty servicio está activado (ID del detector)

Si el análisis de malware detecta un archivo potencialmente malicioso en un recurso de Backup escaneado, GuardDuty generará un hallazgo asociado. Puede ver los detalles del resultado y seguir los pasos recomendados para remediarlo potencialmente. Según la [frecuencia de tus hallazgos de exportación](#), el hallazgo generado se exporta a un bucket de S3 y a un bus de EventBridge eventos de Amazon.

Para obtener información sobre el tipo de hallazgo que se generaría, consulte [Tipos de búsqueda de Malware Protection for Backup](#) Búsqueda de tipos de Malware Protection for Backup.

Uso de Malware Protection for Backup como función independiente (sin ID de detector)

GuardDuty no podrá generar resultados porque no hay un ID de detector asociado. Para conocer el estado del escaneo de su recurso de respaldo, puede ver el resultado del escaneo que GuardDuty se publica automáticamente en su bus de eventos predeterminado.

Para obtener información sobre el estado y el resultado del escaneo, consulte [Supervisión de los estados de los escaneos y de los resultados en Malware Protection for Backup](#).

 Note

Si también utiliza Malware Protection para S3, existe la posibilidad de que su archivo S3 se haya etiquetado anteriormente como NO\_THREATS\_FOUND y, sin embargo, el mismo archivo aparezca en la lista de amenazas del Punto de Recuperación de Backup al que pertenece ese objeto. Esto ocurre porque el servicio actualiza con frecuencia sus firmas de malware, lo que puede haber cambiado el estado del archivo. Tenga en cuenta que, en esos casos, GuardDuty no actualiza la etiqueta del archivo en el depósito de S3 original. La única forma de aplicar una etiqueta actualizada al archivo es volver a cargar el objeto en el depósito o utilizar la función de escaneo bajo demanda de S3.

## GuardDuty Protección contra malware para Backup: permisos de rol de IAM

### Se proporcionó un rol de cliente para el análisis de malware

GuardDuty Malware Protection espera que se proporcione una función de cliente (función de escáner) cuando se inicien los escaneos en los recursos de Backup, es decir, instantáneas, AMI y puntos de EBS/EC2/S3 recuperación. Esta función proporciona los permisos necesarios GuardDuty para realizar el escaneo en esos recursos específicos. La política de permisos y la política de confianza para este rol se encuentran en [Política de permisos y confianza para el rol](#). En la siguiente sección se describe por qué se requiere cada uno de estos permisos.

## Detalles sobre los permisos

- **ModifySnapshotAttribute**- Permite acceder a las instantáneas no cifradas y cifradas con clave gestionada por el cliente mediante la cuenta del servicio de protección contra GuardDuty malware.
- **CreateGrant**- Permite a GuardDuty Malware Protection crear y acceder a un volumen de EBS cifrado con clave gestionada por el cliente a partir de la instantánea cifrada con clave gestionada por el cliente a la que tiene acceso la cuenta de GuardDuty servicio.
- **RetireGrant**- Permite que GuardDuty Malware Protection retire las concesiones que se crearon en la clave gestionada por el cliente para leer instantáneas cifradas
- **ReEncryptTo** **ReEncryptFrom** - Lo exige EBS para dar GuardDuty acceso a las instantáneas cifradas con claves administradas por el cliente y crear volúmenes cifrados a partir de ellas. Si bien los clientes pueden considerar ReEncryption la posibilidad de compartir una instantánea como una transición clave, las instantáneas permanecen inmutables desde la perspectiva del cliente una vez creadas.
- **ListSnapshotBlocks** **GetSnapshotBlock** - Las API de EBS Direct se utilizan para acceder a los bloques de instantáneas de una instantánea cifrada con clave AWS gestionada. Esto se debe a que, de lo contrario, no se puede acceder a las instantáneas cifradas con clave AWS administrada desde varias cuentas.
- **Decrypt**- Permite descifrar las instantáneas básicas cifradas con clave gestionada por el cliente cuando se descargan en la memoria mediante las API de EBS Direct como parte del escaneo incremental.
- **ListChangedBlocks**- La API EBS Direct se utiliza en el escaneo incremental de instantáneas para obtener la lista de bloques modificados entre dos instantáneas.
- **DescribeKey**- Permite que GuardDuty Malware Protection determine el ID clave de la clave AWS gestionada en la cuenta del cliente.
- **DescribeImages**- Permite describir una AMI para obtener la lista de instantáneas que pertenecen a la AMI.
- **DescribeRecoveryPoint**- Permite al servicio obtener los detalles del punto de recuperación y verificar el tipo de recurso del punto de recuperación.
- **CreateBackupAccessPoint**, **DescribeBackupAccessPoint**, **DeleteBackupAccessPoint** - Permite que el servicio cree, describa y elimine el punto de acceso necesario para acceder a los puntos de recuperación.

- `kms:Decrypt`- Permite que el servicio acceda a los objetos de un punto de recuperación S3 durante un escaneo del punto de recuperación S3.

## Asegurar el rol

El rol debe configurarse con una política de confianza que confíe en el director del servicio de protección contra GuardDuty malware. Esto garantiza que ningún otro responsable que no sea el GuardDuty servicio pueda asumir esta función. Además, le recomendamos que limite las políticas a recursos específicos en lugar de hacerlo\*. Esto incluye los identificadores de instantáneas y los identificadores clave. De este modo, se asegurará de que el rol solo proporcione acceso a esos recursos específicos.

### Important

Una configuración incorrecta podría provocar errores en el escaneo debido a la falta de permisos.

## Cómo utiliza GuardDuty Malware Protection las subvenciones en AWS KMS

GuardDuty La protección contra el malware requiere [subvenciones](#) para usar sus claves de KMS.

Al iniciar un análisis de una instantánea cifrada o de una AMI de EC2 compuesta por instantáneas cifradas, GuardDuty Malware Protection crea concesiones en su nombre mediante el envío de una [CreateGrants](#) solicitud a AWS KMS. Estas concesiones dan GuardDuty acceso a una clave específica de su cuenta.

GuardDuty La protección contra malware requiere la autorización para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe [DescribeKey](#) solicitudes AWS a para obtener detalles sobre la clave simétrica administrada por el cliente con la que se cifra el recurso enviado para el análisis de software malicioso.
- Cree un volumen de EBS a partir de una instantánea cifrada mediante la [CreateVolume](#) API y cifre el volumen con la misma clave.
- Acceda a los bloques de instantáneas de la instantánea a través de la [GetSnapshotBlock](#) API durante un escaneo incremental.

- Envíe solicitudes de [descifrado](#) a AWS KMS para descifrar las claves de datos cifrados, de modo que puedan usarse para leer los datos de la instantánea durante el escaneo.

Puede revocar la concesión creada o eliminar el acceso del servicio a la clave gestionada por el cliente en cualquier momento. Si lo haces, GuardDuty no podrás acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos.

## GuardDuty Contexto de cifrado y protección contra malware

Un [contexto de cifrado](#) es un conjunto opcional de pares clave-valor que pueden contener información contextual adicional sobre los datos.

Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS; vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, debe incluir el mismo contexto de cifrado en la solicitud.

GuardDuty La protección contra malware utiliza uno de los dos contextos de cifrado.

Contexto de cifrado 1: La clave es `aws:guardduty:id`.

```
"encryptionContext": {  
  "aws:guardduty:id": "snap-11112222333344"  
}
```

Este contexto de cifrado se utiliza con las operaciones de concesión: `CreateGrant`, `Decrypt`, `GenerateDataKeyWithoutPlaintext`, `ReEncryptTo`, `RetireGrant`, `DescribeKey`.

Se crea una concesión en el recurso actual con este contexto de cifrado y estas operaciones de concesión.

Contexto de cifrado 2: La clave es `aws:ebs:id`

```
"encryptionContext": {  
  "aws:ebs:id": "snap-11112222333344"  
}
```

Este contexto de cifrado se utiliza con las operaciones de concesión: `ReEncryptFrom`, `Decrypt`, `RetireGrant`, `DescribeKey`.

Se crean tres subvenciones con estos contextos de cifrado y operaciones de concesión. Una en la instantánea de destino con la operación de ReEncryptFrom concesión. Una segunda en la instantánea de destino con Decrypt, RetireGrant, DescribeKey las operaciones. Y una tercera en la instantánea base con las mismas operaciones de subvención que la segunda subvención.

## Política de permisos y confianza para el rol

### Política de permisos

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ebs:ListSnapshotBlocks",
      "ebs:ListChangedBlocks",
      "ebs:GetSnapshotBlock"
    ],
    "Resource": "arn:aws:ec2:*::snapshot/*"
  },
  {
    "Sid": "CreateGrantPermissions",
    "Effect": "Allow",
    "Action": "kms:CreateGrant",
    "Resource": "arn:aws:kms:*::key/*",
    "Condition": {
      "ForAnyValue:StringLike": {
        "kms:EncryptionContext:aws:guardduty:id": "snap-*",
        "kms:ViaService": [
          "guardduty.*.amazonaws.com",
          "backup.*.amazonaws.com"
        ]
      }
    },
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Decrypt",
        "CreateGrant",
        "GenerateDataKeyWithoutPlaintext",
        "ReEncryptFrom",
        "ReEncryptTo",
        "RetireGrant",
        "DescribeKey"
      ]
    }
  }
]
```

```

        ]
      },
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    },
    {
      "Sid": "CreateGrantPermissionsForReEncryptAndDirectAPIs",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "kms:EncryptionContext:aws:ebs:id": "snap-*",
          "kms:ViaService": [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        }
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "Decrypt",
          "ReEncryptTo",
          "ReEncryptFrom",
          "RetireGrant",
          "DescribeKey"
        ]
      },
      "Bool": {
        "kms:GrantIsForAWSResource": "true"
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ShareSnapshotPermission",

```



```

    "Effect": "Allow",
    "Action": [
        "ec2:ModifySnapshotAttribute"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*"
},
{
    "Sid": "ShareSnapshotKMSPermission",
    "Effect": "Allow",
    "Action": [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
        "StringLike": {
            "kms:ViaService": "ec2.*.amazonaws.com"
        }
    }
},
{
    "Sid": "DescribeKeyPermission",
    "Effect": "Allow",
    "Action": "kms:DescribeKey",
    "Resource": "arn:aws:kms:*:*:key/*"
},
{
    "Sid": "DescribeRecoveryPointPermission",
    "Effect": "Allow",
    "Action": [
        "backup:DescribeRecoveryPoint"
    ],
    "Resource": "*"
},
{
    "Sid": "CreateBackupAccessPointPermissions",
    "Effect" : "Allow",
    "Action" : [
        "backup:CreateBackupAccessPoint"
    ],
    "Resource": "arn:aws:backup:*:*:recovery-point:*"
},
{
    "Sid": "ReadAndDeleteBackupAccessPointPermissions",

```

```

        "Effect" : "Allow",
        "Action" : [
            "backup:DescribeBackupAccessPoint",
            "backup>DeleteBackupAccessPoint"
        ],
        "Resource": "*"
    },
    {
        "Sid": "KMSKeyPermissionsForInstantAccess",
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "backup.*.amazonaws.com"
            }
        }
    }
]
}

```

## Política de confianza

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

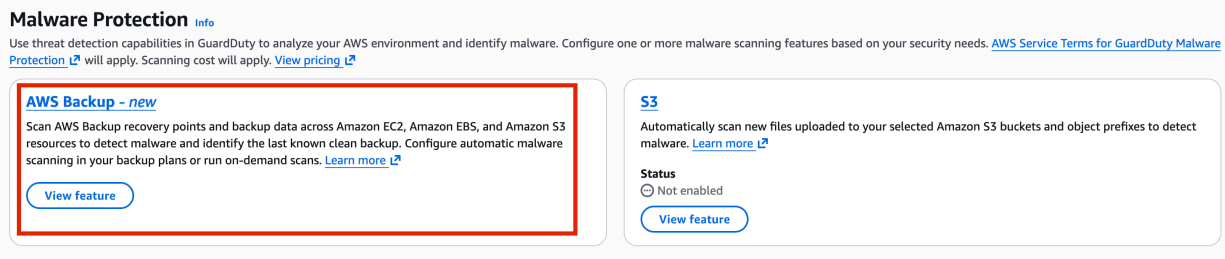
## (Opcional) Comience a utilizar Malware Protection for Backup Independent (solo en consola)

Utilice este paso opcional cuando desee empezar a utilizar la opción de detección de amenazas de Malware Protection for Backup, independientemente del GuardDuty estado de su AWS cuenta.

Si también quieres utilizar otros planes de protección dedicados GuardDuty, debes empezar con el GuardDuty servicio de Amazon. Para obtener información sobre los planes de GuardDuty protección, consulte [Características de GuardDuty](#).

### Pasos para empezar a usar Malware Protection for Backup

1. Inicie sesión en la consola AWS de administración y abra la <https://console.aws.amazon.com/guardduty/console> en <https://console.aws.amazon.com/guardduty/>
2. Seleccione Descubra las funciones de protección contra malware y haga clic en Comenzar.
3. Al hacer clic en Comenzar, puede elegir entre opciones, incluidas las funciones AWS de Backup y S3 Malware Protection.



**Malware Protection** Info

Use threat detection capabilities in GuardDuty to analyze your AWS environment and identify malware. Configure one or more malware scanning features based on your security needs. [AWS Service Terms for GuardDuty Malware Protection](#) will apply. Scanning cost will apply. [View pricing](#)

**AWS Backup - new**

Scan AWS Backup recovery points and backup data across Amazon EC2, Amazon EBS, and Amazon S3 resources to detect malware and identify the last known clean backup. Configure automatic malware scanning in your backup plans or run on-demand scans. [Learn more](#)

[View feature](#)

**S3**

Automatically scan new files uploaded to your selected Amazon S3 buckets and object prefixes to detect malware. [Learn more](#)

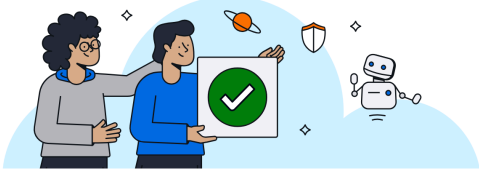
**Status**

⊖ Not enabled

[View feature](#)

4. Accederá a la página Malware Protection for Backup, donde podrá elegir entre Iniciar un análisis bajo demanda o Ver análisis de malware.

**Malware Protection for AWS Backup - new** [Info](#)  
[AWS Service Terms for GuardDuty Malware Protection](#) will apply. Malware detection from scanning cost will apply. [View pricing](#)



**Detect malware in your backup data**  
Integrate with AWS Backup to scan backups and recovery points across Amazon EC2, Amazon EBS, and Amazon S3 resources. When GuardDuty detects malware, you can restore to the last known clean backup in AWS Backup.  
To get started, enable malware scanning in your new and existing backup plans. [Learn more](#)  
[Start with AWS Backup](#)

**Explore capabilities**

**Malware scan results**  
Monitor the progress of both automatic and on-demand scans of your backups. Access detailed scan results in GuardDuty.  
[View malware scans](#)

**Investigate malware findings**  
Provides comprehensive threat information from scans of your backup resources, helping you quickly identify and respond to potential threats in your stored data.  
[View all findings](#)

**On-demand scanning mode**  
Start full or incremental scans of your backup data anytime from GuardDuty. Run scans to meet compliance requirements or verify backup contents.  
[Start on-demand scan](#)

**Cross-account monitoring with AWS Organizations**  
Strengthen your organization's security posture by monitoring malware threats across throughout your backup environment. [Learn more](#)

## Inicio de un On-Demand análisis en busca de Malware Protection for Backup

### Consola

1. Inicie sesión en la consola AWS de administración y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Vaya a Malware Protection for Backup y haga clic en Iniciar análisis bajo demanda.
3. Elija entre el análisis completo y el análisis incremental.
  1. Para iniciar un análisis completo, introduzca el ARN del recurso que se va a escanear.
  2. Para un análisis incremental, introduzca el ARN del recurso de destino y el ARN del recurso de referencia.
  3. Si el recurso que se está escaneando es un punto de recuperación, también debe introducir el nombre del AWS Backup Vault al que pertenece.
  4. En el caso de un recurso PITR de S3, introduzca una marca de tiempo de finalización. La marca de tiempo de finalización no puede ser anterior a (hora actual: 15 minutos).

4. Acceso al servicio: debe elegir un rol que tenga los permisos necesarios para acceder al recurso y realizar el escaneo. Haga clic en Ver política para ver los permisos exactos necesarios para el rol, junto con la política de confianza requerida.

Puedes realizar cambios en la política en función de tus requisitos o limitar los permisos para el recurso exacto. Para obtener más información sobre cómo crear o actualizar un rol de IAM, consulte [GuardDuty Protección contra malware para Backup: permisos de rol de IAM](#).

Si tiene problemas con los permisos de los roles de IAM, consulte [Solución de problemas con los permisos de los roles de IAM](#).

## API/CLI

Invoca [StartMalwareScan](#) el resourceArn recurso para el que quieres iniciar un análisis de malware bajo demanda. Si quieres iniciar un análisis incremental, pásalo. baselineResourceArn incrementalScanDetails Como parte de la configuración del escaneo, también debe proporcionar una función de IAM que tenga todos los permisos necesarios para iniciar el escaneo. Si el recurso que se está escaneando es un recurso Pitr de S3, debe incluir una marca de tiempo de finalización. Tras iniciar correctamente un análisis, StartMalwareScan devuelve un scanId. Invoque la GetMalwareScan API para supervisar el progreso del análisis iniciado y obtener los detalles del análisis una vez finalizado.

## Supervisión de los estados de los escaneos y de los resultados en Malware Protection for Backup

Tras iniciar un análisis de malware, GuardDuty proporciona algunos mecanismos mediante los que puede supervisar el estado y el resultado del análisis. En la siguiente tabla se muestran algunos de los valores asociados a los escaneos de malware.

Valores potenciales de

RUNNING COMPLETED COMPLETED\_WITH\_ISSUES , FAILED o SKIPPED

## Valores potenciales de

FULL\_SCAN o INCREMENTAL\_SCAN

GUARDDUTY\_INITIATED , ON\_DEMAND o BACKUP\_INITIATED

NO\_THREATS\_FOUND o THREATS\_FOUND

\*Tenga en cuenta que es posible que el estado del resultado del escaneo no esté presente si el escaneo no se completó. El estado del resultado del análisis de THREATS\_FOUND indica que se ha GuardDuty detectado la presencia de malware.

En el caso de los puntos de recuperación de S3, COMPLETED\_WITH\_ISSUES indica que algunos archivos se omitieron o fallaron. En el caso de las AMI, COMPLETED\_WITH\_ISSUES indica que no se ha podido escanear al menos una instantánea. Consulte a continuación la lista de motivos omitidos.

Los escaneos también se pueden omitir por varios motivos. En la siguiente tabla se explican los motivos por los que se pueden omitir los escaneos:

## Motivo

El rol del cliente no tiene los permisos necesarios para que el servicio realice el escaneo

## Motivo

El recurso que se intenta escanear no existe en la cuenta o se eliminó durante el escaneo

El tamaño de la instantánea es superior al que admite actualmente GuardDuty

Los recursos especificados en la solicitud de escaneo incremental no tienen ninguna diferencia

El recurso no está en el estado esperado. Si el escaneo es incremental, el punto de recuperación base no está en el estado DISPONIBLE o COMPLETADO

En el caso de los escaneos incrementales, el recurso base y el actual no son del mismo linaje

En el caso de los escaneos incrementales, el recurso base no se escaneó previamente o no se encontró ningún escaneo completo

En el caso de los escaneos incrementales, la fecha de creación del recurso base es superior a la fecha de creación del recurso actual

El tipo de recurso solicitado no admite el análisis incremental

## Motivo

Las AMI públicas, las AMI con solo almacenamiento efímero y las AMI que no estén en un estado disponible no son aptas para el escaneo

Las instantáneas almacenadas en frío no son aptas para el escaneo

El escaneo no es compatible con los tipos de recursos compuestos

El recurso solicitado contiene un código de producto de Amazon Marketplace que no admite el escaneo

Las AMI no admiten el escaneo de más de 40 instantáneas

No se encontraron mapeos de dispositivos de bloques de Ebs para el recurso solicitado

Para los escaneos incrementales, el arn del recurso base es diferente del arn del recurso esperado



## Motivo

Todos los archivos del escaneo se omitieron o fallaron

Los resultados del escaneo tienen un período de retención de 90 días. Elija el método de acceso que prefiera para realizar un seguimiento del estado de su análisis de malware.

Supervisión de los escaneos mediante la consola

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Análisis de malware.
3. Puede filtrar los análisis de malware según las siguientes Propiedades disponibles en la barra de criterios de filtro.
  - ID de escaneo: identificador único asociado al escaneo de malware.
  - ID de cuenta: cuenta en la que se inició el análisis de malware.
  - ARN de recurso: nombre de recurso de Amazon (ARN) asociado al recurso de Amazon asociado al escaneo.
  - Tipo de recurso: el tipo de recurso asociado al escaneo, como la instancia EC2, la instantánea de EBS | AMI de EC2, el punto de recuperación de EBS, el punto de recuperación de EC2 o el punto de recuperación de S3.
  - Estado: el estado del escaneo, como en ejecución, omitido, completado, completado con problemas o fallido.
  - Tipo de análisis: indica si se trata de un análisis On-demand GuardDuty-initiated, o de un análisis de Backup-Initiated malware.

Supervisar los escaneos mediante el API/CLI

- Puede invocarlo `ListMalwareScans` para filtrar los escaneos de malware por `RESOURCE_ARNSCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUSRESOURCE_TYPE`, y `SCAN_START_TIME`. También puede invocarlo `GetMalwareScan` para recuperar metadatos más detallados de un escaneo proporcionando un identificador de escaneo como entrada. Los criterios `GUARDDUTY_FINDING_ID` de filtrado están disponibles cuando se inicia el `SCAN_TYPE`. GuardDuty
- Puede cambiar *filter-criteria* el ejemplo del comando siguiente y filtrar de uno `CriterionKey` en uno. Las opciones para `CriterionKey` son `Resource_ARNSCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE`, `GUARDDUTY_FINDING_ID`, `SCAN_STATUS`, `RESOURCE_TYPE`, y `SCAN_START_TIME`. Puede cambiar el *max-results* (hasta 50) y el *sort-criteria*. El `AttributeName` campo es obligatorio `sort-criteria` y debe estar configurado `scanStartTime`. En el ejemplo siguiente, los valores de *red* son marcadores de posición. Sustitúyalos por los valores adecuados para la cuenta. Si usa los `CriterionKey` mismos que se muestran a continuación `ListMalwareScans`, asegúrese de reemplazar el ejemplo `EqualsValue` por el *resource-type* que desee filtrar.

```
aws guardduty list-malware-scans --max-results 25 --sort-criteria
'{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
'{"FilterCriterion":[{"CriterionKey":"RESOURCE_TYPE", "FilterCondition":
{"EqualsValue":"EBS_SNAPSHOT"}}] }
```

```
aws guardduty get-malware-scan --scan-id abc123
```

- La respuesta al comando anterior `ListMalwareScans` devolverá hasta 25 escaneos con algunos detalles sobre los recursos afectados. La respuesta al comando anterior `GetMalwareScan` devolverá un solo escaneo con metadatos detallados sobre el escaneo.

## Supervisar escaneos mediante EventBridge

Amazon EventBridge es un servicio de bus de eventos sin servidor que facilita la conexión de sus aplicaciones con datos de diversas fuentes. EventBridge ofrece un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones Software-as-a-Service (SaaS) y servicios de Amazon, y dirige esos datos a destinos como Lambda. Esto le permite monitorear los eventos que ocurren en los servicios y crear arquitecturas basadas en eventos. Para obtener más información, consulta la [Guía del EventBridge usuario de Amazon](#).

GuardDuty publica EventBridge las notificaciones en el bus de eventos predeterminado una vez que se determina el estado del escaneo. Puedes configurar EventBridge reglas en tu cuenta para enviar eventos a otros servicios integrados con Amazon EventBridge. Se aplicará el EventBridge precio estándar. Para obtener más información, consulta los [EventBridge precios de Amazon](#).

Muchos de los valores que se muestran a continuación son marcadores de posición para el ejemplo y variarán en función del escaneo.

### Eventos de resultados del análisis de malware

Posibles valores de tipo de detalle para Backup:

- «Resultado del escaneo instantáneo de EBS con protección contra GuardDuty malware»
- «Resultado del escaneo de la AMI EC2 de GuardDuty Malware Protection»
- «Resultado del escaneo del punto de recuperación S3 de GuardDuty Malware Protection»
- «Resultado del escaneo del punto de recuperación de EBS con protección contra GuardDuty malware»
- «Resultado del escaneo del punto de recuperación EC2 de GuardDuty Malware Protection»

Ejemplo de patrón de eventos:

```
{
  "detail-type": ["GuardDuty Malware Protection EC2 AMI Scan Result"],
  "source": ["aws.guardduty"]
}
```

Ejemplo de esquema de notificación para el escaneo de AMI de EC2 sin encontrar amenazas:

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
  "source": "aws.guardduty",
  "account": "1111222233334444",
  "time": "2025-11-01T00:00:00Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/ami-1234567890abcdef0"],
  "detail": {
```

```

    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "EC2_AMI",
    "scanId": "d41d8cd98f00b204e9800998ecf8427e",
    "scanStatusReason": null,
    "scanType": "ON_DEMAND",
    "triggerType": "GUARDDUTY",
    "scanCategory": "FULL_SCAN",
    "scanStartTime": 1234567890123,
    "scanCompleteTime": 2345678901234,
    "scanResultDetails": {
      "scanResultStatus": "NO_THREATS_FOUND",
      "uniqueThreatCount": null
    }
  }
}

```

Ejemplo de esquema de notificación para el escaneo de AMI de EC2 con amenazas encontradas:

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
  "source": "aws.guardduty",
  "account": "1111222233334444",
  "time": "2025-11-01T00:00:00Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/ami-1234567890abcdef0"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "COMPLETED",
    "resourceType": "EC2_AMI",
    "scanId": "d41d8cd98f00b204e9800998ecf8427e",
    "scanStatusReason": null,
    "scanType": "ON_DEMAND",
    "triggerType": "GUARDDUTY",
    "scanCategory": "FULL_SCAN",
    "scanStartTime": 1234567890123,
    "scanCompleteTime": 2345678901234,
    "scanResultDetails": {
      "scanResultStatus": "THREATS_FOUND",
      "uniqueThreatCount": 1,

```

```

    "threats": {
      "name": "EICAR-Test-File (not a virus)",
      "source": "AMAZON",
      "count": 2,
      "itemDetails": [{
        "resourceArn": "arn:aws:ec2:us-east-1:1111222233334444:snapshot/
snap-abcdef01234567890",
        "hash":
        "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
        "itemPath": "/eicar.txt",
        "additionalInfo": {
          "versionId": null,
          "deviceName": "/dev/sdf"
        }
      }]
    }
  }
}

```

Ejemplo de esquema de notificación para el escaneo de AMI de EC2 omitido:

```

{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "detail-type": "GuardDuty Malware Protection EC2 AMI Scan Result",
  "source": "aws.guardduty",
  "account": "1111222233334444",
  "time": "2025-11-01T00:00:00Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:1111222233334444:image/
ami-1234567890abcdef0"],
  "detail": {
    "schemaVersion": "1.0",
    "scanStatus": "SKIPPED",
    "resourceType": "EC2_AMI",
    "scanId": "d41d8cd98f00b204e9800998ecf8427e",
    "scanStatusReason": "UNSUPPORTED_AMI",
    "scanType": "ON_DEMAND",
    "triggerType": "GUARDDUTY",
    "scanCategory": "FULL_SCAN",
    "scanStartTime": 1234567890123,
    "scanCompleteTime": 2345678901234,

```

```

    "scanResultDetails": {
      "uniqueThreatCount": null,
      "threats": null
    }
  }
}

```

## Cuotas de protección contra malware para Backup

### Protección contra malware para cuotas de Backup

| Nombre de la cuota                                                   | AWS valor de cuota predeterminado                                                                                                                                                                                                             | ¿Se puede ajustar? | Description (Descripción) |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------|
| StartMalwareScan límite de TPS para todos los tipos de recursos      | 10                                                                                                                                                                                                                                            | No                 |                           |
| Tamaño máximo de instantánea admitido                                | 2 TB                                                                                                                                                                                                                                          | No                 |                           |
| Sistemas de archivos compatibles para escaneos de instantáneas y AMI | <ul style="list-style-type: none"> <li>• Sistema de archivos de nueva tecnología (NTFS)</li> <li>• Sistema de archivos X (XFS)</li> <li>• Sistema de archivos de segunda extensión (ext2)</li> <li>• Sistema de archivos de cuarta</li> </ul> | No                 |                           |

| Nombre de la cuota                                                              | AWS valor de cuota predeterminado                                                                                                                                                                                             | ¿Se puede ajustar? | Description (Descripción) |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------|
|                                                                                 | <p>extensión (ext4)</p> <ul style="list-style-type: none"> <li>• Sistema de archivos con tabla de asignación de archivos (FAT)</li> <li>• Sistema de archivos con tabla de asignación de archivos virtuales (VFAT)</li> </ul> |                    |                           |
| Número máximo de instantáneas en una AMI compatibles con el análisis de malware | 40 para un análisis completo. Si hay más de 40, solo GuardDuty escaneará 40 de todas las instantáneas. En el caso de un escaneo incremental, se omite el escaneo.                                                             | No                 |                           |

| Nombre de la cuota                                               | AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|-----------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tamaño máximo de un objeto dentro de un punto de recuperación S3 | 100 GB                            | No                 | <p>El tamaño máximo de un objeto S3 que GuardDuty se intentará escanear en busca de malware.</p> <p>Aunque esta cuota no se puede ajustar, si necesita escanear objetos más grandes, póngase en contacto con Support para determinar si GuardDuty puede aumentar la cuota para su caso de uso.</p> |
| Bytes de archivo extraídos                                       | 100 GB                            | No                 | <p>La cantidad máxima de datos que GuardDuty se pueden extraer y analizar de un archivo comprimido.</p> <p>GuardDuty omitirá los archivos archivados que se extraigan a más de 100 GB.</p>                                                                                                         |



| Nombre de la cuota                        | AWS valor de cuota predeterminado | ¿Se puede ajustar? | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|-----------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archivos extraídos                        | 10 000                            | No                 | <p>El número máximo de archivos que GuardDuty se pueden extraer y analizar en un archivo comprimido. Si el archivo contiene más de 10 000 archivos, GuardDuty tendrá que omitir el archivo archivado.</p> <div>  <b>Note</b><br/>           Estos límites pueden aplicarse a los tipos de archivos compuestos. Los tipos de archivo incluyen, entre otros, mensajes de correo electrónico codificados con extensiones multipropósito de correo de Internet (MIME), archivos Python compilados (PYC), archivos de ayuda HTML compilados (CHM), todos los instaladores y documentos de OpenDocument formato (ODF).         </div> |
| Niveles máximos de profundidad de archivo | 5                                 | No                 | <p>Los niveles máximos de archivos anidados que se pueden extraer. GuardDuty Si el archivo incluye archivos anidados por encima de este valor, GuardDuty omitirá esos archivos anidados.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

# GuardDuty Protección RDS

## Note

Puede configurar RDS Protection junto con todos los demás planes de protección desde una sola página de la consola. GuardDuty Para obtener más información, consulte [Configuración de planes de protección](#).

RDS Protection de Amazon GuardDuty analiza y perfila la actividad de inicio de sesión en RDS para detectar posibles amenazas de acceso a sus [bases de datos de Amazon Aurora](#) (Amazon Aurora MySQL-Compatible Edition y Aurora PostgreSQL-Compatible Edition) y [Amazon RDS for PostgreSQL](#).

RDS Protection le ayuda a identificar comportamientos de inicio de sesión potencialmente sospechosos en estas bases de datos compatibles. GuardDuty monitorea y elabora perfiles de forma continua [Actividad de inicio de sesión de RDS](#) para detectar actividades anómalas. Por ejemplo, un actor externo previamente inadvertido accede sin autorización a la base de datos, o un adversario intenta acceder por fuerza bruta al intentar adivinar la contraseña de la base de datos.

Con el lanzamiento de [Amazon Aurora PostgreSQL Limitless](#) Database GuardDuty, RDS Protection ahora también admite la supervisión de la actividad de inicio de sesión desde bases de datos ilimitadas. En el caso de Cuentas de AWS que ya tengan habilitada la protección RDS, GuardDuty empezarán automáticamente a monitorizar los datos de inicio de sesión de sus bases de datos Limitless. En el caso de las cuentas que aún no tienen habilitada la protección RDS, puede obtener más información sobre esta característica [30-day free trial](#) y optar por habilitarla. Para habilitar esta característica, consulte [Habilitar RDS Protection en entornos de varias cuentas](#) o [Habilitar RDS Protection para una cuenta independiente](#).

## Nota

Las instancias de réplica de lectura de RDS para PostgreSQL requieren que la instancia de base de datos principal esté en una versión de base de datos compatible y que se replique de manera correcta desde la base de datos principal. Para obtener más información sobre las réplicas de lectura de PostgreSQL, consulte [Trabajo con réplicas de lectura de instancias de base de datos](#) en la Guía del usuario de Amazon RDS.

La protección de RDS no requiere infraestructura adicional; está diseñada para no afectar al rendimiento de las instancias de bases de datos. Cuando RDS Protection detecta un intento de inicio de sesión potencialmente sospechoso o anómalo, GuardDuty genera uno o varios [Tipos de resultados de la protección de RDS](#) con detalles sobre la base de datos potencialmente comprometida.

### Prueba gratuita de 30 días

- Al activarlo GuardDuty Cuenta de AWS en una nueva región por primera vez, dispondrá de una prueba gratuita de 30 días. En este caso, también GuardDuty habilitará la protección RDS, que está incluida en la prueba gratuita. La protección de RDS empezará a supervisar el comportamiento de inicio de sesión de su base de datos.
- Si ya está utilizando RDS Protection GuardDuty y decide activar RDS Protection en una nueva región por primera vez, su cuenta de esa región dispondrá de una prueba gratuita de 30 días de RDS Protection.
- Si ya ha activado la protección RDS, con el lanzamiento de [Amazon Aurora PostgreSQL Limitless Database GuardDuty](#), [empezará automáticamente a supervisar la actividad de inicio de sesión de las bases de datos ilimitadas](#). Si su período de prueba gratuito de 30 días de protección de RDS ya ha caducado, empezará a incurrir en gastos de uso relacionados con la supervisión de bases de datos ilimitadas.
- Puede optar por desactivar RDS Protection en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, RDS Protection no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#).

Cuando la función de protección RDS no está habilitada, GuardDuty no detecta un comportamiento de inicio de sesión anómalo o sospechoso. Si deshabilita la protección con RDS, deja de supervisar GuardDuty inmediatamente la actividad de inicio de sesión en RDS y no detectará ninguna amenaza potencial para las instancias de bases de datos compatibles ni generará ningún tipo de búsqueda asociado.

Para saber Regiones de AWS dónde se admiten las bases de datos Aurora PostgreSQL Limitless, consulte Requisitos de la base de datos [Aurora](#) PostgreSQL Limitless.

## Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles

En la siguiente tabla aparecen las versiones de bases de datos de Aurora y Amazon RDS compatibles con RDS Protection.

| Motor de base de datos de Amazon Aurora y Amazon RDS | Versiones del motor admitidas                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aurora MySQL                                         | <ul style="list-style-type: none"> <li>• 2.10.2 o posteriores</li> <li>• 3.02.1 o posteriores</li> </ul>                                                                                                                                                                                                                                                                                                   |
| Aurora PostgreSQL                                    | <ul style="list-style-type: none"> <li>• 10.23 o posterior</li> <li>• 11.12 o posteriores</li> <li>• 12.7 o posteriores</li> <li>• 13.3 o posteriores</li> <li>• 14.3 o posteriores</li> <li>• 15.2 o posterior</li> <li>• 16.1 o posterior</li> </ul>                                                                                                                                                     |
| RDS para PostgreSQL                                  | <ul style="list-style-type: none"> <li>• 11.17 o posteriores</li> <li>• 12.12 o posteriores</li> <li>• 13.8 o posteriores</li> <li>• 14.5 o posteriores</li> <li>• <a href="#">RDS para PostgreSQL versión 15</a></li> <li>• <a href="#">RDS para PostgreSQL versión 16</a></li> <li>• <a href="#">RDS para PostgreSQL versión 17</a></li> <li>• <a href="#">RDS para PostgreSQL versión 18</a></li> </ul> |
| Base de datos ilimitada de Amazon Aurora PostgreSQL  | 16.4-limitless                                                                                                                                                                                                                                                                                                                                                                                             |

## Actividad de inicio de sesión de RDS

Cuando habilita la función de protección de RDS, comienza a monitorear GuardDuty automáticamente la actividad de inicio de sesión de RDS para sus bases de datos, directamente desde los servicios Aurora y Amazon RDS. La actividad de inicio de sesión de RDS captura los intentos de inicio de sesión correctos y fallidos realizados en su entorno. [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) AWS Si hay indicios de un comportamiento de inicio de sesión anómalo, GuardDuty genera un resultado con detalles sobre la base de datos potencialmente comprometida. Al habilitar RDS Protection por primera vez o al contar con una instancia de base de datos recién creada, habrá un período de aprendizaje para determinar la referencia de lo que constituye un comportamiento normal. Por esta razón, las instancias de base de datos recién habilitadas o creadas recientemente podrían no generar un resultado de inicio de sesión anómalo asociado hasta después de un período de dos semanas.

Cuando RDS Protection detecta una amenaza potencial, como un patrón inusual en una serie de intentos de inicio de sesión correctos, fallidos o incompletos, GuardDuty genera una o varias. [Tipos de resultados de la protección de RDS](#) Según el tipo de resultado, es posible que se incluyan detalles específicos sobre el comportamiento anómalo, como [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

GuardDuty no gestiona su actividad de inicio de sesión [Bases de datos compatibles](#) ni la de RDS, ni pone a su disposición la actividad de inicio de sesión de RDS.

## Habilitar RDS Protection en entornos de varias cuentas

En un entorno de varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de activar o desactivar la función de protección de RDS para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra sus cuentas de miembros mediante AWS Organizations. Esta cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente la supervisión de la actividad de inicio de sesión de RDS para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre entornos de varias cuentas, consulte [Varias cuentas en GuardDuty](#).

### Habilitar la protección de RDS para la cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para configurar la supervisión de la actividad de inicio de sesión de RDS para la cuenta de administrador delegado GuardDuty .

## Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones.
4. Realice una de las siguientes acciones:

### Utilización Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
- Seleccione Save.

### Utilización Configure las cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar cuentas manualmente.
- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Save.

## API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como RDS\_LOGIN\_EVENTS y status como ENABLED.

Como alternativa, puede utilizarla AWS CLI para habilitar la protección RDS. Ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID del detector de su cuenta y `us-east-1` por la región en la que desee activar la protección RDS.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

## Auto-enable Protección RDS para todas las cuentas de los miembros

Elija su método de acceso preferido para habilitar la característica de protección de RDS en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

### Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

#### Uso de Planes de protección page

1. En el panel de navegación, elija Planes de protección.
2. Elija Configurar todas las habilitaciones.
3. En Protección RDS, seleccione Activar para todas las cuentas. Esta acción habilita automáticamente RDS Protection para las cuentas nuevas y existentes de la organización.
4. Selecciona Guardar todo y, a continuación, selecciona Confirmar y guardar.

#### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

#### Uso de Cuentas page

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de habilitación automática, elija Habilitar para todas las cuentas en Supervisión de la actividad de inicio de sesión de RDS.
4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitar RDS Protection para las cuentas de miembro de forma selectiva](#).

## API/CLI

Para activar o desactivar la protección RDS de forma selectiva para sus cuentas de miembros, invoque la operación de la [updateMemberDetectors](#) API con la suya propia. *detector ID*

Como alternativa, puede utilizarla AWS CLI para activar la protección RDS. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la protección RDS.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"name":
"RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitación de RDS Protection para todas las cuentas de miembros activos existentes

Elija su método de acceso preferido para habilitar RDS Protection en todas las cuentas de miembros activos existentes en la organización. Las cuentas de miembros que ya están GuardDuty habilitadas se denominan miembros activos existentes.

### Console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.



2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. En Protección RDS, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Elija Confirmar.

## API/CLI

Ejecute la operación [updateMemberDetectors](#) de la API con la suya propia. *detector ID*

Como alternativa, puede utilizarla AWS CLI para habilitar la protección RDS. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la protección RDS.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"name":
"RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Auto-enable Protección RDS para cuentas de nuevos miembros

Elija su método de acceso preferido para habilitar la actividad de inicio de sesión de RDS para las cuentas nuevas que se unan a la organización.

### Console

La cuenta de GuardDuty administrador delegado puede habilitar nuevas cuentas de miembros en una organización a través de la consola, desde la página de protección de RDS o desde la página de cuentas.

## Habilitación automática de la Protección de RDS para las cuentas de miembros nuevos

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:
  - Mediante la página de planes de protección:
    1. En el panel de navegación, elija Planes de protección.
    2. Elija Configurar todas las habilitaciones.
    3. Elija Configurar cuentas manualmente.
    4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que, cada vez que una nueva cuenta se una a su organización, RDS Protection se habilite automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.
  - 5. Seleccione Save.
  - Mediante la página Cuentas:
    1. En el panel de navegación, elija Cuentas.
    2. En la página Cuentas, seleccione Auto-enable las preferencias.
    3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las cuentas nuevas en Supervisión de la actividad de inicio de sesión de RDS.
    4. Seleccione Save.

## API/CLI

Para activar o desactivar la protección RDS de forma selectiva para sus cuentas de miembros, invoque la operación de la [UpdateOrganizationConfiguration](#) API con la suya propia. *detector ID*

Como alternativa, puede utilizarla AWS CLI para activar la protección RDS. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la protección RDS. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `autoEnable` en `NONE`.

Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectorsAPI](#).

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features '[{"Name": "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitar RDS Protection para las cuentas de miembro de forma selectiva

Elija el método de acceso que prefiera para habilitar de forma selectiva la supervisión de la actividad de inicio de sesión en RDS para las cuentas de miembro.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.

En la página Cuentas, revise la columna Actividad de inicio de sesión de RDS para ver el estado de su cuenta de miembro.

3. Activación o desactivación de forma selectiva de la actividad de inicio de sesión en RDS

Seleccione la cuenta para la que desee configurar RDS Protection. Puede seleccionar varias cuentas de manera simultánea. En el menú desplegable Editar planes de protección, seleccione Actividad de inicio de sesión de RDS y, a continuación, elija la opción adecuada.

### API/CLI

Para activar o desactivar la protección RDS de forma selectiva para sus cuentas de miembros, invoque la operación de la [updateMemberDetectorsAPI](#) con la suya propia. *detector ID*

Como alternativa, puede utilizarla AWS CLI para activar la protección RDS. Ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID del detector de su cuenta y `us-east-1` por la región en la que desee activar la protección RDS.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectorsAPI](#).

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"RDS_LOGIN_EVENTS", "Status": "ENABLED"}]'
```

#### Note

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitar RDS Protection para una cuenta independiente

Una cuenta independiente es la que decide activar o desactivar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar RDS Protection en entornos de varias cuentas](#).

Tras activar RDS Protection, GuardDuty empezará a supervisar las [Actividad de inicio de sesión de RDS](#) bases de datos compatibles de su cuenta.

Elija el método de acceso que prefiera para configurar RDS Protection para una cuenta independiente.

### Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>

2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. En Protección RDS, elija Activar para activar la protección RDS.
4. Selecciona Guardar todo y, a continuación, selecciona Confirmar y guardar.

## API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como RDS\_LOGIN\_EVENTS y status como ENABLED.

Como alternativa, puede utilizarla AWS CLI para activar la protección RDS. Ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID del detector de su cuenta y `us-east-1` por la región en la que desee activar la protección RDS.

Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#)API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

## Solución de problemas de monitoreo de protección de RDS

GuardDuty RDS Protection analiza y perfila su actividad de inicio de sesión en RDS para detectar posibles amenazas de acceso al. [Bases de datos compatibles](#) Para recopilar la telemetría de seguridad de forma eficaz, es GuardDuty necesario que su base de datos esté configurada y funcione sin problemas. Si su base de datos está mal configurada o tiene problemas, es posible que el monitoreo de la seguridad se vea afectado.

En la siguiente sección se describen los problemas más comunes y los pasos para solucionarlos.

### Almacenamiento de RDS completo

Cuando su instancia de RDS se quede sin espacio de almacenamiento, es GuardDuty posible que no recopile la telemetría de seguridad. Alcanzar la asignación de capacidad de almacenamiento de instancias de base de datos (`storage-full`) es un estado crítico y RDS recomienda solucionar

este problema de inmediato. Para obtener más información, consulte [ver estado de las instancias](#) en la Guía del usuario de Amazon RDS.

Para resolver el estado `storage-full`, puede realizar una de las siguientes acciones:

- Habilitar el escalado automático del almacenamiento (recomendado): active el escalado automático del almacenamiento de Amazon RDS para administrar automáticamente la capacidad de almacenamiento y evitar futuras condiciones de `storage-full`. Para obtener más información, consulte [Administrar la capacidad de manera automática con el escalado automático de almacenamiento de Amazon RDS](#) en la Guía del usuario de Amazon RDS.
- Monitoree el uso del almacenamiento: verifique el uso del almacenamiento mediante uno de los siguientes métodos:
  - Utilice CloudWatch las métricas para ver los detalles del almacenamiento. Para obtener más información, consulta [CloudWatch Database Insights](#) en la Guía del CloudWatch usuario de Amazon.
  - Para ver las métricas de almacenamiento, siga los pasos que se indican en [Monitorear las métricas de una instancia de Amazon RDS](#) en la Guía del usuario de Amazon RDS.
- Modifique la capacidad de almacenamiento: para obtener información sobre cómo aumentar la capacidad de almacenamiento de la instancia, consulte [Aumentar la capacidad de almacenamiento de la instancia de base de datos](#) en la Guía del usuario de Amazon RDS.

## Versiones no compatibles en la base de datos principal de RDS para PostgreSQL

Las instancias de réplica de lectura de RDS para PostgreSQL requieren que la instancia de base de datos principal esté en una versión de base de datos compatible y que se replique correctamente desde la base de datos principal. GuardDuty monitorea las instancias solo cuando se cumplen estos requisitos.

Para resolver el problema con la versión no compatible, siga una de estas opciones:

- Verifique la compatibilidad de la versión de la base de datos: verifique que la base de datos principal de RDS para PostgreSQL ejecute una de las versiones compatibles. Para obtener más información, consulte [Bases de datos compatibles](#).
- Solucione un posible problema de replicación: revise y resuelva cualquier problema de replicación entre las instancias principales y de réplica. Para obtener más información sobre cómo realizarlo,

consulte [Trabajar con réplicas de lectura para RDS para PostgreSQL](#) en la Guía del usuario de Amazon RDS.

## Consideraciones adicionales de seguridad

Si su organización tiene requisitos de cumplimiento estrictos, le recomendamos implementar una auditoría de bases de datos además de utilizar RDS Protection. Para obtener más información sobre sus responsabilidades de seguridad y su modelo de responsabilidad compartida, consulte [Seguridad en Amazon RDS](#) en la Guía del usuario de Amazon RDS.

# GuardDuty Protección Lambda

## Note

Puede configurar Lambda Protection junto con todos los demás planes de protección desde una sola página de la GuardDuty consola. Para obtener más información, consulte [Configuración de planes de protección](#).

La protección de Lambda lo ayuda a identificar posibles amenazas de seguridad cuando se invoca una función de [AWS Lambda](#) en su entorno de AWS . Al habilitar Lambda Protection, GuardDuty comienza a monitorear los registros de actividad de la red Lambda. Esto incluye [Logs de flujo de VPC](#) de todas las funciones de Lambda para la cuenta (incluidos los registros que no utilizan redes VPC) y los registros que se generan cuando se invoca la función de Lambda. Cuando GuardDuty identifica tráfico de red sospechoso que es indicativo de la presencia de un fragmento de código potencialmente malicioso en su función Lambda, GuardDuty genera uno o más. [Tipos de resultados de la protección de Lambda](#)

## Prueba gratuita de 30 días

En la siguiente lista se explica cómo funciona la prueba gratuita de 30 días para la cuenta:

- Al activarla GuardDuty Cuenta de AWS en una nueva región por primera vez, dispondrá de una prueba gratuita de 30 días. En este caso, también GuardDuty habilitará Lambda Protection, que se incluye en la versión de prueba gratuita.
- Cuando ya utilice Lambda Protection GuardDuty y decida habilitarlo por primera vez, su cuenta de esta región dispondrá de una prueba gratuita de 30 días de Lambda Protection.
- Puede optar por desactivar la protección de Lambda en cualquier región y en cualquier momento.
- Durante los 30 días de la prueba gratuita, puede obtener una estimación de los costos de su uso en esa cuenta y región. Una vez finalizada la prueba gratuita de 30 días, la protección de Lambda no se desactivará automáticamente. La cuenta en esta región comenzará a incurrir en costos de uso. Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#).

Los registros de actividad de red de Lambda están sujetos a cambios, incluida la ampliación a otra actividad de red, como los datos de consulta de DNS generados al invocar las funciones de Lambda.



La expansión a otras formas de supervisión de la actividad de la red aumentará el volumen de datos que GuardDuty se procesarán para Lambda Protection. Esto afectará directamente al costo de uso de la protección de Lambda. Cada vez que GuardDuty comience a monitorear un registro de actividad de red adicional, enviará un aviso a las cuentas que hayan activado Lambda Protection, al menos 30 días antes del lanzamiento.

 Note

La supervisión de la actividad de red de Lambda no incluye los registros de las [funciones de Lambda@Edge](#).

## Supervisión de la actividad de red de Lambda

Al habilitar Lambda Protection, supervisa los registros de actividad de red de GuardDuty Lambda que se generan cuando se invoca una función de Lambda asociada a su cuenta. Esto lo ayuda a detectar posibles amenazas de seguridad de la función de Lambda. En el caso de las funciones de Lambda que están configuradas para usar redes de VPC, no es necesario habilitar los registros de flujo de VPC para las interfaces de red elásticas (ENI) creadas por Lambda. GuardDuty solo cobra por la cantidad de datos de registro de actividad de red Lambda procesados (en GB) para generar un hallazgo. GuardDuty optimiza los costes mediante la aplicación de filtros inteligentes y el análisis de un subconjunto de registros de actividad de la red Lambda que son relevantes para la detección de amenazas.

GuardDuty no administra los registros de actividad de la red Lambda (incluidos los registros de flujo de VPC y no VPC) ni los hace accesibles en su cuenta.

## Habilitar la protección de Lambda en entornos de varias cuentas

En un entorno de varias cuentas, solo la cuenta de GuardDuty administrador delegado tiene la opción de activar o desactivar Lambda Protection para las cuentas de los miembros de su organización. Las cuentas de GuardDuty los miembros no pueden modificar esta configuración desde sus cuentas. La cuenta de GuardDuty administrador delegado administra las cuentas de los miembros mediante AWS Organizations. La cuenta de GuardDuty administrador delegado puede optar por habilitar automáticamente Lambda Network Activity Monitoring para todas las cuentas nuevas a medida que se unan a la organización. Para obtener más información sobre los entornos de varias cuentas, consulta [Administrar varias cuentas en Amazon](#). GuardDuty

## Activación de Lambda Protection para una cuenta de administrador delegado GuardDuty

Elija el método de acceso que prefiera para activar o desactivar la supervisión de actividad de red Lambda para la cuenta de administrador delegado. GuardDuty

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda, seleccione Editar.
4. Realice una de las siguientes acciones:

#### Uso de Habilitar para todas las cuentas

- Elija Habilitar para todas las cuentas. Esto habilitará el plan de protección para todas las GuardDuty cuentas activas de su AWS organización, incluidas las nuevas cuentas que se unan a la organización.
- Seleccione Save.

#### Uso de Configurar cuentas manualmente

- Para habilitar el plan de protección solo para la cuenta de GuardDuty administrador delegado, elija Configurar las cuentas manualmente.
- Seleccione Activar en la sección de la cuenta de GuardDuty administrador delegado (esta cuenta).
- Seleccione Save.

### API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el features del objeto name como LAMBDA\_NETWORK\_LOGS y status como ENABLED.

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la Protección Lambda.

Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectorsAPI](#).

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
region us-east-1 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

## Auto-enable Supervisión de la actividad de red Lambda para todas las cuentas de los miembros

Elija su método de acceso preferido para habilitar la característica de supervisión de la actividad de red de Lambda en todas las cuentas de miembros. Esto incluye las cuentas de miembros existentes y las cuentas nuevas que se unen a la organización.

### Console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:

#### Uso de la página de planes de protección

1. En el panel de navegación, elija Planes de protección.
2. Elija Configurar todas las habilitaciones.
3. En Protección Lambda, seleccione Activar para todas las cuentas. Esta acción habilita automáticamente la supervisión de la actividad de red de Lambda para las cuentas nuevas y existentes de la organización.
4. Seleccione Guardar todo y, a continuación, seleccione Confirmar y guardar.

#### Note

La actualización de la configuración de las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

## Uso de la página Cuentas

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, selecciona Auto-enable tus preferencias antes de Añadir cuentas por invitación.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para todas las cuentas en Supervisión de la actividad de red de Lambda.

### Note

De forma predeterminada, esta acción activa automáticamente la opción Auto-enable GuardDuty para cuentas de nuevos miembros.

4. Seleccione Save.

Si no puede utilizar la opción Habilitar para todas las cuentas, consulte [Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros](#).

## API/CLI

Para activar o desactivar de forma selectiva el Monitoreo de Actividad de Red Lambda para sus cuentas de miembros, invoque la operación de API con [updateMemberDetectors](#) la suya propia. *detector ID*

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la Protección Lambda.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-ids 111122223333 --region us-east-1 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitación de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes de la organización.

### Console

Configuración de la supervisión de la actividad de red de Lambda para todas las cuentas de miembros activas existentes

1. Inicia sesión en Consola de administración de AWS y abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Inicie sesión con las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija Planes de protección.
3. Elija Configurar todas las habilitaciones. En Protección Lambda, puede ver el estado actual de la configuración. En la sección Cuentas de miembros activas, seleccione Acciones.
4. En el menú desplegable Acciones, seleccione Habilitar para todas las cuentas de miembros activas existentes.
5. Elija Confirmar.

### API/CLI

Para activar o desactivar de forma selectiva el Monitoreo de Actividad de Red Lambda para sus cuentas de miembros, invoque la operación de API con [updateMemberDetectors](#) la suya propia.  
*detector ID*

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda. Ejecute el siguiente comando y *12abc34d567e8fa901bc2d34e56789f0* sustitúyalo por el ID del detector de su cuenta y *us-east-1* por la región en la que desee activar la Protección Lambda.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Auto-enable Supervisión de actividad de red Lambda para cuentas de nuevos miembros

Elija su método de acceso preferido para habilitar la supervisión de la actividad de red de Lambda en las nuevas cuentas de miembros que se unen a la organización.

### Console

La cuenta de GuardDuty administrador delegado puede activar Lambda Network Activity Monitoring para las cuentas de los nuevos miembros de una organización mediante la página Lambda Protection o la página Cuentas.

Habilitación automática de la Supervisión de la actividad de red de Lambda para las nuevas cuentas de miembros

1. Abra la consola en GuardDuty . <https://console.aws.amazon.com/guardduty/>

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. Realice una de las siguientes acciones:
  - A través de la página de planes de protección:
    1. En el panel de navegación, elija Planes de protección.
    2. Elija Configurar todas las habilitaciones.
    3. Elija Configurar cuentas manualmente.
    4. Elija Habilitar automáticamente las cuentas de miembros nuevas. Este paso garantiza que cada vez que una nueva cuenta se una a su organización, la protección de Lambda se habilitará automáticamente para la cuenta. Solo la cuenta de GuardDuty administrador delegado de la organización puede modificar esta configuración.

## 5. Seleccione Save.

- Mediante la página Cuentas:

1. En el panel de navegación, elija Cuentas.
2. En la página Cuentas, seleccione Auto-enable las preferencias.
3. En la ventana Administrar preferencias de habilitación automática, seleccione Habilitar para las nuevas cuentas en Supervisión de la actividad de red de Lambda.
4. Seleccione Save.

## API/CLI

Para habilitar la supervisión de actividad de red Lambda para las cuentas de los nuevos miembros, invoque la operación de la [UpdateOrganizationConfiguration](#) API con la suya propia.

*detector ID*

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda. En el siguiente ejemplo se muestra cómo se puede habilitar la supervisión de la actividad de red de Lambda para una sola cuenta de miembro. *12abc34d567e8fa901bc2d34e56789f0* Sustitúyalo por el ID del detector de tu cuenta y *us-east-1* por la región en la que quieres activar la Protección Lambda. Si no quiere habilitarla para todas las cuentas nuevas que se unan a la organización, establezca `AutoEnable` en `NONE`.

Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1 --auto-enable --features ' [{"Name": "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"} ] '
```

Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitación o deshabilitación selectiva de la supervisión de la actividad de red de Lambda para las cuentas de miembros

Elija el método de acceso que prefiera para habilitar o deshabilitar de forma selectiva la supervisión de la actividad de red de Lambda en las cuentas de miembros.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Asegúrese de utilizar las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, en Configuración, seleccione Cuentas.

En la página Cuentas, revise la columna Supervisión de la actividad de red de Lambda. Indica si la supervisión de la actividad de red de Lambda está habilitada o no.

3. Elija la cuenta para la que desee configurar la protección de Lambda. Puede elegir varias cuentas a la vez.
4. En el menú desplegable Editar planes de protección, elija Supervisión de la actividad de red de Lambda y, a continuación, elija una acción adecuada.

### API/CLI

Invoca la [updateMemberDetectors](#) API con la tuya propia. *detector ID*

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda.

*12abc34d567e8fa901bc2d34e56789f0* Sustitúyalo por el ID del detector de tu cuenta y *us-east-1* por la región en la que quieres activar la Protección Lambda.

Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
--region us-east-1 --account-ids 111122223333 --features '[{"Name":
"LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
```

También puede pasar una lista de ID de cuentas separadas por un espacio.



Cuando el código se haya ejecutado correctamente, devolverá una lista de `UnprocessedAccounts` vacía. Si se ha producido algún problema al cambiar la configuración del detector de una cuenta, se muestra el ID de la cuenta junto con un resumen del problema.

## Habilitar la protección de Lambda para una cuenta independiente

Una cuenta independiente es la que decide activar o desactivar un plan de protección Cuenta de AWS en un plan específico Región de AWS.

Si su cuenta está asociada a una cuenta de GuardDuty administrador mediante AWS Organizations una invitación o mediante el método de invitación, esta sección no se aplica a su cuenta. Para obtener más información, consulte [Habilitar la protección de Lambda en entornos de varias cuentas](#).

Tras activar Lambda Protection, GuardDuty empezará a monitorizar [Supervisión de la actividad de red de Lambda](#) en su cuenta.

Elija el método de acceso que prefiera para configurar la protección de Lambda para una cuenta independiente.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, en Configuración, elija Protección de Lambda.
3. En la página Protección de Lambda se muestra el estado actual de su cuenta. Elija Habilitar para habilitar la protección de Lambda en la cuenta.
4. Elija Confirmar para guardar su selección.

### API/CLI

Ejecute la operación de la API [updateDetector](#) con el ID del detector regional propio y transmita el `features` del objeto `name` como `LAMBDA_NETWORK_LOGS` y `status` como `ENABLED`.

Como alternativa, puede utilizar AWS CLI para activar la Protección Lambda. Ejecute el siguiente comando y `12abc34d567e8fa901bc2d34e56789f0` sustitúyalo por el ID del detector de su cuenta y `us-east-1` por la región en la que desee activar la Protección Lambda.

Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0  
--region us-east-1 --features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" :  
"ENABLED"}]'
```

# Proteja las cargas de trabajo de IA con GuardDuty

[La detección de amenazas GuardDuty fundamental](#) de Amazon y [Lambda](#) Protection le ayudan a proteger y detectar mejor las amenazas a las cargas de trabajo de IA basadas en ellas. AWS

[La detección de GuardDuty amenazas básica monitorea los eventos AWS CloudTrail de administración para detectar actividades sospechosas y maliciosas en las cargas de trabajo generativas de IA creadas mediante el uso de AWS servicios, incluidos Amazon Bedrock y Amazon AI. SageMaker](#) Por ejemplo, GuardDuty puede identificar actividades como:

- Supresión inusual de las barreras de protección de seguridad de Amazon Bedrock
- Cambio del origen de los datos de entrenamiento del modelo que puede provocar potencialmente un ataque de envenenamiento de datos.
- Invocación sospechosa del modelo de Amazon Bedrock
- Se ha desactivado el registro de las invocaciones del modelo Amazon Bedrock que pueden indicar intentos de evadir la detección.
- Ejemplo inusual de cuaderno o formación para la creación de puestos de trabajo en IA SageMaker
- Credenciales exfiltradas de Amazon Elastic Compute Cloud que pueden haberse utilizado para llamar a las API de Amazon Bedrock, Amazon SageMaker AI o a cargas de trabajo de IA autogestionadas en instancias de EC2, clústeres de EKS o tareas de ECS.

GuardDuty Lambda Protection puede ayudar a detectar posibles amenazas relacionadas con los agentes de Amazon Bedrock. Esto puede incluir actividad sospechosa en la red, como la minería de criptomonedas, y la comunicación con servidores de mando y control maliciosos que pueden ser provocados por un ataque a la cadena de suministro o peticiones complejas.

En el siguiente video se puede ver cómo serían los resultados asociados.

En el siguiente video se puede ver cómo serían los resultados asociados. [Cómo usar Amazon GuardDuty para monitorear y proteger sus cargas de trabajo de IA basadas en AWS](#)

# Varias cuentas en Amazon GuardDuty

Cuando su AWS entorno tiene varias cuentas, puede administrarlas designando una Cuenta de AWS como cuenta de administrador. A continuación, puede asociar el múltiplo Cuentas de AWS a esta cuenta de administrador como sus cuentas de miembros. Con esta configuración, una cuenta de GuardDuty administrador designada puede evaluar y supervisar la seguridad general de su organización. La cuenta de administrador también puede realizar tareas de administración de cuentas, como revisar todos los hallazgos generados y configurar los planes de protección en ella GuardDuty.

En GuardDuty, una organización consta de una cuenta de GuardDuty administrador delegado y una o más cuentas de miembros asociadas. Puede asociar las cuentas de dos maneras: integrándolas o utilizando un método tradicional de enviar y aceptar invitaciones de membresía en la GuardDuty consola. AWS Organizations GuardDuty recomienda que se integre con AWS Organizations.

## Note

El botón Editar de la sección de activación automática de la página Cuentas lo redirige a la [Configuración de planes de protección](#) página en lugar de abrir el modal de configuración anterior.

AWS Organizations es un servicio de administración de cuentas global que permite a AWS los administradores consolidar y administrar múltiples cuentas de forma centralizada. Cuentas de AWS Proporciona características de facturación unificada y administración de cuentas que están diseñadas para satisfacer las necesidades de presupuestos, seguridad y conformidad. Se ofrece sin cargo adicional y se integra con varios Servicios de AWS, incluidos Macie y Amazon GuardDuty. AWS Security Hub CSPM Para obtener más información, consulte la [Guía del usuario de AWS Organizations](#).

## Contenido

- [Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros](#)
- [Administrar GuardDuty cuentas con AWS Organizations](#)
- [Administrar GuardDuty cuentas por invitación](#)
- [GuardDuty consideraciones para exportar los detalles de las cuentas de los miembros en formato CSV](#)

# Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros

Cuando se utiliza GuardDuty en un entorno de varias cuentas, la cuenta de administrador puede gestionar ciertos aspectos de las cuentas de los miembros GuardDuty en nombre de las cuentas de los miembros. Una cuenta de administrador puede realizar las siguientes funciones principales:

- Agregar y eliminar cuentas de miembros asociadas: el proceso mediante el cual una cuenta de administrador puede hacerlo varía según la forma en que administre las cuentas, mediante el método de invitación AWS Organizations o según el método de GuardDuty invitación.

GuardDuty recomienda administrar sus cuentas de miembros mediante AWS Organizations.

- Habilitación de la cuenta de GuardDuty administrador delegado GuardDuty en la cuenta de administración: si la cuenta AWS Organizations de administración alguna vez se desactiva GuardDuty, la cuenta de GuardDuty administrador delegado puede habilitarla GuardDuty en la cuenta de administración. Sin embargo, es necesario que la cuenta de administración no haya eliminado explícitamente el [Service-linked permisos de rol para GuardDuty](#).
- Configurar el estado de las cuentas de los miembros: una cuenta de administrador puede habilitar o deshabilitar el estado de los planes de GuardDuty protección y habilitar, suspender o deshabilitar el estado GuardDuty en nombre de las cuentas de los miembros asociadas.

La cuenta de GuardDuty administrador delegado gestionada con AWS Organizations puede activarse automáticamente GuardDuty cuando Cuentas de AWS se añaden como miembros.

- Personalice cuándo generar hallazgos: una cuenta de administrador puede personalizar los hallazgos dentro de la GuardDuty red mediante la creación y administración de reglas de supresión, listas de IP confiables y listas de amenazas. En un entorno de cuentas múltiples, el soporte para configurar estas funciones solo está disponible para una cuenta de administrador delegado GuardDuty . Una cuenta de miembro no puede actualizar esta configuración.

En la siguiente tabla se detalla la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros.

Clave para la tabla

- Auto: una cuenta solo puede realizar la acción enumerada para su propia cuenta.
- Cualquiera: una cuenta puede realizar la acción enumerada para cualquier cuenta asociada.

- Todas: una cuenta puede realizar la acción enumerada y se aplica a todas las cuentas asociadas. Por lo general, la cuenta que realiza esta acción es una cuenta de GuardDuty administrador designada
- Celdas con guión (-): las celdas de la tabla con guión (-) indican que la cuenta no puede realizar la acción indicada.

| Action                                                                                            | A través de AWS Organizations              |                            | Por invitación                    |                            |
|---------------------------------------------------------------------------------------------------|--------------------------------------------|----------------------------|-----------------------------------|----------------------------|
|                                                                                                   | Cuenta de GuardDuty administrador delegado | Cuenta de miembro asociada | GuardDuty cuenta de administrador | Cuenta de miembro asociada |
| Habilitar GuardDuty                                                                               | Cualquiera                                 | –                          | Auto                              | Auto                       |
| Habilitar GuardDuty automáticamente para toda la organización (ALL,NEW,NONE)                      | Todos                                      | –                          | –                                 | –                          |
| Ver todas las cuentas de los miembros de Organizations, independientemente de su GuardDuty estado | Cualquiera                                 | –                          | –                                 | –                          |
| Genere ejemplos de hallazgos                                                                      | Auto                                       | Auto                       | Auto                              | Auto                       |

|                                                                |            |        |            |        |
|----------------------------------------------------------------|------------|--------|------------|--------|
| Ver todos los GuardDuty hallazgos                              | Cualquiera | Propia | Cualquiera | Propia |
| Archive GuardDuty los hallazgos                                | Cualquiera | —      | Cualquiera | —      |
| Aplicar reglas de supresión                                    | Todos      | —      | Todos      | —      |
| Cree listas de IP confiables o listas de amenazas              | Todos      | —      | Todos      | —      |
| Actualice la lista de IP de confianza o las listas de amenazas | Todos      | —      | Todos      | —      |
| Elimine la lista de IP de confianza o las listas de amenazas   | Todos      | —      | Todos      | —      |
| Establezca la frecuencia EventBridge de las notificaciones     | Todos      | —      | Todos      | —      |
| Establecer la ubicación de Amazon S3 para exportar resultados  | Todos      | Auto   | Auto       | Auto   |

|                                                                                                   |            |      |            |      |
|---------------------------------------------------------------------------------------------------|------------|------|------------|------|
| Habilitar uno o varios planes de protección opcionales para toda la organización (ALL, NEW, NONE) | Todos      | —    | —          | —    |
| Esto no incluye la protección contra malware para S3.                                             |            |      |            |      |
| Habilite cualquier plan de GuardDuty protección para cuentas individuales                         | Cualquiera | —    | Cualquiera | —    |
| Esto no incluye Malware Protection for EC2 y la protección contra malware para S3.                |            |      |            |      |
| Malware Protection for EC2                                                                        | Cualquiera | —    | Propia     | —    |
| Protección contra malware para EC2: análisis de On-demand malware                                 | Cualquiera | Auto | Auto       | Auto |



|                                             |             |      |             |      |
|---------------------------------------------|-------------|------|-------------|------|
| Protección contra malware para S3           | –           | Auto | –           | Auto |
| Desasociar una cuenta de miembro            | Cualquier + | –    | Cualquiera  | –    |
| Desasociarse de una cuenta de administrador | –           | –    | –           | Auto |
| Eliminar una cuenta de miembro disociada    | Cualquiera  | –    | Cualquiera  | –    |
| Suspender GuardDuty                         | Cualquier * | –    | Cualquier * | –    |
| Desactivar GuardDuty                        | Cualquier * | –    | Cualquier * | Auto |

<sup>+</sup> Indica que la cuenta de GuardDuty administrador delegado solo puede realizar esta acción si no ha configurado las preferencias de activación automática para los miembros de ALL la organización.

<sup>\*</sup> Indica que una cuenta de GuardDuty administrador delegado no se puede deshabilitar directamente GuardDuty en la cuenta de un miembro. La cuenta de GuardDuty administrador delegado primero debe desasociar la cuenta de miembro y, a continuación, eliminarla. Después de esto, cada cuenta de miembro puede desactivarse GuardDuty en sus propias cuentas. Para obtener más información sobre cómo realizar estas tareas en la organización, consulte [Administre continuamente sus cuentas de miembros dentro GuardDuty](#).

## Administrar GuardDuty cuentas con AWS Organizations

En una AWS organización, la cuenta de administración puede designar cualquier cuenta de esta organización como cuenta de administrador delegado. GuardDuty Para esta cuenta de administrador, GuardDuty se habilita automáticamente solo en la cuenta actual Región de AWS. De forma

predeterminada, la cuenta de administrador puede habilitar y administrar todas GuardDuty las cuentas de los miembros de la organización dentro de esa región. La cuenta de administrador puede ver y añadir miembros a esta AWS organización.

En las siguientes secciones, se explican diversas tareas que puede realizar como cuenta de GuardDuty administrador delegado.

## Contenido

- [Consideraciones y recomendaciones para su uso con GuardDuty AWS Organizations](#)
- [Permisos necesarios para designar una cuenta de GuardDuty administrador delegado](#)
- [Designación de una cuenta de administrador delegado GuardDuty](#)
- [Configuración de las preferencias de habilitación automática de la organización](#)
- [Cómo agregar miembros a la organización](#)
- [\(Opcional\) Habilitar planes de protección para cuentas de miembro existentes](#)
- [Administre continuamente sus cuentas de miembros dentro GuardDuty](#)
- [Suspensión GuardDuty para la cuenta de un miembro](#)
- [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#)
- [Eliminar las cuentas de los miembros de GuardDuty la organización](#)
- [Cambiar la cuenta de administrador delegado GuardDuty](#)

## Consideraciones y recomendaciones para su uso con GuardDuty AWS Organizations

Las siguientes consideraciones y recomendaciones pueden ayudarle a entender cómo funciona una cuenta de GuardDuty administrador delegado en GuardDuty:

Una cuenta de GuardDuty administrador delegado puede gestionar un máximo de 50 000 miembros.

Hay un límite de 50 000 cuentas de miembros por cuenta de GuardDuty administrador delegado. Esto incluye las cuentas de miembros que se agreguen a través de su organización AWS Organizations o las que hayan aceptado la invitación de la cuenta de GuardDuty administrador para unirse a su organización. Sin embargo, puede haber más de 50 000 cuentas en su AWS organización.

Si superas el límite de 50 000 cuentas de CloudWatch miembros, recibirás una notificación y un correo electrónico a la cuenta de GuardDuty administrador delegado designada. Panel de estado

Una cuenta de GuardDuty administrador delegado es regional.

A diferencia AWS Organizations de, GuardDuty es un servicio regional. Las cuentas de GuardDuty administrador delegado y sus cuentas de miembros deben añadirse AWS Organizations en cada región deseada en la que se haya GuardDuty activado. Si la cuenta de administración de la organización designa una cuenta de GuardDuty administrador delegado solo en EE. UU. Este (Norte de Virginia), la cuenta de GuardDuty administrador delegado solo administrará las cuentas de los miembros que se agreguen a la organización en esa región. Para obtener más información sobre la paridad de funciones en las regiones en las que GuardDuty está disponible, consulte. [Regiones y puntos de conexión](#)

### Casos especiales para las regiones incluidas

- Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (NEW) o para todas las cuentas de miembros (ALL), GuardDuty no se puede habilitar para ninguna cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la [GuardDuty consola](#) o utilice la API. [ListMembers](#)
- Cuando trabaje con la configuración de GuardDuty activación automática establecida en NEW, asegúrese de que se cumpla la siguiente secuencia:
  1. Las cuentas de miembro se incluyen en una región incluida.
  2. Agregue las cuentas de miembro a la organización en AWS Organizations.

Si cambias el orden de estos pasos, la configuración de GuardDuty activación automática con no **NEW** funcionará en la región de suscripción específica porque la cuenta de miembro ya no es nueva en la organización. GuardDuty ofrece dos soluciones alternativas:

- Establezca la configuración de GuardDuty activación automática en ALL, que incluye las cuentas de los miembros nuevas y existentes. En este caso, el orden de estos pasos no es relevante.
- Si la cuenta de un miembro ya forma parte de su organización, gestione la GuardDuty configuración de esta cuenta de forma individual en la región de suscripción específica mediante la GuardDuty consola o la API.

Es obligatorio para que una AWS organización tenga la misma cuenta de GuardDuty administrador delegado en todas las. Regiones de AWS

Debe designar una cuenta de miembro como cuenta de GuardDuty administrador delegado en todos los Regiones de AWS lugares GuardDuty que estén habilitados. Por ejemplo, si designa una cuenta de miembro **111122223333** en **Europe (Ireland)**, no podrá designar otra cuenta de miembro **555555555555** en **Canada (Central)**. Es obligatorio que utilices la misma cuenta que la cuenta de GuardDuty administrador delegado en todas las demás regiones.

Puede designar una nueva cuenta de GuardDuty administrador delegado en cualquier momento. Para obtener más información sobre cómo eliminar la cuenta de GuardDuty administrador delegado existente, consulte [Cambiar la cuenta de administrador delegado GuardDuty](#)

No se recomienda configurar la cuenta de administración de la organización como cuenta de GuardDuty administrador delegado.

La cuenta de administración de su organización puede ser la cuenta de GuardDuty administrador delegado. Sin embargo, las prácticas recomendadas de seguridad de AWS siguen el principio de privilegios mínimos y no recomiendan esta configuración.

El cambio de una cuenta de GuardDuty administrador delegado no desactiva las cuentas de GuardDuty los miembros.

Si elimina una cuenta de GuardDuty administrador delegado, GuardDuty elimina todas las cuentas de miembro asociadas a esta cuenta de administrador delegado GuardDuty . GuardDuty sigue habilitada para todas estas cuentas de miembros.

## Permisos necesarios para designar una cuenta de GuardDuty administrador delegado

Para empezar a usar Amazon GuardDuty con AWS Organizations, la cuenta AWS Organizations de administración de la organización designa una cuenta como cuenta de GuardDuty administrador delegado. Esto se habilita GuardDuty como un servicio confiable en. AWS Organizations También habilita GuardDuty la cuenta de GuardDuty administrador delegado y también permite que la cuenta de administrador delegado active y gestione otras cuentas GuardDuty de la organización en la región actual. Para obtener información sobre cómo se conceden estos permisos, consulte [Utilización AWS Organizations con otros AWS servicios](#).

Como cuenta de AWS Organizations administración, antes de designar la cuenta de GuardDuty administrador delegado para su organización, compruebe que puede realizar la siguiente GuardDuty

acción: `guardduty:EnableOrganizationAdminAccount`. Esta acción le permite designar la cuenta de GuardDuty administrador delegado para su organización mediante GuardDuty. También debe asegurarse de que está autorizado a realizar las AWS Organizations acciones que le ayuden a recuperar información sobre su organización.

Para conceder estos permisos, incluye la siguiente declaración en la política AWS Identity and Access Management (IAM) de tu cuenta:

```
{
  "Sid": "PermissionsForGuardDutyAdmin",
  "Effect": "Allow",
  "Action": [
    "guardduty:EnableOrganizationAdminAccount",
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
}
```

Si desea designar su cuenta AWS Organizations de administración como cuenta de GuardDuty administrador delegado, su cuenta también necesitará la acción de IAM: `CreateServiceLinkedRole`. Esta acción le permite inicializar la cuenta de GuardDuty administración. Sin embargo, revise [Consideraciones y recomendaciones para su uso con GuardDuty AWS Organizations](#) antes de proceder a agregar los permisos.

Para continuar designando la cuenta de administración como cuenta de GuardDuty administrador delegado, añada la siguiente declaración a la política de IAM y **111122223333** sustitúyala por el ID de la cuenta de administración de su organización:

```
{
  "Sid": "PermissionsToEnableGuardDuty",
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "*"
}
```

```
"Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
"Condition": {
  "StringLike": {
    "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
}
```

## Designación de una cuenta de administrador delegado GuardDuty

En esta sección se indican los pasos para designar un administrador delegado en la organización de GuardDuty.

Como cuenta de administración de la AWS organización, asegúrese de leer detenidamente el funcionamiento [Recomendaciones y consideraciones](#) de una cuenta de GuardDuty administrador delegado. Antes de continuar, asegúrese de contar con [Permisos necesarios para designar una cuenta de GuardDuty administrador delegado](#).

Elija un método de acceso preferido para designar una cuenta de GuardDuty administrador delegado para su organización. Solo una cuenta de administración puede realizar este paso.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Para iniciar sesión, utilice las credenciales de la cuenta de administración de la organización de AWS Organizations .

2. Con el Región de AWS selector situado en la esquina superior derecha de la página, seleccione la región en la que desee designar la cuenta de GuardDuty administrador delegado de su organización.
3. Realice una de las siguientes acciones, en función de si GuardDuty está habilitada para su cuenta de administración en la región actual:
  - Si no GuardDuty está activado, selecciona Amazon GuardDuty : todas las funciones y elige Comenzar. Esta acción te llevará a la GuardDuty página de bienvenida.
  - Si GuardDuty está habilitada, selecciona Configuración en el panel de navegación.
4. En Administrador delegado, introduzca el Cuenta de AWS ID de 12 dígitos de la cuenta que desee designar como cuenta de GuardDuty administrador delegado de la organización.

Asegúrese de activar la cuenta GuardDuty de GuardDuty administrador delegado recién designada; de lo contrario, no podrá realizar ninguna acción.

5. Elija Delegar.
6. (Recomendado) Repita los pasos anteriores para designar la cuenta de GuardDuty administrador delegado en cada una de las cuentas que Región de AWS haya GuardDuty activado.

## API/CLI

1. Ejecute [enableOrganizationAdminAccount](#) con las credenciales de la cuenta Cuenta de AWS de administración de la organización.
  - Alternativamente, puede usarlo AWS Command Line Interface para hacer esto. El siguiente AWS CLI comando designa una cuenta de GuardDuty administrador delegado únicamente para su región actual. Ejecute el siguiente AWS CLI comando y asegúrese de **111111111111** reemplazarlo por el Cuenta de AWS ID de la cuenta que desea designar como cuenta de administrador delegado GuardDuty :

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
```

Para designar la cuenta de GuardDuty administrador delegado para otras regiones, especifique la región en el AWS CLI comando. El siguiente ejemplo muestra cómo habilitar una cuenta de GuardDuty administrador delegado en el oeste de EE. UU. (Oregón). Asegúrese de **us-west-2** sustituirla por la región a la que desee asignar la cuenta de GuardDuty administrador delegado.

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111 --region us-west-2
```

Para obtener información sobre la Regiones de AWS ubicación GuardDuty disponible, consulte [Regiones y puntos de conexión](#).

Si GuardDuty está deshabilitado para tu cuenta de GuardDuty administrador delegado, no podrá realizar ninguna acción. Si aún no lo ha hecho, asegúrese de activar la GuardDuty cuenta de GuardDuty administrador delegado recién designada.

2. (Recomendado) Repita los pasos anteriores para designar la cuenta de GuardDuty administrador delegado en cada uno de los lugares en los que Región de AWS haya GuardDuty activado la cuenta.

## Configuración de las preferencias de habilitación automática de la organización

La función de organización de activación automática le GuardDuty ayuda a establecer el mismo estado GuardDuty y el estado de los planes de protección para ALL las cuentas existentes o de NEW los miembros de su organización, en un solo paso. Del mismo modo, también puede especificar cuándo no desea realizar ninguna acción en las cuentas de miembro. Para ello, seleccione NONE. En los siguientes pasos se explica esta configuración y también se indica cuándo conviene utilizar un ajuste específico.

### Note

Puede configurar las preferencias de activación automática para todos los planes de protección excepto [Protección contra malware para S3](#).

Elija un método de acceso preferente para actualizar las preferencias de habilitación automática de la organización.

### Console

1. Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

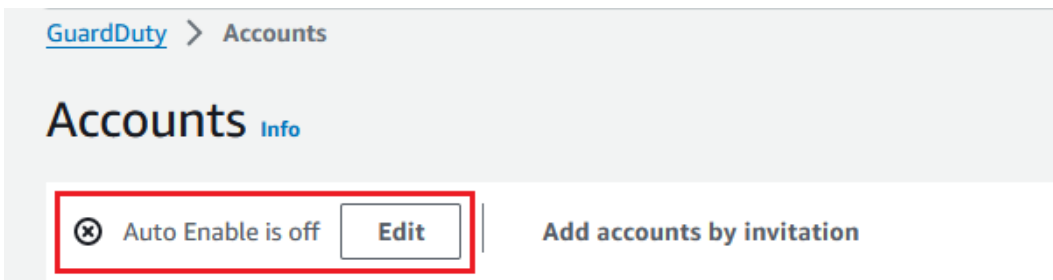
Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador.

2. En el panel de navegación, elija Cuentas.

La página Cuentas proporciona opciones de configuración para la cuenta GuardDuty del administrador Auto-enable GuardDuty y los planes de protección opcionales en nombre de las cuentas de los miembros que pertenecen a la organización.

3. Para actualizar la configuración de habilitación automática existente, seleccione Editar.





Este soporte está disponible para configurar GuardDuty y todos los planes de protección opcionales compatibles con usted Región de AWS. Puede seleccionar una de las siguientes opciones de configuración GuardDuty en nombre de sus cuentas de miembro:

- Habilitar para todas las cuentas (**ALL**): seleccione esta opción para habilitar la opción correspondiente para todas las cuentas de una organización. Esto incluye las cuentas nuevas que se unen a la organización y las cuentas que pueden haber sido suspendidas o eliminadas de la organización. Esto también incluye la cuenta de GuardDuty administrador delegado.

 Note

Es posible que la actualización de la configuración de todas las cuentas de miembro tarde hasta 24 horas.

- Auto-enable para cuentas nuevas (**NEW**): seleccione habilitar automáticamente GuardDuty o los planes de protección opcionales solo para las cuentas de los nuevos miembros cuando se unan a su organización.
- No habilitar (**NONE**): seleccione esta opción para impedir que se habilite la opción correspondiente en las cuentas de su organización. En este caso, la cuenta de GuardDuty administrador administrará cada cuenta de forma individual.

Al actualizar la configuración de habilitación automática de ALL o NEW a NONE, esta acción no desactiva la opción correspondiente para las cuentas existentes. Esta configuración se aplicará a las nuevas cuentas que se unan a la organización. Después de actualizar la configuración de habilitación automática, ninguna cuenta nueva tendrá la opción correspondiente como habilitada.

 Note

Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (NEW) o para todas las cuentas de miembros (ALL), GuardDuty no se puede habilitar para ninguna cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la [GuardDuty consola](#) o utilice la API. [ListMembers](#)

4. Seleccione Save changes (Guardar cambios).
5. (Opcional) si desea utilizar las mismas preferencias en cada región, actualice las preferencias en cada una de las regiones admitidas por separado.

Es posible que algunos de los planes de protección opcionales no estén disponibles en todos los Regiones de AWS lugares GuardDuty disponibles. Para obtener más información, consulte [Regiones y puntos de conexión](#).

## API/CLI

1. Utilice [UpdateOrganizationConfiguration](#) las credenciales de la cuenta de GuardDuty administrador delegado para configurar GuardDuty automáticamente los planes de protección opcionales en esa región para su organización. Para obtener información sobre las distintas configuraciones de activación automática, consulte [automático EnableOrganizationMembers](#).

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

Para configurar las preferencias de habilitación automática para cualquiera de los planes de protección opcionales admitidos en su región, siga los pasos que se indican en las secciones de la documentación correspondientes a cada plan de protección.

2. Puede validar las preferencias de su organización en la región actual. Ejecute [describeOrganizationConfiguration](#). Asegúrese de especificar el ID de detector de la cuenta de GuardDuty administrador delegado.

 Note

La actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse.

3. También puede ejecutar el siguiente AWS CLI comando para configurar las preferencias y habilitar o deshabilitar automáticamente GuardDuty en esa región las cuentas nuevas (NEW) que se unan a la organización, todas las cuentas (ALL) o ninguna de las cuentas (NONE) de la organización. Para obtener más información, consulte [auto EnableOrganizationMembers](#). Según sus preferencias, es posible que deba sustituir NEW por ALL o NONE. Si configura el plan de protección con ALL, el plan de protección también se habilitará para la cuenta de GuardDuty administrador delegado. Asegúrese de especificar el ID del detector de la cuenta de GuardDuty administrador delegado que gestiona la configuración de la organización.

Para encontrar el `detectorId` de su cuenta y su región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
```

4. Puede validar las preferencias de su organización en la región actual. Ejecute el siguiente AWS CLI comando mediante el ID de detector de la cuenta de GuardDuty administrador delegado.

```
aws guardduty describe-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0
```

(Se recomienda) repita los pasos anteriores en cada región utilizando el ID de detector de la cuenta de GuardDuty administrador delegado.

 Note

Cuando una cuenta de GuardDuty administrador delegado opta por no participar en una región de suscripción, incluso si su organización tiene la configuración de activación GuardDuty automática configurada solo para cuentas de miembros nuevos (NEW) o para todas las cuentas de miembros (ALL), GuardDuty no se puede habilitar para ninguna

cuenta de miembro de la organización que esté deshabilitada actualmente. GuardDuty Para obtener información sobre la configuración de las cuentas de sus miembros, abra Cuentas en el panel de navegación de la [GuardDuty consola](#) o utilice la API. [ListMembers](#)

## Cómo agregar miembros a la organización

Como cuenta de GuardDuty administrador delegado, puede añadir una o varias Cuentas de AWS a la GuardDuty organización. Al añadir una cuenta como GuardDuty miembro, se GuardDuty habilitará automáticamente en esa región. Hay una excepción a la cuenta de administración de la organización. Antes de que la cuenta de administración se añada como GuardDuty miembro, debe estar GuardDuty habilitada.

Elige el método que prefieras para añadir una cuenta de miembro a tu GuardDuty organización.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.

La tabla de cuentas muestra todas las cuentas de los miembros que están activas (no suspendidas Cuentas de AWS) y que pueden estar asociadas a la cuenta de GuardDuty administrador delegado. Si la cuenta de miembro está asociada a la cuenta de administrador de la organización, el Tipo será uno de los siguientes: A través de Organizations o Por invitación. Si una cuenta de miembro no está asociada a la cuenta de GuardDuty administrador de la organización, el tipo de esta cuenta de miembro es No miembro.

3. Seleccione uno o varios ID de cuenta que desee agregar en calidad de miembros. Estos ID de cuenta deben tener el Tipo como A través de organizaciones.

Las cuentas que se agregan por invitación no forman parte de su organización. Puede administrador dichas cuentas de forma individual. Para obtener más información, consulte [Administración de cuentas por invitación](#).

4. Seleccione el menú desplegable Acciones y, a continuación, elija Agregar miembro. Después de añadir esta cuenta como miembro, se aplicará la GuardDuty configuración de activación automática. En función de los ajustes establecidos [Configuración de las preferencias de](#)

[habilitación automática de la organización](#), la GuardDuty configuración de estas cuentas puede cambiar.

5. Puede seleccionar la flecha hacia abajo de la columna Estado para ordenar las cuentas según el estado No es miembro y, a continuación, elegir las cuentas que no GuardDuty estén habilitadas en la región actual.

Si aún no se ha agregado como miembro ninguna de las cuentas que figuran en la tabla de cuentas, puedes habilitarlas GuardDuty en la región actual para todas las cuentas de la organización. Elija Habilitar en el encabezado de la parte superior de la página. Esta acción activa automáticamente la Auto-enable GuardDuty configuración para que GuardDuty se habilite para cualquier cuenta nueva que se una a la organización.

6. Elija Confirmar para agregar las cuentas como miembros. Esta acción también se activa GuardDuty para todas las cuentas seleccionadas. El Estado de las cuentas invitadas cambiará a Habilitado.
7. (Recomendado) Repita estos pasos en cada una de ellas Región de AWS. Esto garantiza que la cuenta de GuardDuty administrador delegado pueda gestionar las búsquedas y otras configuraciones de las cuentas de los miembros en todas las regiones en las que haya GuardDuty activado la cuenta.

La función de activación automática se habilita GuardDuty para todos los futuros miembros de su organización. Esto permite que su cuenta de GuardDuty administrador delegado administre los nuevos miembros que se creen o se agreguen a la organización. Cuando el número de cuentas de miembros alcanza el límite de 50 000, la Auto-enable función se desactiva automáticamente. Si eliminas una cuenta de miembro y el número total de miembros se reduce a menos de 50 000, la Auto-enable función se vuelve a activar.

## API/CLI

- Se ejecuta [CreateMembers](#) con las credenciales de la cuenta de GuardDuty administrador delegado.

Debe especificar el ID de detector regional de la cuenta de GuardDuty administrador delegado y los detalles de la cuenta (Cuenta de AWS ID y direcciones de correo electrónico correspondientes) de las cuentas que desee añadir como GuardDuty miembros. Puede crear uno o varios miembros con esta operación de API.

Cuando ejecute `CreateMembers` en la organización, las preferencias de habilitación automática para nuevos miembros se aplicarán a medida que nuevas cuentas de miembro se unan a la organización. Cuando se ejecuta `CreateMembers` con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de miembro existentes.

Ejecuta [ListAccounts](#) la referencia de la AWS Organizations API para ver todas las cuentas de la AWS organización.

- Como alternativa, puede utilizar AWS Command Line Interface. Ejecute el siguiente comando de la AWS CLI y asegúrese de utilizar su propio ID de detector válido, su ID de Cuenta de AWS y la dirección de correo electrónico asociada al ID de la cuenta.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0
--account-details AccountId=111122223333,Email=guardduty-member-
name@amazon.com
```

Para ver una lista de todos los miembros de la organización, ejecuta el siguiente AWS CLI comando:

```
aws organizations list-accounts
```

Después de añadir esta cuenta como miembro, se aplicará la GuardDuty configuración de activación automática.

## (Opcional) Habilitar planes de protección para cuentas de miembro existentes

El siguiente procedimiento incluye los pasos para habilitar planes de protección para cuentas de miembro existentes mediante la página Cuentas. Para conocer los pasos para hacerlo mediante la API o AWS CLI consulte los documentos relacionados con el plan de protección específico.

Puede habilitar planes de protección para cuentas individuales a través de la página Cuentas.

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Utilice las credenciales de la cuenta GuardDuty de administrador delegado.

2. En el panel de navegación, elija Cuentas.
3. Seleccione una o más cuentas donde desee configurar un plan de protección. Repita los pasos siguientes para cada plan de protección que desee configurar:
  - a. Seleccione Editar planes de protección.
  - b. En la lista de planes de protección, elija aquel que desee configurar.
  - c. Elija una de las acciones que desee llevar a cabo para este plan de protección y, a continuación, seleccione Confirmar.
  - d. Para la cuenta seleccionada, la columna correspondiente al plan de protección configurado mostrará la configuración actualizada como Habilitado o No habilitado.

## Administre continuamente sus cuentas de miembros dentro GuardDuty

Como cuenta de GuardDuty administrador delegado, usted es responsable de mantener la configuración GuardDuty y sus planes de protección opcionales para todas las cuentas de su organización, en cada una de ellas compatibles. Región de AWS En las siguientes secciones se proporcionan las opciones para mantener el estado de configuración de cualquiera de sus planes de protección opcionales GuardDuty o de cualquiera de sus planes de protección opcionales:

Para mantener el estado de configuración de toda la organización en cada región

- Configure las preferencias de activación automática para toda la organización mediante la GuardDuty consola: puede habilitarla GuardDuty automáticamente para todos (ALL) los miembros de la organización o para los nuevos (NEW) miembros que se unan a la organización, o puede optar por no (NONE) habilitarla automáticamente para ninguno de los miembros de la organización.

También puede configurar los mismos ajustes o ajustes diferentes para cualquiera de los planes de protección incluidos. GuardDuty

Es posible que la actualización de la configuración de todas las cuentas de miembro de la organización tarde hasta 24 horas.

- Actualice las preferencias de activación automática mediante la API: ejecute [UpdateOrganizationConfiguration](#) para configurar GuardDuty automáticamente sus planes de protección opcionales para la organización. Cuando vaya [CreateMembers](#) a añadir nuevas

cuentas de miembros a tu organización, los ajustes configurados se aplicarán automáticamente. Cuando se ejecuta `CreateMembers` con una cuenta de miembro existente, la configuración de la organización también se aplicará a los miembros existentes. Esto podría cambiar la configuración actual de las cuentas de miembro existentes.

Para ver todas las cuentas de tu organización, consulta la [ListAccounts](#) referencia de la AWS Organizations API.

Para mantener el estado de configuración de las cuentas de miembro individualmente en cada región

- Para ver todas las cuentas de tu organización, consulta la [ListAccounts](#) referencia de la AWS Organizations API.
- Si desea que algunas cuentas de miembros tengan un estado de configuración diferente, ejecútelas [UpdateMemberDetectors](#) para cada cuenta de miembro de forma individual.

Puede utilizar la GuardDuty consola para realizar la misma tarea accediendo a la página de cuentas de la GuardDuty consola.

Para obtener información sobre cómo habilitar planes de protección para cuentas individuales ya sea mediante la consola o la API, consulte la página de configuración del plan de protección correspondiente.

## Suspensión GuardDuty para la cuenta de un miembro

Como cuenta de GuardDuty administrador delegado, puede suspender el GuardDuty servicio de una cuenta de miembro de su organización. Si lo hace, la cuenta de miembro seguirá perteneciendo a su GuardDuty organización. También puedes volver a activarlas GuardDuty para estas cuentas de miembros más adelante. Sin embargo, si finalmente desea desasociar (eliminar) esta cuenta de miembro, después de seguir los pasos que se indican en esta sección, deberá seguir los pasos que se indican en [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#).

Si GuardDuty suspendes una cuenta de miembro, puedes esperar los siguientes cambios:

- GuardDuty ya no supervisa la seguridad del AWS medio ambiente ni genera nuevos hallazgos.
- Los resultados existentes en la cuenta de miembro permanecen intactos.
- Una cuenta de miembro GuardDuty suspendida no conlleva ningún cargo por. GuardDuty



Si la cuenta del miembro ha activado Malware Protection for S3 en uno o varios segmentos de su cuenta, la suspensión GuardDuty no afectará a la configuración de Malware Protection for S3. La cuenta de miembro aún incurrirá en el costo de uso correspondiente a la protección contra malware para S3. Para que la cuenta de miembro deje de utilizar la protección contra malware para S3, se debe desactivar esta característica para los buckets protegidos. Para obtener más información, consulte [Desactivar la protección contra malware para S3 para un bucket protegido](#).

Elige el método que prefieras GuardDuty para suspender la cuenta de un miembro de tu organización.

## Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.
3. En la página Cuentas, selecciona una o más cuentas para las que quieras suspender GuardDuty.
4. Selecciona el menú desplegable Acciones y, a continuación, selecciona Suspender GuardDuty.
5. Selecciona Suspender GuardDuty para confirmar la selección.

Esto cambiará el Estado de la cuenta de miembro a Desactivado (suspendido).

Repita los pasos anteriores en cada región adicional en la que desee desasociar o eliminar la cuenta de miembro.

## API

1. Para recuperar el ID de la cuenta de miembro cuya suspensión deseas suspender GuardDuty, usa la [ListMembers](#) API. Incluye el parámetro `OnlyAssociated` en la solicitud. Si estableces el valor de este parámetro en `true`, GuardDuty devuelve una `members` matriz que proporciona detalles solo sobre las cuentas que son GuardDuty miembros actualmente.

Como alternativa, puedes usar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sustitúyala *us-east-1* por la región en la que deseas suspender GuardDuty esta cuenta.

2. Para suspender una o más cuentas de GuardDuty miembros, ejecuta [StopMonitoringMembers](#) la suspensión GuardDuty de una cuenta de miembro.

Como alternativa, puede AWS CLI ejecutar el siguiente comando:

```
aws guardduty stop-monitoring-members --detector-id  
12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

Sustitúyala *us-east-1* por la región en la que deseas suspender esta cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

Si además desea desasociar (eliminar) esta cuenta de miembro, siga los pasos que se indican en [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#).

## Desasociar (eliminar) la cuenta de miembro de la cuenta de administrador

Cuando desee dejar de configurar los GuardDuty ajustes y de acceder a los datos de una cuenta de miembro, elimine esa cuenta como cuenta de GuardDuty miembro. Puede hacerlo desasociando (eliminando) esa cuenta de la cuenta de GuardDuty administrador.

Al desasociar una cuenta de GuardDuty miembro, ocurre lo siguiente:

- GuardDuty permanece habilitada para la cuenta actual Región de AWS, pero la cuenta se disocia de la cuenta de administrador delegado GuardDuty .
- La cuenta desvinculada aún aparece en el inventario de cuentas.
- La cuenta de GuardDuty administrador ya no tiene acceso a los resultados de esta cuenta independiente.
- El propietario de la cuenta no recibe ninguna notificación de la desvinculación.

Puede volver a agregar la cuenta desvinculada a la organización en un momento posterior.

Elija el método que prefiera para desasociar (eliminar) una cuenta de miembro de la organización.

## Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>

Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.
3. En la tabla Cuentas, puede eliminar una cuenta que tenga Tipo como Vía Organizations y Estado como Habilitado.

Seleccione una o más cuentas que tengan el mismo Tipo y Estado.

4. En el menú desplegable Acciones, seleccione Desasociar cuenta.
5. Elija Desasociar cuenta para confirmar la opción elegida.
6. El valor de Estado de las cuentas seleccionadas cambiará a No es miembro. El recuento de Via Organizations (Active/All) que aparece en la esquina superior derecha de la página de cuentas cambiará para reflejar la actualización.

Repita los pasos descritos anteriormente en cada región adicional en la que desee desasociar la cuenta de miembro.

## API

1. Para recuperar el ID de cuenta de la cuenta de miembro que desea eliminar, utilice la API [ListMembers](#). Incluya el parámetro `OnlyAssociated` en la solicitud. Si establece el valor de este parámetro en `true`, GuardDuty devuelve una `members` matriz que proporciona detalles solo sobre las cuentas de las que actualmente son GuardDuty miembros.

Como alternativa, puedes usar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --only-associated true --region us-east-1
```

Sustitúyala *us-east-1* por la región en la que desees eliminar esta cuenta.

2. Para eliminar una o más cuentas de GuardDuty miembros, ejecute el [DisassociateMembers](#) comando para eliminar la cuenta de miembro que está asociada a la cuenta de administrador.

Como alternativa, puede AWS CLI ejecutar el siguiente comando:

```
aws guardduty disassociate-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE  
--account-ids 111122223333 --region us-east-1
```

Sustitúyala *us-east-1* por la región en la que deseas eliminar esta cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

## Eliminar las cuentas de los miembros de GuardDuty la organización

Como cuenta de GuardDuty administrador delegado, una vez que haya desasociado una cuenta de miembro y ya no desee conservar esa cuenta de miembro en la GuardDuty organización, puede eliminarla de la organización GuardDuty . Esta cuenta de miembro dejará de aparecer en el inventario de cuentas. Sin embargo, si no GuardDuty se suspendió en esta cuenta de miembro, la configuración GuardDuty y los planes de protección dedicados siguen siendo los mismos. Esta cuenta pasará a ser una cuenta independiente y podrá [GuardDutyinhabilitarse automáticamente](#).

Este paso no eliminará la cuenta de miembro de su AWS organización.

Elige el método que prefieras para eliminar una cuenta de miembro de tu GuardDuty organización.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de GuardDuty administrador delegado.

2. En el panel de navegación, elija Cuentas.
3. En la tabla Cuentas, puede eliminar una cuenta que tenga Tipo como Vía Organizations y Estado como Eliminada (desasociada).

Seleccione una o más cuentas que tengan el mismo Tipo y Estado.

4. En el menú desplegable Acciones, elija Eliminar cuenta.
5. Elija Eliminar cuentas para confirmar la opción elegida. La cuenta de miembro seleccionada ya no aparecerá en la tabla Cuentas.

Repita los pasos descritos anteriormente en cada región adicional en la que desee eliminar esta cuenta de miembro.

## API/CLI

1. Para recuperar el ID de cuenta de la cuenta de miembro que desea eliminar, utilice la API [ListMembers](#). Incluya el parámetro `OnlyAssociated` en la solicitud. Si establece el valor de este parámetro en `false`, GuardDuty devuelve una `members` matriz que proporciona detalles únicamente sobre las cuentas que actualmente son miembros GuardDuty disociados.

Como alternativa, puedes usar AWS Command Line Interface (AWS CLI) para ejecutar el siguiente comando:

```
aws guardduty list-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --only-associated="false" --region us-east-1
```

**12abc34d567e8fa901bc2d34EXAMPLE** Sustitúyalo por el ID del detector de cuentas de GuardDuty administrador delegado y **us-east-1** por la región en la que deseas eliminar esta cuenta.

2. Para eliminar una o más cuentas de GuardDuty miembros, ejecuta [DeleteMembers](#) para eliminar la cuenta de miembro de la GuardDuty organización.

Como alternativa, puede AWS CLI ejecutar el siguiente comando:

```
aws guardduty delete-members --detector-id 12abc34d567e8fa901bc2d34EXAMPLE --account-ids 111122223333 --region us-east-1
```

**12abc34d567e8fa901bc2d34EXAMPLE** Sustitúyalo por el ID del detector de cuentas de GuardDuty administrador delegado y **us-east-1** por la región en la que deseas eliminar esta cuenta. Si tiene una lista de identificadores de cuenta que desea eliminar, sepárelos con un espacio.

## Cambiar la cuenta de administrador delegado GuardDuty

Puede eliminar la cuenta de GuardDuty administrador delegado de su organización en cada región y, a continuación, delegar un nuevo administrador en cada región. Para mantener el nivel de seguridad de las cuentas de los miembros de su organización en una región, debe tener una cuenta de GuardDuty administrador delegado en esa región.

 Nota

Antes de eliminar una cuenta de GuardDuty administrador delegado, debe desasociar todas las cuentas de miembro asociadas a la cuenta de GuardDuty administrador delegado y, a continuación, eliminarlas de la organización. GuardDuty Para obtener más información sobre estos pasos, consulte los siguientes documentos:

- [Desasociar \(eliminar\) la cuenta de miembro de la cuenta de administrador](#)
- [Eliminar las cuentas de los miembros de GuardDuty la organización](#)

## Eliminar la cuenta de administrador delegado existente GuardDuty

Paso 1: Eliminar la cuenta de GuardDuty administrador delegado existente en cada región

1. Como cuenta de GuardDuty administrador delegado existente, enumere todas las cuentas de miembros asociadas a su cuenta de administrador. Ejecutar [ListMembers](#) con `OnlyAssociated=false`.
2. Si la preferencia de activación automática de alguno de los planes de protección opcionales GuardDuty o alguno de ellos está establecida en ALL, ejecute [UpdateOrganizationConfiguration](#) para actualizar la configuración de la organización a uno NEW de los dos. NONE Esta acción evitará que se produzca un error al desasociar todas las cuentas de miembro en el paso siguiente.
3. Ejecute [DisassociateMembers](#) para desasociar todas las cuentas de miembro que están asociadas a la cuenta de administrador.
4. Ejecute [DeleteMembers](#) para eliminar las asociaciones entre la cuenta de administrador y las cuentas de miembro.
5. Como cuenta de administración de la organización, ejecute [DisableOrganizationAdminAccount](#) para eliminar la cuenta de GuardDuty administrador delegado existente.
6. Repita estos pasos en cada uno de los Región de AWS lugares en los que tenga esta cuenta de GuardDuty administrador delegado.

## Paso 2: Para anular el registro de la cuenta de GuardDuty administrador delegado existente en AWS Organizations (acción global) One-time

- Ejecute [DeregisterDelegatedAdministrator](#) la referencia de la AWS Organizations API para anular el registro de la cuenta de administrador delegado GuardDuty existente en. AWS Organizations

Como alternativa, puede ejecutar el siguiente comando: AWS CLI

```
aws organizations deregister-delegated-administrator --account-id 111122223333 --  
service-principal guardduty.amazonaws.com
```

Asegúrese de **111122223333** reemplazarla por la cuenta de GuardDuty administrador delegado existente.

Tras anular el registro de la antigua cuenta de GuardDuty administrador delegado, puede añadirla como cuenta de miembro a la nueva cuenta de administrador delegado GuardDuty .

## Designar una nueva cuenta de administrador delegado GuardDuty en cada región

1. Diseñe una nueva cuenta de GuardDuty administrador delegado en cada región mediante el método de acceso que prefiera: GuardDuty consola, API o. AWS CLI Para obtener más información, consulte [Designación de una cuenta de administrador delegado GuardDuty](#).
2. Ejecute [DescribeOrganizationConfiguration](#) para ver la configuración de activación automática actual de su organización.

### Important

Antes de añadir miembros a la nueva cuenta de GuardDuty administrador delegado, debe comprobar la configuración de activación automática de su organización. Esta configuración es específica de la nueva cuenta de GuardDuty administrador delegado y de la región seleccionada, y no está relacionada con ellas. AWS Organizations Al añadir una cuenta de miembro de la organización (nueva o existente) a la nueva cuenta de GuardDuty administrador delegado, la configuración de activación automática de la nueva cuenta de GuardDuty administrador delegado se aplicará en el momento de la activación GuardDuty o en cualquiera de sus planes de protección opcionales.

Cambie la configuración organizativa de la nueva cuenta de GuardDuty administrador delegado mediante el método de acceso que prefiera: GuardDuty consola, API o. AWS CLI Para obtener más información, consulte [Configuración de las preferencias de habilitación automática de la organización](#).

## Administrar GuardDuty cuentas por invitación

Para administrar cuentas que estén fuera de la organización, puede utilizar el método de invitación heredado. Con este método, su cuenta se designa como cuenta de administrador cuando otra cuenta acepta su invitación para convertirse en cuenta de miembro.

### Note

GuardDuty recomienda utilizarlas, AWS Organizations en lugar de GuardDuty invitaciones, para gestionar sus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Si la cuenta no es de administrador, podrá aceptar una invitación de otra cuenta. Al aceptar, su cuenta se convierte en cuenta miembro. Una AWS cuenta no puede ser una cuenta de GuardDuty administrador y una cuenta de miembro al mismo tiempo.

Si acepta una invitación de una cuenta, no podrá aceptar una invitación de otra cuenta. Para aceptar una invitación de otra cuenta, primero tendrá que desasociar su cuenta de la cuenta de administrador existente. Como alternativa, la cuenta de administrador también puede desasociar la cuenta y eliminarla de su organización.

Las cuentas asociadas mediante invitación tienen una relación general de administrador y miembro similar a la de las cuentas asociadas AWS Organizations, tal como se describe en. [Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros](#) Sin embargo, los usuarios de las cuentas de administrador de invitaciones no pueden habilitar GuardDuty en nombre de las cuentas de los miembros asociadas ni ver otras cuentas que no sean miembros de su organización. AWS Organizations



 Important

Cross-regional la transferencia de datos puede producirse cuando se GuardDuty crean cuentas de miembros con este método. Para verificar las direcciones de correo electrónico de las cuentas de los miembros, GuardDuty utiliza un servicio de verificación de correo electrónico que opera solo en la región de EE. UU. Este (Virginia del Norte).

## Temas

- [Agregar cuentas por invitación](#)
- [Consolidar las cuentas de GuardDuty administrador en una sola organización](#)

## Agregar cuentas por invitación

Como cuenta de administrador que ya está GuardDuty habilitada, puedes añadir miembros para empezar a utilizarla. GuardDuty Después de añadir a los miembros, puedes invitarlos a unirse GuardDuty y ellos pueden optar por responder a tu invitación.

 Note

GuardDuty recomienda utilizarla, AWS Organizations en lugar de GuardDuty invitaciones, para gestionar sus cuentas de miembros. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Elija un método de acceso preferido para añadir cuentas de GuardDuty miembros como cuentas de GuardDuty administrador.

## Console

## Paso 1: agregación de una cuenta

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Cuentas.
3. Seleccione Agregar cuentas mediante invitación en el panel superior.

4. En la página Agregar cuentas de miembros, en Escribir los detalles de la cuenta, introduzca el ID de la Cuenta de AWS y la dirección de correo electrónico asociada a la cuenta que desea agregar.
5. Para agregar otra fila para introducir los detalles de la cuenta de uno en uno, elija Agregar otra cuenta. También puede seleccionar Cargar un archivo .csv con los detalles de la cuenta para agregar cuentas en bloque.

 Important

La primera línea del archivo .csv debe contener el encabezado, tal como se muestra en el ejemplo siguiente: Account ID,Email. Cada línea subsiguiente debe contener un único Cuenta de AWS identificador válido y su dirección de correo electrónico asociada. El formato de una fila es válido si contiene solo un ID de Cuenta de AWS y la dirección de correo electrónico asociada separados por una coma.

Account ID,Email

555555555555,user@example.com

6. Después de agregar todos los detalles de las cuentas, seleccione Siguiente. Puede ver las cuentas recién agregadas en la tabla Cuentas. El Estado de estas cuentas será Invitación no enviada. Para obtener información sobre cómo enviar una invitación a una o más cuentas agregadas, consulte [Step 2 - Invite an account](#).

## Paso 2: invitación a una cuenta

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Cuentas.
3. Seleccione una o más cuentas a las que quieras invitar a Amazon GuardDuty.
4. Seleccione el menú desplegable Acciones y, a continuación, elija Invitar.
5. En el cuadro de GuardDuty diálogo Invitación a, introduce un mensaje de invitación (opcional).

Si la cuenta invitada no tiene acceso al correo electrónico, active la casilla Enviar también una notificación por correo electrónico al usuario raíz del invitado Cuenta de AWS y generar una alerta en el nombre del invitado. Panel de AWS Health

6. Seleccione Send invitation (Enviar invitación). Si los invitados tienen acceso a la dirección de correo electrónico especificada, pueden ver la invitación abriendo la consola en GuardDuty <https://console.aws.amazon.com/guardduty/>
7. Cuando el invitado acepta la invitación, el valor de la columna Estado cambia a Invitado. Para obtener más información sobre la aceptación de una invitación, consulte [Step 3 - Accept an invitation](#).

### Paso 3: aceptación de una invitación

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>



#### Important

Debe habilitarla GuardDuty antes de poder ver o aceptar una invitación de membresía.

2. Haz lo siguiente solo si GuardDuty aún no la has activado; de lo contrario, puedes saltarte este paso y continuar con el siguiente.

Si aún no lo has activado GuardDuty, selecciona Get Started en la GuardDuty página de Amazon.

En la página Welcome to GuardDuty (Bienvenido a), elija Enable GuardDuty (Habilitar).

3. Después de activar GuardDuty tu cuenta, sigue los siguientes pasos para aceptar la invitación a ser miembro:
  - a. En el panel de navegación, seleccione Configuración.
  - b. Elija Cuentas.
  - c. En Cuentas, asegúrese de verificar el propietario de la cuenta desde la que acepta la invitación. Active Aceptar para aceptar la invitación para hacerse miembro.
4. Tras aceptar la invitación, su cuenta pasará a ser una cuenta de GuardDuty miembro. La cuenta cuyo propietario envió la invitación pasa a ser la cuenta de GuardDuty administrador. La cuenta de administrador sabrá que ha aceptado la invitación. Se actualizará la tabla de GuardDuty cuentas de su cuenta. El valor de la columna Estado correspondiente al ID de la cuenta de miembro cambiará a Habilitado. El propietario de la cuenta de administrador ahora puede ver GuardDuty y administrar las configuraciones del plan de protección en nombre

de su cuenta. La cuenta de administrador también puede ver y gestionar las GuardDuty conclusiones generadas para su cuenta de miembro.

## API/CLI

Puede designar una cuenta de GuardDuty administrador y crear o añadir cuentas de GuardDuty miembros mediante invitación a través de las operaciones de la API. Ejecute las siguientes operaciones de GuardDuty API para designar la cuenta de administrador y las cuentas de los miembros GuardDuty.

Complete el siguiente procedimiento con las credenciales de la cuenta Cuenta de AWS que desee designar como cuenta de GuardDuty administrador.

### Creación o agregación de cuentas de miembro

1. Ejecute la operación de [CreateMembers](#) API con las credenciales de la AWS cuenta que se ha GuardDuty activado. Esta es la cuenta que quieres que sea la GuardDuty cuenta de administrador.

Debe especificar el ID de detección de la AWS cuenta actual y el ID de cuenta y la dirección de correo electrónico de las cuentas de las que quiere convertirse en GuardDuty miembro. Puede crear uno o varios miembros con esta operación de API.

También puede usar las herramientas de línea de AWS comandos para designar una cuenta de administrador mediante la ejecución del siguiente comando CLI. No olvide utilizar su propio ID de detector, ID de cuenta y correo electrónico.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Se ejecuta [InviteMembers](#) con las credenciales de la AWS cuenta que se ha GuardDuty activado. Esta es la cuenta que desea que sea la GuardDuty cuenta de administrador.

Debe especificar el identificador del detector de la AWS cuenta actual y los identificadores de las cuentas de las que quiere convertirse en GuardDuty miembro. Con esta operación de la API, puede invitar a uno o varios miembros.

 Note

También puede especificar un mensaje de invitación opcional mediante el parámetro de solicitud `message`.

También puede utilizarla AWS Command Line Interface para designar las cuentas de los miembros ejecutando el siguiente comando. No olvide utilizar su propio ID de detector y unos ID válidos para las cuentas a las que desea invitar.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

```
aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --  
account-ids 111122223333
```

## Aceptación de invitaciones

Complete el siguiente procedimiento con las credenciales de cada AWS cuenta que desee designar como cuenta de GuardDuty miembro.

1. Ejecute la operación de [CreateDetector](#) API para cada AWS cuenta que haya sido invitada a convertirse en cuenta de GuardDuty miembro y para la que desee aceptar una invitación.

Debe especificar si el recurso detector se va a habilitar mediante el GuardDuty servicio. Se debe crear y habilitar un detector GuardDuty para que entre en funcionamiento. Primero debe activarlo GuardDuty antes de aceptar una invitación.

También puede hacerlo mediante las herramientas de línea de AWS comandos mediante el siguiente comando CLI.

```
aws guardduty create-detector --enable
```

2. Ejecute la operación de [AcceptAdministratorInvitation](#) API para cada AWS cuenta en la que desee aceptar la invitación de membresía, utilizando las credenciales de esa cuenta.

Debe especificar el ID de detección de esta AWS cuenta para la cuenta del miembro, el ID de cuenta de la cuenta de administrador que envió la invitación y el ID de invitación de la invitación que está aceptando. Puede consultar el ID de cuenta de la cuenta de administrador en el correo electrónico de invitación o con la operación [ListInvitations](#) de la API.

También puede aceptar una invitación mediante las herramientas de línea de AWS comandos ejecutando el siguiente comando CLI. No olvide utilizar un ID de detector, un ID de cuenta de administrador y un ID de invitación que sean válidos.

Para encontrar la `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.

```
aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
--administrator-id 444455556666 --invitation-
id 84b097800250d17d1872b34c4daadcf5
```

## Consolidar las cuentas de GuardDuty administrador en una sola organización

GuardDuty recomienda utilizar la asociación AWS Organizations para gestionar las cuentas de los miembros en una cuenta de GuardDuty administrador delegado. Puede utilizar el proceso de ejemplo que se describe a continuación para consolidar la cuenta de administrador y el miembro asociado por invitación en una organización en una única cuenta de GuardDuty administrador GuardDuty delegado.

### Note

GuardDuty recomienda utilizarla, AWS Organizations en lugar de GuardDuty invitaciones, para gestionar las cuentas de los miembros. Para obtener más información, consulte [Administración de cuentas con AWS Organizations](#).

Las cuentas que ya están siendo administradas por una cuenta de GuardDuty administrador delegado o las cuentas de miembros activos que están asociadas a una cuenta de GuardDuty administrador delegado no se pueden agregar a una cuenta de administrador delegado GuardDuty diferente. Cada organización solo puede tener una cuenta de GuardDuty administrador delegado

por región y cada cuenta de miembro solo puede tener una cuenta de administrador delegado. GuardDuty

Elija un método de acceso preferido para consolidar las cuentas de GuardDuty administrador en una única cuenta de administrador delegado. GuardDuty

## Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>

Para iniciar sesión, utilice las credenciales de la cuenta de administración de la organización.

2. Todas las cuentas que desee gestionar GuardDuty deben formar parte de su organización. Para obtener información sobre cómo agregar una cuenta a su organización, consulte [Invitar a un usuario Cuenta de AWS a unirse a su organización](#).
3. Asegúrese de que todas las cuentas de los miembros estén asociadas a la cuenta que desee designar como cuenta única de GuardDuty administrador delegado. Desasocie cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.

Los siguientes pasos le ayudarán a desasociar las cuentas de miembro de la cuenta de administrador preexistente:

- a. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>
  - b. Para iniciar sesión, utilice las credenciales de la cuenta de administrador preexistente.
  - c. En el panel de navegación, elija Cuentas.
  - d. En la página Cuentas, seleccione una o más cuentas que quiera desasociar de la cuenta de administrador.
  - e. Seleccione Acciones y, a continuación, seleccione Desasociar cuenta.
  - f. Seleccione Confirmar para finalizar el paso.
4. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

Para iniciar sesión, utilice las credenciales de la cuenta de administración.

5. En el panel de navegación, seleccione Configuración. En la página de configuración, designe la cuenta de GuardDuty administrador delegado de la organización.
6. Inicie sesión en la cuenta de GuardDuty administrador delegado designada.
7. Agregue miembros de la organización. Para obtener más información, consulte [Administrar GuardDuty cuentas con AWS Organizations](#).

## API/CLI

1. Todas las cuentas que desee gestionar GuardDuty deben formar parte de su organización. Para obtener información sobre cómo agregar una cuenta a su organización, consulte [Invitar a un usuario Cuenta de AWS a unirse a su organización](#).
2. Asegúrese de que todas las cuentas de los miembros estén asociadas a la cuenta que desee designar como cuenta única de GuardDuty administrador delegado.
  - a. Ejecute [DisassociateMembers](#) para desasociar cualquier cuenta de miembro que aún esté asociada a las cuentas de administrador preexistentes.
  - b. Como alternativa, puede ejecutar el siguiente comando y sustituirlo **777777777777** por el identificador de detección de la cuenta de administrador preexistente de la que desea desasociar la cuenta de miembro. AWS Command Line Interface **666666666666** Sustitúyalo por el Cuenta de AWS ID de la cuenta de miembro que desee desasociar.

```
aws guardduty disassociate-members --detector-id 777777777777 --account-ids 666666666666
```

3. Ejecute [EnableOrganizationAdminAccount](#) para delegar an Cuenta de AWS como cuenta de GuardDuty administrador delegado.

Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface para delegar una cuenta de GuardDuty administrador delegado:

```
aws guardduty enable-organization-admin-account --admin-account-id 777777777777
```

4. Agregue miembros de la organización. Para obtener más información, consulte [Create or add member member accounts using API](#).

 Important

Para maximizar la eficacia de un servicio regional GuardDuty, le recomendamos que designe su cuenta de GuardDuty administrador delegado y añada todas las cuentas de los miembros de cada región.



# GuardDuty consideraciones para exportar los detalles de las cuentas de los miembros en formato CSV

Como cuenta de GuardDuty administrador, puede exportar los detalles de la cuenta del miembro en formato CSV. Estos detalles incluyen el ID de la cuenta del miembro, el nombre, el tipo (agregado mediante invitación AWS Organizations o mediante invitación) y el estado de la configuración GuardDuty y los planes de protección específicos.

La opción Exportar CSV se muestra en la página de GuardDuty cuentas en función de cómo administres las cuentas de varios miembros. Al utilizar la opción Exportar CSV, podrá identificar qué cuentas de miembro tienen habilitado un plan de protección específico.

En la siguiente lista se indican los criterios para determinar si el CSV de exportación estará disponible o no en la página de GuardDuty cuentas:

- Solo se usa AWS Organizations para administrar varias cuentas de miembros y el número total de cuentas de miembros de su GuardDuty organización es de hasta 5000.
- Utiliza ambos métodos de invitación AWS Organizations y el número total de cuentas de miembros en su GuardDuty organización es de hasta 5000.

En este escenario, el CSV exportado incluirá si la cuenta de un miembro se agregó mediante un método basado en invitaciones AWS Organizations o mediante él.

- Si utiliza únicamente el método basado en invitaciones para administrar varias cuentas de miembro, no existirá la opción Exportar CSV.

# GuardDuty buscar tipos

Un hallazgo es una notificación que se GuardDuty genera cuando detecta un indicio de una actividad sospechosa o maliciosa en su parte Cuenta de AWS. GuardDuty genera un hallazgo en una cuenta que está habilitada GuardDuty.

Para obtener información sobre los cambios importantes en los tipos de GuardDuty búsqueda, incluidos los tipos de búsqueda recién agregados o retirados, consulte [Historial de documentos de Amazon GuardDuty](#).

Para obtener información sobre tipos de resultados que ya se han retirado, consulte [Tipos de resultados retirados](#).

## GuardDuty Tipos de búsqueda de EC2

Los siguientes resultados son específicos de los recursos de Amazon EC2 y siempre tendrán un tipo de recurso de Instance. La gravedad y los detalles de los resultados variarán en función del rol de recurso que indicará si la instancia de EC2 fue objeto de actividad sospechosa o el agente que llevó a cabo la actividad.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para más información sobre los orígenes de datos y modelos, consulte [GuardDuty fuentes de datos fundamentales](#).

### Notas

- Es posible que falten detalles de la instancia de resultados de EC2 si la instancia ya se terminó o si la llamada a la API subyacente se originó en una instancia de EC2 en una región diferente.
- Los resultados de EC2 que utilizan registros de flujo de VPC como origen de datos no admiten el tráfico IPv6.

Para todos los resultados de EC2, se recomienda examinar el recurso en cuestión para determinar si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar reglas de supresión o listas de IP confiables para evitar las notificaciones de falsos positivos para ese recurso.

Si la actividad es inesperada, la práctica recomendada de seguridad consiste en asumir que la instancia se ha visto afectada y llevar a cabo las acciones detalladas en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Temas

- [Backdoor:EC2/C&CActivity.B](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Tcp](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [Backdoor:EC2/DenialOfService.UdpOnTcpPorts](#)
- [Backdoor:EC2/DenialOfService.UnusualProtocol](#)
- [Backdoor:EC2/Spambot](#)
- [Behavior:EC2/NetworkPortUnusual](#)
- [Behavior:EC2/TrafficVolumeUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.B](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Custom](#)
- [Impact:EC2/PortSweep](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Impact:EC2/WinRMBruteForce](#)
- [Recon:EC2/PortProbeEMRUnprotectedPort](#)
- [Recon:EC2/PortProbeUnprotectedPort](#)
- [Recon:EC2/Portscan](#)

- [Trojan:EC2/BlackholeTraffic](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.B](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)
- [Trojan:EC2/DropPoint](#)
- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/MetadataDNSRebind](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [UnauthorizedAccess:EC2/TorClient](#)
- [UnauthorizedAccess:EC2/TorRelay](#)

## Backdoor:EC2/C&CActivity.B

Una instancia de EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que hay una instancia que aparece en la lista dentro del entorno de AWS que está consultando a una IP asociada con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por

un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

 Note

Si la IP consultada está relacionada con log4j, los campos del resultado asociado incluirán los siguientes valores:

- service.additional = Amazon Info.threatListName
- service.additional = Relacionado Info.threatName con Log4j

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/C&CActivity.B!DNS

La instancia de EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia que se muestra en la lista dentro del entorno de AWS que está consultando a un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia de la lista podría haberse visto afectada. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de

**Note**

Si el nombre de dominio consultado está relacionado con log4j, los campos del hallazgo asociado incluirán los siguientes valores:

- service.additional = Amazon Info.threatListName
- service.additional = Relacionado Info.threatName con Log4j

**Note**

Para comprobar cómo se GuardDuty genera este tipo de búsqueda, puedes realizar una solicitud de DNS desde tu instancia (`dig` para Linux o `nslookup` Windows) y compararla con un dominio de prueba. `guardduty2activityb.com`

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo DNS.

- Origen de datos: registros de flujo de VPC

---

Backdoor:EC2/DenialOfService.Dns

629

que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo DNS.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/DenialOfService.Tcp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo TCP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico TCP saliente. Esto puede indicar que la instancia se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo TCP.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/DenialOfService.Udp

Una instancia EC2 se comporta de una manera que indica que se está utilizando para realizar un ataque de denegación de servicio (DoS) mediante el protocolo UDP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente. Esto puede indicar que la instancia que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo UDP.

### Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) mediante el protocolo UDP en un puerto TCP.

Gravedad predeterminada: alta



- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico UDP saliente cuyo objetivo es un puerto que usualmente se utiliza para la comunicación mediante TCP. Esto puede indicar que la instancia que aparece en la lista se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante el protocolo UDP a un puerto TCP.

 Note

Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/DenialOfService.UnusualProtocol

Una instancia EC2 tiene un comportamiento que puede indicar que se está utilizando para llevar a cabo un ataque de denegación de servicio (DoS) utilizando un protocolo inusual.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS está generando un gran volumen de tráfico saliente mediante un tipo de protocolo inusual que no suelen utilizar las instancias de EC2 (por ejemplo, el protocolo de administración de grupos de Internet). Esto puede indicar que la instancia se ha visto afectada y que se está utilizando para llevar a cabo ataques de denegación de servicio (DoS) mediante un protocolo inusual. Este resultado solo detecta los ataques DoS contra direcciones IP enrutables públicamente, que son los objetivos principales de este tipo de ataques.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/Spambot

Una instancia de EC2 exhibe un comportamiento inusual al comunicarse con un host remoto en el puerto 25.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista dentro del entorno de AWS se está comunicando con un host remoto en el puerto 25. Este comportamiento es inusual, ya que esta instancia de EC2 no tiene un historial previo de comunicaciones en el puerto 25. El puerto 25 lo utilizan tradicionalmente los servidores de correo para las comunicaciones SMTP. Este resultado indica que la instancia EC2 es posible que se vea comprometida para su uso en el envío de spam.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Behavior:EC2/NetworkPortUnusual

Una instancia EC2 se comunica con un host remoto en un puerto de servidor inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene historial previo de comunicaciones en este puerto remoto.

 Note

Si la instancia de EC2 se ha comunicado en los puertos 389 o 1389, la gravedad del resultado asociado se modificará a Alta y los campos del resultado incluirán el siguiente valor:

- service.additional Info.context = Posible devolución de llamada de log4j

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Behavior:EC2/TrafficVolumeUnusual

Una instancia EC2 genera una cantidad inusualmente elevada de tráfico de red a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene historial previo de envío de esta cantidad de tráfico a este host remoto.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## CryptoCurrency:EC2/BitcoinTool.B

Una instancia EC2 consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## CryptoCurrency:EC2/BitcoinTool.B!DNS

Una instancia EC2 consulta un nombre de dominio asociado con la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría ser la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:EC2/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## DefenseEvasion:EC2/UnusualDNSResolver

Una instancia de Amazon EC2 se está comunicando con un solucionador de DNS público inusual.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene un historial reciente de comunicación con este solucionador de DNS público. El campo Insólito del panel de detalles de búsqueda de la GuardDuty consola puede proporcionar información sobre la resolución de DNS consultada.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## DefenseEvasion:EC2/UnusualDoHActivity

Una instancia de Amazon EC2 se comunica de manera inusual con un DNS a través de HTTPS (DoH).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de HTTPS (DoH) con este servidor DoH público. El campo Inusual de los detalles de resultado puede proporcionar información sobre el servidor de DoH consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## DefenseEvasion:EC2/UnusualDoTActivity

Una instancia de Amazon EC2 se está comunicando de manera inusual con un DNS a través de TLS (DoT).

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS se está comportando de una manera que se desvía de la referencia establecida. Esta instancia de EC2 no tiene ningún historial reciente de comunicaciones de DNS a través de TLS (DoT) con este servidor DoT público. El campo Inusual del panel de detalles de resultado puede proporcionar información sobre el servidor DoT consultado.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/AbusedDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se han utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia de Amazon EC2 que aparece en la lista puede haberse visto afectada, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/BitcoinDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que está asociado a la actividad relacionada con criptomonedas.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Bitcoin es una criptomoneda mundial y un sistema de pago digital que se puede cambiar por otras monedas, productos y servicios. Bitcoin es una recompensa por la extracción de bitcoins y es muy solicitado por los actores de amenazas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si utiliza esta instancia de EC2 para extraer o administrar criptomonedas, o esta instancia está involucrada de otra manera en la actividad de cadena de bloques, este resultado podría representar la actividad esperada para su entorno. Si este es el caso en su entorno de AWS, le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Impact:EC2/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia involucrada en la actividad de blockchain. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/MaliciousDomainRequest.Reputation

Una instancia de EC2 consulta un dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que son maliciosos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos



que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/MaliciousDomainRequest.Custom

La instancia de EC2 está consultando un dominio en una lista de entidades de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este resultado informa que la instancia de Amazon EC2 mostrada en el entorno de AWS está consultando un nombre de dominio incluido en la lista de entidades de amenazas personalizada que cargó y activó. En GuardDuty, una lista de entidades de amenaza se compone de nombres de dominio y direcciones IP maliciosos conocidos. GuardDuty genera resultados en función de la actividad asociada a la lista de entidades de amenazas cargada. Puede ver el nombre de esta lista de entidades de amenazas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/PortSweep

Una instancia de EC2 está sondeando un puerto en un gran número de direcciones IP.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este hallazgo indica que la instancia EC2 de su AWS entorno que aparece en la lista está explorando un puerto en un gran número de direcciones IP enrutables públicamente. Este tipo de actividad se suele utilizar para encontrar hosts vulnerables y explotarlos. En el panel de detalles de búsqueda de la GuardDuty consola, solo se muestra la dirección IP remota más reciente

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/SuspiciousDomainRequest.Reputation

Una instancia de EC2 consulta un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha que es malicioso. Se observaron características de este dominio que eran consistentes con las de dominios maliciosos observados anteriormente; sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Impact:EC2/WinRMBruteForce

Una instancia de EC2 está realizando un ataque de fuerza bruta saliente con Windows Remote Management.

Gravedad predeterminada: baja\*

### Note

La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que la instancia de EC2 incluida en su AWS entorno está realizando un ataque de fuerza bruta de Administración remota de Windows (WinRM) destinado a obtener acceso al servicio de Administración remota de Windows en los sistemas. Windows-based

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Recon:EC2/PortProbeEMRUnprotectedPort

Una instancia de EC2 tiene un puerto relacionado con EMR desprotegido sondeado por un host malicioso conocido.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que un puerto confidencial relacionado con el EMR de la instancia EC2 de la lista que forma parte de un clúster de su AWS entorno no está bloqueado por un grupo de seguridad, una lista de control de acceso (ACL) o un firewall del host, como IPTables de Linux.

Además, este resultado informa de que analizadores conocidos en Internet sondean activamente este puerto. Los puertos que pueden desencadenar este resultado, como el puerto 8088 (puerto de IU web de YARN), se pueden utilizar potencialmente para la ejecución de código remoto.

Recomendaciones de corrección:

Debería bloquear el acceso libre a los puertos en los clústeres desde Internet y restringir el acceso solo a direcciones IP específicas que requieren acceso a estos puertos. Para obtener más información, consulte [Grupos de seguridad para clústeres de EMR](#).

## Recon:EC2/PortProbeUnprotectedPort

Una instancia EC2 tiene un puerto sin protección que un host malintencionado conocido está sondeando.

Gravedad predeterminada: baja\*

### Note

La gravedad predeterminada de este resultado es Baja. Sin embargo, si el puerto sondeado es utilizado por Elasticsearch (9200 o 9300), la gravedad del resultado es Alta.

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que un puerto en la instancia de EC2 que aparece en la lista del entorno de AWS no está bloqueado por un grupo de seguridad, una lista de control de acceso (ACL) o un firewall del host (por ejemplo, IPTables) y está siendo sondeado activamente por análisis conocidos en Internet.

Si el puerto desprotegido identificado es 22 o 3389 y utiliza estos puertos para conectarse a la instancia, aún puede limitar la exposición permitiendo el acceso a estos puertos solo a las direcciones IP desde el espacio de direcciones IP de la red corporativa. Para restringir el acceso al puerto 22 en Linux, consulte [Autorización del tráfico de entrada para sus instancias de Linux](#). Para restringir el acceso al puerto 3389 en Windows, consulte [Autorización del tráfico de entrada para sus instancias de Windows](#).

GuardDuty no genera este hallazgo para los puertos 443 y 80.

Recomendaciones de corrección:

Puede haber casos en los que las instancias se expongan de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso en su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de Recon:EC2/PortProbeUnprotectedPort. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Recon:EC2/Portscan

Una instancia EC2 realiza exploraciones de puertos salientes a un host remoto.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está involucrada en un posible ataque de análisis de puertos porque está intentando conectarse a varios puertos en un período corto de tiempo. El objetivo de un ataque de análisis de puertos es localizar puertos abiertos para detectar los servicios que está ejecutando el equipo e identificar su sistema operativo.

Recomendaciones de corrección:

Este resultado puede ser un falso positivo cuando se implementan aplicaciones de evaluación de vulnerabilidades en instancias de EC2 en su entorno, ya que estas aplicaciones analizan los puertos para alertarle sobre puertos abiertos mal configurados. Si este es el caso en su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de Recon:EC2/Portscan. El segundo criterio de filtro debe coincidir con la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad es inesperada, puede que su instancia esté comprometida; consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/BlackholeTraffic

Una instancia EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este hallazgo indica que la instancia EC2 de su AWS entorno que aparece en la lista podría estar comprometida porque está intentando comunicarse con la dirección IP de un agujero negro (o sumidero). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/BlackholeTraffic!DNS

Una instancia EC2 consulta un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este hallazgo indica que la instancia EC2 de su AWS entorno que aparece en la lista podría estar comprometida porque está consultando un nombre de dominio que se está redirigiendo a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DGADomainRequest.B

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). Su instancia EC2 podría estar en peligro.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

### Note

Este resultado se basa en el análisis de nombres de dominio mediante heurística avanzada, por lo que podría identificar nuevos dominios de DGA que no están presentes en fuentes de información de amenazas.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DGADomainRequest.C!DNS

Una instancia EC2 consulta dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar una instancia EC2 comprometida.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está intentando hacer consultas en dominios de algoritmos de generación de dominios (DGA). Su instancia EC2 podría estar en peligro.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

### Note

Esta conclusión se basa en los dominios de DGA conocidos de las fuentes de inteligencia sobre amenazas GuardDuty de las que dispone.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DNSDataExfiltration

Una instancia EC2 sustrae datos a través de consultas de DNS.

Gravedad predeterminada: alta



- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de EC2 que aparece en la lista del entorno de AWS está ejecutando malware que utiliza consultas de DNS para transferencias de datos salientes. Este tipo de transferencia de datos indica que se trata de una instancia afectada y podría provocar la exfiltración de datos. Por lo general, el tráfico de DNS no está bloqueado por los firewalls. Por ejemplo, el malware de una instancia de EC2 comprometida puede codificar datos (como el número de la tarjeta de crédito) en una consulta de DNS y enviarlos a un servidor DNS remoto controlado por un atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DriveBySourceTraffic!DNS

Una instancia EC2 consulta el nombre de dominio de un host remoto que es una fuente conocida de ataques de Drive-By descarga.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que la instancia de Amazon EC2 que aparece en la lista dentro del entorno de AWS podría haberse visto afectada, ya que está consultando un nombre de dominio de un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no deseadas de software informático desde Internet que pueden desencadenar la instalación automática de un virus, spyware o malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DropPoint

Una instancia EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno está intentando comunicarse con una dirección IP de un host remoto que se sabe que contiene credenciales y otros datos robados capturados por el malware.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/DropPoint!DNS

Una instancia EC2 está consultando un nombre de dominio de un host remoto que se conoce que mantiene credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Origen de datos: registros de DNS

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno está consultando el nombre de dominio de un host remoto del que se sabe que contiene credenciales y otros datos robados capturados por software malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Trojan:EC2/PhishingDomainRequest!DNS

Una instancia EC2 consulta dominios implicados en ataques de phishing. Su instancia EC2 podría estar en peligro.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este resultado le informa de que hay una instancia de EC2 en el entorno de AWS que está intentando hacer consultas a un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia de EC2 esté intentando recuperar información confidencial almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. Su instancia EC2 podría estar en peligro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Una instancia de EC2 establece conexiones con una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: media

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno se está comunicando con una dirección IP incluida en una lista de amenazas que ha subido. En GuardDuty, una lista de amenazas consta de direcciones IP malintencionadas. GuardDuty genera resultados en función de las listas de amenazas cargadas. La lista de amenazas utilizada para generar este resultado se mostrará en los detalles del resultado.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## UnauthorizedAccess:EC2/MetadataDNSRebind

Una instancia de EC2 está haciendo búsquedas de DNS que se resuelven en el servicio de metadatos de la instancia.

Gravedad predeterminada: alta

- Origen de datos: registros de DNS

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno está consultando un dominio que se resuelve en la dirección IP de los metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

## Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, debe corregir la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, debe bloquear el dominio o impedir que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe [revocar la sesión asociada a la instancia de EC2](#).

Algunos AWS clientes asignan intencionadamente la dirección IP de los metadatos a un nombre de dominio de sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de UnauthorizedAccess:EC2/MetaDataDNSRebind. El segundo criterio de filtro debe ser Dominio de la solicitud DNS y el valor debe coincidir con el dominio que ha mapeado a la dirección IP de metadatos (169.254.169.254). Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

## UnauthorizedAccess:EC2/RDPBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta RDP.

Gravedad predeterminada: baja\*

### Note

La gravedad de este resultado es baja si su instancia de EC2 era el objetivo de un ataque de fuerza bruta. La gravedad de este resultado es alta si su instancia de EC2 es el actor que se utiliza para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno sufrió un ataque de fuerza bruta destinado a obtener contraseñas para los servicios RDP de los sistemas. Windows-based Esto puede significar un acceso no autorizado a los recursos de AWS .

Recomendaciones de corrección:

Si el Rol de recurso de su instancia es ACTOR, indica que su instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a RDP. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como Target, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

Si el Rol de recurso de su instancia es TARGET, este resultado puede corregirse mediante la delegación de la protección de su puerto RDP solo a direcciones IP de confianza a través de grupos

de seguridad, ACL o firewalls. Para obtener más información, consulte [Tips for securing your EC2 instances \(Linux\)](#).

## UnauthorizedAccess:EC2/SSHBruteForce

Una instancia EC2 se ve implicada en ataques de fuerza bruta SSH.

Gravedad predeterminada: baja\*

### Note

La gravedad de este resultado es baja si se dirige un ataque de fuerza a una de las instancias de EC2. La gravedad de este resultado es alta si la instancia de EC2 se está utilizando para llevar a cabo el ataque de fuerza bruta.

- Origen de datos: registros de flujo de VPC

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno sufrió un ataque de fuerza bruta destinado a obtener contraseñas para los servicios SSH de los sistemas. Linux-based Esto puede significar un acceso no autorizado a los recursos de AWS .

### Note

Este resultado solo se genera mediante el monitoreo del tráfico en el puerto 22 por parte de . Si los servicios de SSH están configurados para usar otros puertos, no se genera este resultado.

Recomendaciones de corrección:

Si el objetivo del intento de fuerza bruta es un host bastión, esto puede representar el comportamiento esperado de su entorno. AWS Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las

instancias que alojan estas herramientas. Para más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

Si esta actividad no se espera en su entorno y el Rol de recurso de su instancia es TARGET, este resultado puede corregirse mediante la delegación de la protección de su puerto SSH solo a direcciones IP de confianza a través de grupos de seguridad, ACL o firewalls. Para obtener más información, consulte [Tips for securing your EC2 instances \(Linux\)](#).

Si el Rol de recurso de su instancia es ACTOR, indica que la instancia se ha utilizado para llevar a cabo ataques de fuerza bruta a SSH. A no ser que esta instancia tenga un motivo legítimo para contactar con la dirección IP mostrada en la lista como Target, se recomienda que asuma que su instancia se ha visto afectada y lleve a cabo las acciones que aparecen en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## UnauthorizedAccess:EC2/TorClient

La instancia EC2 está estableciendo conexiones con un guardia Tor o un nodo Authority.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este hallazgo indica que una instancia de EC2 de su AWS entorno está realizando conexiones a un nodo de Tor Guard o de Authority. Tor es un software que permite la comunicación anónima. Los nodos Guard y Authority de Tor actúan como puertas de enlace a una red de Tor. Este tráfico puede indicar que esta instancia de EC2 se ha visto afectada y está actuando como cliente en una red de Tor. Este hallazgo puede indicar un acceso no autorizado a tus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## UnauthorizedAccess:EC2/TorRelay

La instancia EC2 establece conexiones a una red Tor como repetidor Tor.

Gravedad predeterminada: alta

- Origen de datos: registros de flujo de VPC

Este hallazgo indica que una instancia de EC2 de su AWS entorno está realizando conexiones a una red Tor de una manera que sugiere que actúa como un repetidor de Tor. Tor es un software que permite la comunicación anónima. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## GuardDuty Tipos de búsqueda de IAM

Los siguientes resultados son específicos de las entidades y claves de acceso de IAM y siempre tendrán un Tipo de recurso de AccessKey. La gravedad y los detalles de los resultados varían en función del tipo de resultado.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información, consulte [GuardDuty fuentes de datos fundamentales](#).

Para cualquier información IAM-related , le recomendamos que examine la entidad en cuestión y se asegure de que sus permisos siguen la práctica recomendada de mínimo privilegio. Si la actividad es inesperada, las credenciales pueden verse afectadas. Para obtener más información sobre los resultados de corrección, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

Temas

- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/CompromisedCredentials](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)



- [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)
- [Discovery:IAMUser/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [PenTest:IAMUser/KaliLinux](#)
- [PenTest:IAMUser/ParrotLinux](#)
- [PenTest:IAMUser/PentoolLinux](#)
- [Persistence:IAMUser/AnomalousBehavior](#)
- [Policy:IAMUser/RootCredentialUsage](#)
- [Policy:IAMUser/ShortTermRootCredentialUsage](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Recon:IAMUser/MaliciousIPCaller](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)

## CredentialAccess:IAMUser/AnomalousBehavior

Una API utilizada para acceder a un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una sola solicitud de API o una serie de solicitudes de API relacionadas que haya hecho en proximidad una sola [identidad de usuario](#). La API observada suele asociarse a la fase de acceso a las credenciales en un ataque, donde un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su entorno. Las API de esta categoría son GetPasswordData, GetSecretValue, BatchGetSecretValue y GenerateDbAuthToken.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## CredentialAccess:IAMUser/CompromisedCredentials

La inteligencia de amenazas de Amazon identificó una clave de acceso de IAM como potencialmente comprometida.

Gravedad predeterminada: alta

- Característica: incluida en la protección fundamental de las fuentes de datos

Descripción completa:

Este hallazgo le informa de que la inteligencia de amenazas de Amazon ha identificado una clave de acceso de IAM asociada a su AWS cuenta como potencialmente comprometida. A continuación, la credencial comprometida se utilizó para invocar las operaciones de la API en su entorno. AWS La lista de llamadas a la API realizadas con la credencial comprometida, junto con el recuento y las marcas temporales de cada llamada, la clave de acceso implicada y la dirección IP de origen, se incluyen en los detalles del resultado.

La inteligencia de amenazas de Amazon identifica el compromiso de credenciales en este hallazgo. AWS monitorea las credenciales potencialmente comprometidas a través de los patrones de uso y genera esta información cuando se observa que se está utilizando una credencial de este tipo.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## DefenseEvasion:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API utilizada para evadir las medidas defensivas.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus rastros para evitar ser detectado. Las API de esta categoría suelen eliminar, deshabilitar o detener operaciones, como DeleteFlowLogs, DisableAlarmActions o StopLogging.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## DefenseEvasion:IAMUser/BedrockLoggingDisabled

Se ha desactivado el registro para Amazon Bedrock.

Gravedad predeterminada: media

- Fuente de datos: eventos de gestión CloudTrail

Este resultado informa de que el registro se ha desactivado para las invocaciones del modelo de Bedrock en la cuenta. Puede tratarse de un intento de un atacante de ocultar actividades maliciosas, como la exfiltración de datos o el abuso de modelos de IA. Al desactivar el registro, se elimina la visibilidad de los datos que se envían a los modelos y de cómo se utilizan los modelos.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Discovery:IAMUser/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para detectar recursos.

Gravedad predeterminada: baja

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a la fase de descubrimiento de un ataque, cuando un adversario recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Las API de esta categoría suelen obtener, describir o enumerar operaciones, como DescribeInstances, GetRolePolicy o ListAccessKeys.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la

solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Exfiltration:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para recopilar datos de un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: alta

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red mediante el empaquetado y el cifrado para evitar ser detectado. Las API para este tipo de resultado son únicamente operaciones de administración (plano de control) y, por lo general, están relacionadas con S3, instantáneas y bases de datos, como PutBucketReplication, CreateSnapshot o RestoreDBInstanceFromDBSnapshot.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Impact:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para manipular datos o procesos en un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: alta

- Fuente de datos: evento de gestión CloudTrail

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta interrumpir las operaciones y manipular, interrumpir o destruir los datos de la cuenta. Las API para este tipo de resultado suelen eliminar, actualizar o preparar operaciones, como DeleteSecurityGroup, UpdateUser o PutBucketPolicy.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## InitialAccess:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para obtener acceso no autorizado a un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a la fase de acceso inicial de un ataque, cuando un adversario intenta establecer acceso a su entorno. Las API de esta categoría suelen obtener operaciones de token o de sesión, como `StartSession` o `GetAuthorizationToken`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PenTest:IAMUser/KaliLinux

Se invocó una API desde una máquina Kali Linux.

Gravedad predeterminada: media

- Fuente de datos: evento de gestión CloudTrail

Este hallazgo le informa de que una máquina que ejecuta Kali Linux realiza llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PenTest:IAMUser/ParrotLinux

Se ha invocado una API desde una máquina Parrot Security Linux.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de administración

Este hallazgo le informa de que un equipo que ejecuta Parrot Security Linux realiza llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PenTest:IAMUser/PentooLinux

Se ha invocado una API desde una máquina Pentoo Linux.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de administración

Este hallazgo le informa de que una máquina que ejecuta Pentoo Linux está realizando llamadas a la API con credenciales que pertenecen a la AWS cuenta indicada en su entorno. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).



## Persistence:IAMUser/AnomalousBehavior

Se invocó de forma anómala una API que se utiliza habitualmente para mantener el acceso no autorizado a un AWS entorno.

Gravedad predeterminada: media

- Fuente de datos: evento CloudTrail de gestión

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder a su entorno e intenta conservar ese acceso. Las API de esta categoría suelen crear, importar o modificar operaciones, como `CreateAccessKey`, `ImportKeyPair` o `ModifyInstanceAttribute`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Policy:IAMUser/RootCredentialUsage

Se ha invocado una API mediante credenciales de inicio de sesión del usuario raíz.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de administración o eventos de CloudTrail datos para S3

Este resultado le informa de que las credenciales de inicio de sesión del usuario raíz de la Cuenta de AWS que aparece en la lista de su entorno se están utilizando para hacer solicitudes a los servicios

de AWS . Se recomienda que los usuarios nunca utilicen las credenciales de inicio de sesión del usuario raíz para acceder a AWS los servicios. En su lugar, se debe acceder a los AWS servicios con credenciales temporales con privilegios mínimos de AWS Security Token Service (STS). En los casos donde no se admite AWS STS , se recomienda utilizar las credenciales de usuario de IAM. Para obtener más información, consulte las [prácticas recomendadas de IAM](#).

 Note

Si la protección para S3 está habilitada para la cuenta, este resultado se puede generar en respuesta a los intentos de ejecutar operaciones de plano de datos de S3 en recursos de Amazon S3 con credenciales de inicio de sesión de usuario raíz de la Cuenta de AWS. La llamada a la API utilizada aparecerá en los detalles de búsqueda. Si la S3 Protection no está habilitada, este resultado solo se puede activar mediante las API de registro de eventos. Para obtener más información sobre la protección para S3, consulte [S3 Protection](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Policy:IAMUser/ShortTermRootCredentialUsage

Se ha invocado una API mediante el uso de credenciales de usuario raíz restringidas.

Gravedad predeterminada: baja

- Fuente de datos: eventos AWS CloudTrail de administración o eventos de AWS CloudTrail datos para S3

Este hallazgo le informa de que las credenciales de usuario restringidas creadas para los que figuran Cuenta de AWS en su entorno se utilizan para realizar solicitudes a Servicios de AWS. Se recomienda que utilice sus credenciales de usuario raíz únicamente para realizar [tareas que requieran credenciales de usuario raíz](#).

Cuando sea posible, acceda a ellos Servicios de AWS utilizando las funciones de IAM con privilegios mínimos con credenciales temporales de AWS Security Token Service (AWS STS). En los casos en los AWS STS que no se admite, la mejor práctica es utilizar las credenciales de usuario de

IAM. Para más información, consulte [Prácticas recomendadas de seguridad en IAM](#) y las [Prácticas recomendadas de usuario raíz para su Cuenta de AWS](#) en la Guía de usuario de IAM.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PrivilegeEscalation:IAMUser/AnomalousBehavior

Una API que se utiliza habitualmente para obtener permisos de alto nivel para un AWS entorno se invocó de forma anómala.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este hallazgo le informa de que se ha observado una solicitud de API anómala en su cuenta. Este resultado puede incluir una única API o una serie de solicitudes de API relacionadas realizadas en proximidad por una sola [identidad de usuario](#). La API observada suele asociarse a tácticas de derivación de privilegios, en las que un adversario intenta obtener permisos de nivel superior para acceder a un entorno. Las API de esta categoría suelen implicar operaciones que cambian las políticas, los roles y los usuarios de IAM, como `AssociateIamInstanceProfile`, `AddUserToGroup` o `PutUserPolicy`.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta solicitud de API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML hace un seguimiento de varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó. Los detalles sobre qué factores de la solicitud de API son inusuales para la identidad de usuario que ha invocado la solicitud se encuentran en los [detalles del resultado](#).

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos de gestión CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS se ha invocado desde una dirección IP que aparece en una lista de amenazas. Un atacante puede utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos de gestión CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS en una cuenta dentro de su entorno se ha invocado desde una dirección IP que aparece en una lista de amenazas personalizada. La lista de amenazas utilizada se mostrará en los detalles del resultado. Un atacante podría utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos de administración CloudTrail

Este resultado le informa de que una operación de API que puede enumerar o describir los recursos de AWS de una cuenta dentro de su entorno se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Un atacante utilizaría Tor para ocultar su verdadera identidad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail el registro estaba deshabilitado.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de administración

Este hallazgo le informa de que se ha desactivado un CloudTrail sendero de su AWS entorno. Puede tratarse del intento por parte de un atacante de desactivar el registro para cubrir sus rastros mediante la eliminación de cualquier indicio de su actividad y, a su vez, la obtención de acceso a los recursos de AWS con fines maliciosos. Este resultado se puede desencadenar mediante una eliminación o actualización correcta de un registro de seguimiento. Este hallazgo también se puede provocar si se elimina correctamente un depósito de S3 que almacena los registros de un rastro al que está asociado GuardDuty.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Stealth:IAMUser/PasswordPolicyChange

La política de contraseñas de la cuenta se ha debilitado.

Gravedad predeterminada: baja\*

### Note

La gravedad de este resultado puede ser baja, media o alta, según la gravedad de los cambios hechos en la política de contraseñas.

- Fuente de datos: eventos CloudTrail de administración

La política de contraseñas de AWS cuentas se ha debilitado en la cuenta incluida en la lista de su AWS entorno. Por ejemplo, se ha eliminado o actualizado para exigir menos caracteres, no requerir símbolos y números, o se ha requerido la ampliación del periodo de vencimiento de la contraseña. Este descubrimiento también puede deberse a un intento de actualizar o eliminar la política de contraseñas de su AWS cuenta. La política de contraseñas de las AWS cuentas define las reglas que rigen los tipos de contraseñas que se pueden configurar para los usuarios de IAM. Una política de contraseñas más débil permite la creación de contraseñas que son fáciles de recordar y potencialmente más fáciles de adivinar, y que suponen un riesgo para la seguridad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Se han observado varios inicios de sesión correctos en la consola desde distintos lugares del mundo.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que se han observado varios inicios de sesión correctos en la consola para el mismo usuario de IAM aproximadamente al mismo tiempo en diversas ubicaciones

geográficas. Estos patrones de ubicación de acceso anómalos y riesgosos indican un posible acceso no autorizado a sus AWS recursos.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

Se están utilizando las credenciales creadas exclusivamente para una instancia de EC2 a través de un rol de lanzamiento de instancias desde otra cuenta dentro de AWS.

Gravedad predeterminada: alta\*

### Note

La gravedad predeterminada de este resultado es alta. Sin embargo, si la API la ha invocado una cuenta afiliada a su AWS entorno, la gravedad es media.

- Fuente de datos: eventos CloudTrail de administración o eventos de CloudTrail datos para S3

Este resultado informa de cuándo se utilizan las credenciales de la instancia de Amazon EC2 para invocar API desde una dirección IP o un punto de conexión de Amazon VPC que pertenece a una cuenta de AWS diferente de aquella en la que se ejecuta la instancia de Amazon EC2 asociada. La detección de puntos de conexión de VPC solo está disponible para los servicios que admiten eventos de actividad de red para puntos de conexión de VPC. Para obtener información sobre los servicios que admiten eventos de actividad de red para puntos de conexión de VPC, consulte [Registro de eventos de actividad de red](#) en la Guía del usuario de AWS CloudTrail .

AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, AWS aplicaciones, Amazon EC2 o). AWS Lambda Sin embargo, los usuarios autorizados pueden exportar credenciales desde las instancias de Amazon EC2 para realizar llamadas a la API legítimas. Si el campo `remoteAccountDetails.Affiliated` es `True`, se ha invocado la API desde una cuenta asociada a la misma cuenta de administrador. Para descartar un posible ataque y comprobar la legitimidad de la actividad, póngase en contacto con el Cuenta de AWS propietario o el director de IAM al que están asignadas estas credenciales.

 Note

Si GuardDuty observa una actividad continua desde una cuenta remota, su modelo de aprendizaje automático (ML) identificará este comportamiento como esperado. Por lo tanto, GuardDuty dejará de generar este resultado para la actividad de esa cuenta remota. GuardDuty seguirá recopilando información sobre el nuevo comportamiento de otras cuentas remotas y volverá a evaluar las cuentas remotas detectadas a medida que el comportamiento vaya cambiando con el tiempo.

## Recomendaciones de corrección:

Este hallazgo se genera cuando las solicitudes de AWS API se realizan internamente AWS a través de una instancia de Amazon EC2 ajena a la suya Cuenta de AWS, utilizando las credenciales de sesión de su instancia de Amazon EC2. Puede ser habitual, como en la arquitectura Transit Gateway en una configuración de [concentrador y radio](#), enrutar el tráfico a través de una única VPC de salida de hub AWS con puntos de conexión de servicio. Si se espera este comportamiento, le GuardDuty recomienda usar [Reglas de supresión](#) y crear una regla con un criterio de dos filtros. El primer criterio es el tipo de resultado, que en este caso es UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. El segundo criterio de filtrado es el ID de cuenta remota de los detalles de la cuenta remota.

En respuesta a este resultado, puede utilizar el siguiente flujo de trabajo para determinar el curso de acción:

1. Identifique la cuenta remota implicada en el campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Determine si esa cuenta está afiliada a su GuardDuty entorno desde el `service.action.awsApiCallAction.remoteAccountDetails.affiliated terreno`.
3. Si la cuenta está afiliada, contacte al propietario de la cuenta remota y al propietario de las credenciales de la instancia de Amazon EC2 para investigar.

Si la cuenta no está afiliada, el primer paso es evaluar si esa cuenta está asociada a su organización, pero no forma parte del entorno de GuardDuty cuentas múltiples configurado o si aún no se GuardDuty ha activado en esta cuenta. A continuación, contacte al propietario de las credenciales de la instancia de Amazon EC2 para determinar si existe un caso de uso que amerite que una cuenta remota utilice estas credenciales.



4. Si el propietario de las credenciales no reconoce la cuenta remota, es posible que un actor de amenazas que opere dentro de AWS haya puesto en peligro las credenciales. Debe seguir los pasos que se recomiendan en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#) para proteger el entorno.

Además, puedes [enviar una denuncia de uso indebido](#) al equipo de AWS Confianza y Seguridad para iniciar una investigación sobre la cuenta remota. Al enviar el informe al equipo de Seguridad y confianza de AWS, incluya todos los detalles del resultado en JSON.

## UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

Las credenciales creadas exclusivamente para una instancia EC2 a través de un rol de lanzamiento de instancias se utilizan desde una dirección IP externa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de administración o eventos de CloudTrail datos para S3

Este hallazgo le informa de que un host externo AWS ha intentado ejecutar operaciones de AWS API con AWS credenciales temporales que se crearon en una instancia de EC2 de su AWS entorno. Es posible que la instancia de EC2 que aparece en la lista esté comprometida y que las credenciales temporales de esta instancia se hayan transferido a un host remoto externo. AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, AWS aplicaciones, EC2 o Lambda). Sin embargo, los usuarios autorizados pueden exportar credenciales desde sus instancias de EC2 para realizar llamadas a la API legítimas. Para descartar un posible ataque y verificar la legitimidad de la actividad, valide si se espera el uso de credenciales de instancia por parte de la IP remota en el resultado.

### Note

Si GuardDuty observa la actividad continua de un host remoto, su modelo de aprendizaje automático (ML) identificará este comportamiento como esperado. Por lo tanto, GuardDuty dejará de generar este hallazgo para la actividad de ese host remoto. GuardDuty seguirá recopilando información sobre el nuevo comportamiento de otros hosts remotos y volverá a evaluar los hosts remotos aprendidos a medida que el comportamiento vaya cambiando con el paso del tiempo.

## Recomendaciones de corrección:

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de [AWS Outposts](#) o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si se trata de un comportamiento esperado, se recomienda utilizar reglas de supresión y crear una regla que conste de dos criterios de filtrado. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión en GuardDuty](#).

### Note

Si GuardDuty observa la actividad continua de una fuente externa, su modelo de aprendizaje automático identificará este comportamiento como esperado y dejará de generar este resultado para la actividad de esa fuente. GuardDuty seguirá recabando información sobre nuevos comportamientos a partir de otras fuentes y reevaluará las fuentes aprendidas a medida que el comportamiento vaya cambiando con el paso del tiempo.

Si esta actividad es inesperada sus credenciales pueden verse comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/MaliciousIPCaller

Se ha invocado una API desde una dirección IP malintencionada conocida.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS ) se ha invocado desde una dirección IP maliciosa conocida. Esto puede indicar un acceso no autorizado a AWS los recursos de su entorno.

## Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Se ha invocado una API desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este hallazgo indica que se ha invocado una operación de API (por ejemplo, un intento de lanzar una instancia EC2, crear un nuevo usuario de IAM o modificar AWS los privilegios) desde una dirección IP incluida en una lista de amenazas que usted ha subido. En GuardDuty, una lista de amenazas consta de direcciones IP maliciosas conocidas. Esto puede indicar un acceso no autorizado a AWS los recursos de su entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS

Las credenciales que se crearon exclusivamente para un AWS Lambda recurso se utilizan desde una dirección IP externa a AWS.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de administración o eventos de CloudTrail datos para S3

Este hallazgo le informa de que un host externo AWS intentó ejecutar operaciones de AWS API con AWS credenciales temporales que se crearon en un AWS Lambda recurso de su AWS entorno. Es posible que el recurso de Lambda indicado esté comprometido y que las credenciales temporales de esta Lambda se hayan filtrado a un host remoto externo. AWS

AWS no recomienda redistribuir las credenciales temporales fuera de la entidad que las creó (por ejemplo, AWS aplicaciones como Amazon Elastic Compute Cloud (Amazon EC2), o). AWS Lambda

Sin embargo, los usuarios autorizados pueden exportar credenciales desde sus recursos de Lambda para realizar llamadas a la API legítimas. Para descartar un posible ataque y verificar la legitimidad de la actividad, valide si se espera el uso de credenciales de instancia por parte de la IP remota en el resultado.

 Note

Si GuardDuty observa una actividad continua desde un host remoto, su modelo de aprendizaje automático (ML) identificará este comportamiento como esperado. Por lo tanto, GuardDuty dejará de generar este hallazgo para la actividad de ese host remoto. GuardDuty seguirá recopilando información sobre el nuevo comportamiento de otros hosts remotos y volverá a evaluar los hosts remotos aprendidos a medida que el comportamiento vaya cambiando con el paso del tiempo.

#### Recomendaciones de corrección:

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de [AWS Outposts](#) o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si este es el comportamiento esperado, se recomienda usarlo [Reglas de supresión](#) para crear una regla con un criterio de dos filtros. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS`. El segundo requisito de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR para la puerta de enlace de Internet en las instalaciones.

Si esta actividad es inesperada, las credenciales pueden haberse visto afectadas. Para obtener información sobre los pasos para corregir este tipo de hallazgo, consulte [Corregir las credenciales potencialmente comprometidas AWS](#)

## UnauthorizedAccess:IAMUser/TorIPCaller

Se ha invocado una API desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de administración

Este resultado le informa de que una operación de la API (por ejemplo, un intento de lanzar una instancia de EC2, crear un nuevo usuario de IAM o modificar los privilegios de AWS ) se ha invocado desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de AWS con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## GuardDuty tipos de búsqueda de secuencias de ataques

GuardDuty detecta una secuencia de ataque cuando una secuencia específica de múltiples acciones se alinea con una actividad potencialmente sospechosa. Una secuencia de ataque incluye señales como las actividades y los GuardDuty hallazgos de la API. Cuando GuardDuty observa un grupo de señales en una secuencia específica que indican una amenaza a la seguridad en curso, en curso o reciente, GuardDuty genera una detección de la secuencia de ataque. GuardDuty considera que las actividades individuales de la API se deben [weak signals](#) a que no representan una amenaza potencial.

Las detecciones de secuencias de ataques se centran en la posibilidad de comprometer los datos de Amazon S3 (que pueden formar parte de un ataque de ransomware más amplio), AWS las credenciales comprometidas, los clústeres de Amazon EKS comprometidos, los clústeres de Amazon ECS comprometidos y los grupos de instancias de Amazon EC2 comprometidos. En las siguientes secciones, se proporciona información sobre cada una de las secuencias de ataque.

### Temas

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:ECS/CompromisedCluster](#)
- [AttackSequence:EC2/CompromisedInstanceGroup](#)
- [AttackSequence:IAM/CompromisedCredentials](#)
- [AttackSequence:S3/CompromisedData](#)

## AttackSequence:EKS/CompromisedCluster

Secuencia de acciones sospechosas realizadas por un clúster Amazon EKS potencialmente comprometido.

- Gravedad predeterminada: crítica
- Orígenes de datos:
  - [Eventos de registro de auditoría de EKS](#)
  - [Runtime Monitoring de Amazon EKS](#)
  - [Detección de malware de Amazon EKS para Amazon EC2](#)
  - [AWS CloudTrail eventos de datos para S3](#)
  - [AWS CloudTrail eventos de gestión](#)
  - [Logs de flujo de VPC](#)
  - [Registros de consultas de DNS de Route53 Resolver](#)

Este hallazgo le informa de que GuardDuty ha detectado una secuencia de acciones sospechosas que indican un clúster de Amazon EKS potencialmente comprometido en su entorno. Se observaron varios comportamientos de ataque sospechosos y anómalos, como procesos maliciosos o conexiones con puntos de conexión maliciosos, en el mismo clúster de Amazon EKS.

GuardDuty utiliza sus algoritmos de correlación patentados para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. GuardDuty evalúa los resultados de los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar las amenazas, como la reputación de la IP, las secuencias de API, la configuración de los usuarios y los recursos potencialmente afectados.

Medidas correctivas: si este comportamiento es inesperado en su entorno, es posible que su clúster de Amazon EKS esté en peligro. Para obtener una guía completa de correcciones, consulte [Corregir los resultados de EKS Protection](#) y [Corregir los resultados de la Supervisión en tiempo de ejecución](#)

Además, dado que es posible que AWS las credenciales se hayan visto comprometidas a través del clúster de EKS, consulte [Corregir las credenciales potencialmente comprometidas AWS](#). Para ver los pasos a seguir para corregir otros recursos que podrían haberse visto afectados, consulte [Corregir los hallazgos de GuardDuty seguridad detectados](#).

## AttackSequence:ECS/CompromisedCluster

Secuencia de acciones sospechosas realizadas por un clúster de Amazon ECS potencialmente comprometido.

- Gravedad predeterminada: crítica
- Orígenes de datos:
  - [Supervisión del tiempo de ejecución para Amazon ECS Fargate](#)
  - [Supervisión del tiempo de ejecución de instancias EC2 en Amazon ECS](#)
  - [GuardDuty Protección contra malware para Amazon EC2](#)

Este hallazgo le informa de que GuardDuty ha detectado una secuencia de señales sospechosas que indican un clúster de Amazon ECS potencialmente comprometido en su entorno. Estas señales pueden incluir procesos maliciosos, comunicaciones con puntos de conexión maliciosos o comportamientos relacionados con la minería de criptomonedas.

GuardDuty utiliza algoritmos de correlación patentados y varios factores de detección para identificar secuencias de acciones sospechosas dentro de los clústeres de Amazon ECS. Mediante el análisis de los planes de protección y diversas fuentes de señales, GuardDuty identifica los patrones de ataque comunes y emergentes, lo que permite detectar con gran fiabilidad los posibles riesgos.

Medidas correctivas: si este comportamiento es inesperado en su entorno, su clúster de Amazon ECS podría estar en peligro. Para obtener recomendaciones de contención de amenazas, consulte. [Corregir un clúster de ECS potencialmente comprometido](#) Tenga en cuenta que el compromiso puede extenderse a una o más tareas de ECS o cargas de trabajo de contenedores, que podrían haberse utilizado para crear o modificar AWS recursos. Para obtener una guía completa de remediación que abarque los recursos potencialmente afectados, consulte. [Corregir los hallazgos de GuardDuty seguridad detectados](#)

## AttackSequence:EC2/CompromisedInstanceGroup

Secuencia de acciones sospechosas que indican instancias de Amazon EC2 potencialmente comprometidas.

- Gravedad predeterminada: crítica
- Orígenes de datos:
  - [Supervisión del tiempo de ejecución para Amazon EC2](#)

- [Detección de malware para Amazon EC2](#)
- [Logs de flujo de VPC](#)
- [Registros de consultas de DNS de Route53 Resolver](#)

Este hallazgo indica que GuardDuty se detectó una secuencia de acciones sospechosas que sugieren un posible riesgo en un grupo de instancias de Amazon EC2 de su entorno. Los grupos de instancias suelen representar aplicaciones administradas mediante infraestructura como código y que comparten configuraciones similares, como Auto-scaling grupo, rol de perfil de instancia de IAM, pila, plantilla de lanzamiento de AWS CloudFormation Amazon EC2, AMI o ID de VPC. GuardDuty observó varios comportamientos sospechosos en una o más instancias, entre los que se incluyen los siguientes:

- Procesos maliciosos
- Archivos maliciosos
- Conexiones de red sospechosas
- Actividades mineras de criptomonedas
- Uso sospechoso de las credenciales de instancia de Amazon EC2

Método de detección: GuardDuty emplea algoritmos de correlación patentados para identificar secuencias de acciones sospechosas en las instancias de Amazon EC2. Al evaluar los resultados de los planes de protección y diversas fuentes de señales, GuardDuty identifica los patrones de ataque utilizando varios factores, como la reputación de la IP y el dominio y los procesos en ejecución sospechosos.

Medidas correctivas: si este comportamiento es inesperado en su entorno, sus instancias de Amazon EC2 podrían verse comprometidas. El compromiso podría implicar:

- Múltiples procesos
- Credenciales de instancia que pueden haberse utilizado para modificar instancias de Amazon EC2 u otros recursos AWS

Para obtener recomendaciones de contención de amenazas, consulte. [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#) Tenga en cuenta que el compromiso puede extenderse a una o más instancias de Amazon EC2 e implicar procesos o credenciales de instancia comprometidos que podrían haberse utilizado para crear o modificar instancias de



Amazon EC2 u otros recursos. AWS Para obtener una guía completa de remediación que abarque los recursos potencialmente afectados, consulte [Corregir los hallazgos de GuardDuty seguridad detectados](#)

## AttackSequence:IAM/CompromisedCredentials

Secuencia de solicitudes de API que se invocaron mediante AWS credenciales potencialmente comprometidas.

- Gravedad predeterminada: crítica
- Origen de datos: [AWS CloudTrail eventos de gestión](#)

Este hallazgo le informa de que GuardDuty ha detectado una secuencia de acciones sospechosas realizadas mediante el uso de AWS credenciales que afectan a uno o más recursos de su entorno. Se observaron varios comportamientos de ataque sospechosos y anómalos con las mismas credenciales, lo que aumentó la confianza en que se estaba haciendo un uso indebido de las credenciales.

GuardDuty utiliza sus algoritmos de correlación patentados para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. GuardDuty evalúa los resultados de los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar las amenazas, como la reputación de la IP, las secuencias de API, la configuración de los usuarios y los recursos potencialmente afectados.

Medidas correctivas: si este comportamiento es inesperado en su entorno, es posible que sus AWS credenciales se hayan visto comprometidas. Para obtener información sobre los pasos necesarios para solucionarlo, consulte [Corregir las credenciales potencialmente comprometidas AWS](#). Es posible que las credenciales comprometidas se hayan utilizado para crear o modificar recursos adicionales en su entorno, como buckets de Amazon S3, funciones de AWS Lambda o instancias Amazon EC2. Para ver los pasos a seguir para corregir otros recursos que podrían haberse visto afectados, consulte [Corregir los hallazgos de GuardDuty seguridad detectados](#).

## AttackSequence:S3/CompromisedData

Se invocó una secuencia de solicitudes de API en un posible intento de filtrar o destruir datos en Amazon S3.

- Gravedad predeterminada: crítica

- Orígenes de datos: [AWS CloudTrail eventos de datos para S3](#) y [AWS CloudTrail eventos de gestión](#)

Este hallazgo le informa de que GuardDuty detectó una secuencia de acciones sospechosas indicativas de que los datos estaban en peligro en uno o más buckets de Amazon Simple Storage Service (Amazon S3), mediante el uso de credenciales potencialmente comprometidas. AWS Se observaron varios comportamientos de ataque sospechosos y anómalos (solicitudes de API), lo que aumentó la confianza en el uso indebido de las credenciales.

GuardDuty utiliza sus algoritmos de correlación para observar e identificar la secuencia de acciones realizadas mediante la credencial de IAM. GuardDuty a continuación, evalúa los resultados de los planes de protección y otras fuentes de señales para identificar patrones de ataque comunes y emergentes. GuardDuty utiliza varios factores para detectar las amenazas, como la reputación de la IP, las secuencias de API, la configuración de los usuarios y los recursos potencialmente afectados.

Medidas correctivas: si esta actividad es inesperada en su entorno, es posible que sus AWS credenciales o los datos de Amazon S3 se hayan filtrado o destruido. Para ver los pasos a seguir para solucionarlo, consulte [Corregir las credenciales potencialmente comprometidas AWS](#) y [Corregir un bucket de S3 potencialmente comprometido](#).

## GuardDuty Tipos de búsqueda de protección S3

Los siguientes hallazgos son específicos de los recursos de Amazon S3 y tendrán un tipo de recurso igual a S3Bucket si la fuente de datos son eventos de CloudTrail datos de S3 o AccessKey si la fuente de datos son eventos CloudTrail de administración. La gravedad y los detalles de los resultados variarán en función del tipo de resultado y el permiso asociado con el bucket.

Los resultados que se muestran aquí incluyen los orígenes de datos y los modelos utilizados para generar ese tipo de resultado. Para obtener más información sobre orígenes de datos y modelos, consulte [GuardDuty fuentes de datos fundamentales](#).

### Important

Los resultados con una fuente de CloudTrail datos de eventos de datos para S3 solo se generan si se ha activado S3 Protection. De forma predeterminada, después del 31 de julio de 2020, S3 Protection se habilita cuando una cuenta se activa GuardDuty por primera vez o cuando una cuenta de GuardDuty administrador delegado se habilita GuardDuty en una cuenta de miembro existente. Sin embargo, cuando un nuevo miembro se una

a la GuardDuty organización, se aplicarán las preferencias de activación automática de la organización. Para obtener información acerca de las preferencias de habilitación automática, consulte [Configuración de las preferencias de habilitación automática de la organización](#). Para obtener información acerca de cómo habilitar o desactivar la S3 Protection, consulte [GuardDuty Protección S3](#)

Para cualquier resultado del tipo S3Bucket, se recomienda examinar los permisos del bucket en cuestión y los permisos de los usuarios implicados en el resultado. Si la actividad es inesperada, consulte las recomendaciones de corrección que se detallan en [Corregir un bucket de S3 potencialmente comprometido](#).

## Temas

- [Discovery:S3/AnomalousBehavior](#)
- [Discovery:S3/MaliciousIPCaller](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:S3/MaliciousIPCaller](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/MaliciousIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [PenTest:S3/ParrotLinux](#)
- [PenTest:S3/PentooLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)
- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)

## Discovery:S3/AnomalousBehavior

Se ha invocado de forma anómala una API que se utiliza habitualmente para descubrir objetos de S3.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, como, por ejemplo, `ListObjects`. Este tipo de actividad está asociada a la fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Discovery:S3/MaliciousIPCaller

Se invocó una API de S3 que se utiliza habitualmente para descubrir recursos en un AWS entorno desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos de S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a la fase de descubrimiento de un ataque, cuando un adversario recopila información sobre su AWS entorno. Entre los ejemplos se incluyen `GetObjectAcl` y `ListObjects`.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Discovery:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectAcl` o `ListObjects`, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. Este tipo de actividad está asociada a la fase de detección de un ataque, en la que un atacante recopila información para determinar si su entorno de AWS es susceptible de un ataque más amplio.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Discovery:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una API de S3, como `GetObjectACL` o `ListObjects`, desde una dirección IP de nodo de salida de Tor. Este tipo de actividad está asociada a la fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a sus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Exfiltration:S3/AnomalousBehavior

Una entidad de IAM ha invocado una API de S3 de forma sospechosa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado indica que una entidad de IAM está haciendo llamadas a la API que implican un bucket de S3 y que esta actividad difiere de la referencia establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una

solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Exfiltration:S3/MaliciousIPCaller

Una API de S3 que se utiliza habitualmente para recopilar datos de un AWS entorno se invocó desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos de S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de exfiltración, en las que un adversario intenta recopilar datos de su red. Entre los ejemplos se incluyen GetObject y CopyObject.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Impact:S3/AnomalousBehavior.Delete

Una entidad de IAM ha invocado una API de S3 que intenta eliminar datos de forma sospechosa.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una entidad de IAM de su AWS entorno está realizando llamadas a la API que involucran un bucket de S3 y que este comportamiento difiere del punto de referencia

establecido por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta eliminar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para determinar si se puede o se debe restaurar la versión anterior del objeto.

## Impact:S3/AnomalousBehavior.Permission

Se ha invocado de forma anómala una API que se utiliza habitualmente para establecer los permisos de la lista de control de acceso (ACL).

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una entidad de IAM de su AWS entorno ha actualizado una política de bucket o ACL en los buckets de S3 de la lista. Este cambio puede exponer públicamente sus buckets de S3 a todos los usuarios autenticados. AWS

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a



varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que no se haya permitido el acceso público a ningún objeto de forma inesperada.

## Impact:S3/AnomalousBehavior.Write

Una entidad de IAM ha invocado una API de S3 que intenta escribir datos de forma sospechosa.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una entidad de IAM de su AWS entorno está realizando llamadas a la API que involucran un bucket de S3 y que este comportamiento difiere del punto de referencia establecido por esa entidad. La llamada a la API utilizada en esta actividad está asociada a un ataque que intenta escribir datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, una entidad de IAM sin historial previo invoca una API de S3 o una entidad de IAM invoca una API de S3 desde una ubicación inusual.

El modelo de aprendizaje automático (ML) de detección GuardDuty de anomalías identificó esta API como anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Hace un seguimiento a varios factores de las solicitudes de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud, la API específica que se solicitó, el bucket que se solicitó y la cantidad de llamadas que se hicieron a la API. Para obtener más información acerca de los factores de una solicitud de API que son inusuales para la identidad de usuario que ha invocado la solicitud, consulte [Detalles de los resultados](#).

### Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

Se recomienda llevar a cabo una auditoría del contenido del bucket de S3 para asegurarse de que esta llamada a la API no haya escrito datos maliciosos o no autorizados.

### Impact:S3/MaliciousIPCaller

Una API de S3 que se suele utilizar para manipular datos o procesos en un AWS entorno se invocó desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos de S3

Este resultado le informa de que se ha invocado una operación de API de S3 desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto en las que un adversario intenta manipular, interrumpir o destruir los datos de su AWS entorno. Entre los ejemplos se incluyen PutObject y PutObjectAcl.

### Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

### PenTest:S3/KaliLinux

Se ha invocado una API de S3 desde una máquina de Kali Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una máquina que ejecuta Kali Linux realiza llamadas a la API de S3 con las credenciales que pertenecen a su AWS cuenta. Las credenciales podrían estar

comprometidas. Kali Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## PenTest:S3/ParrotLinux

Se ha invocado una API de S3 desde una máquina de Parrot Security Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una máquina que ejecuta Parrot Security Linux realiza llamadas a la API de S3 con las credenciales que pertenecen a su AWS cuenta. Las credenciales podrían estar comprometidas. Parrot Security Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para encontrar puntos débiles en la configuración de EC2 y obtener acceso no autorizado al entorno de AWS .

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## PenTest:S3/PentooLinux

Se ha invocado una API de S3 desde una máquina de Pentoo Linux.

Gravedad predeterminada: media

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una máquina que ejecuta Pentoo Linux realiza llamadas a la API de S3 con las credenciales que pertenecen a su AWS cuenta. Las credenciales podrían estar comprometidas. Pentoo Linux es una popular herramienta de pruebas de intrusión que utilizan los profesionales de la seguridad para identificar puntos débiles en las instancias de EC2 que requieren la aplicación de parches. Los atacantes también utilizan esta herramienta para detectar puntos débiles en la configuración de EC2 y obtener acceso no autorizado a su AWS entorno.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Policy:S3/AccountBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en una cuenta.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de administración

Este resultado le informa de que el bloqueo de acceso público de Amazon S3 estaba desactivado en la cuenta. Cuando se activa la configuración de Bloqueo de acceso público de S3, se utiliza para filtrar las políticas o las listas de control de acceso (ACL) en los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en una cuenta para permitir el acceso público a un bucket o a los objetos que este contiene. Cuando Bloqueo de acceso público de S3 está desactivado para una cuenta, el acceso a sus buckets se controla mediante las políticas, las ACL o la configuración de Bloqueo de acceso público por bucket que se aplique a sus buckets individuales. Esto no necesariamente significa que los buckets se compartan públicamente, pero sí es importante auditar los permisos que se aplican a los buckets para confirmar que proporcionan el nivel de acceso adecuado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Policy:S3/BucketAnonymousAccessGranted

Una entidad principal de IAM ha concedido acceso a Internet a un bucket de S3 al cambiar las políticas o las ACL del bucket.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bucket de S3 que aparece en la lista se ha hecho públicamente accesible en Internet porque una entidad de IAM ha cambiado una política de bucket o una ACL de ese bucket.

Tras detectar un cambio en la política o en la ACL, GuardDuty utiliza el razonamiento automatizado desarrollado por [Zelkova](#) para determinar si el depósito es de acceso público.

### Note

Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de [Bloqueo de acceso público de S3](#) que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como UNKNOWN.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Policy:S3/BucketBlockPublicAccessDisabled

Una entidad de IAM ha invocado una API utilizada para desactivar el bloqueo de acceso público de S3 en un bucket.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de gestión

Este resultado le informa de que el bloqueo de acceso público se ha deshabilitado para el bucket de S3 que aparece en la lista. Cuando se activa, la configuración de Bloqueo de acceso público de S3 se utiliza para filtrar las políticas o las listas de control de acceso (ACL) aplicadas a los buckets como medida de seguridad para prevenir la exposición pública involuntaria de datos.

Normalmente, el Bloqueo de acceso público de S3 está desactivado en un bucket para permitir el acceso público a este o a los objetos que contiene. Cuando el Bloqueo de acceso público de S3 se deshabilita en un bucket, las políticas o las ACL que se han aplicado al bucket controlan el acceso a este. Esto no significa que el bucket se comparta públicamente, pero sí es importante auditar las políticas y ACL que se aplican al bucket para confirmar que se apliquen los permisos adecuados.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Policy:S3/BucketPublicAccessGranted

Un director de IAM ha concedido acceso público a un bucket de S3 a todos AWS los usuarios cambiando las políticas del bucket o las ACL.

Gravedad predeterminada: alta

- Fuente de datos: eventos de gestión CloudTrail

Este hallazgo indica que el bucket de S3 que aparece en la lista se ha expuesto públicamente a todos los AWS usuarios autenticados porque una entidad de IAM ha cambiado una política de bucket o una ACL en ese bucket de S3.

Tras detectar un cambio en la política o en la ACL, GuardDuty utiliza un razonamiento automatizado desarrollado por [Zelkova](#) para determinar si el bucket es de acceso público.

### Note

Si las ACL o las políticas de un bucket están configuradas para denegar explícitamente o denegar todo, es posible que este resultado no refleje el estado actual del bucket. Este resultado no reflejará ninguna configuración de [Bloqueo de acceso público de](#)

[S3](#) que pudiera haberse habilitado para su bucket de S3. En esos casos, el valor `effectivePermission` del resultado se marcará como UNKNOWN.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Stealth:S3/ServerAccessLoggingDisabled

El registro de acceso al servidor de S3 se ha deshabilitado para un bucket.

Gravedad predeterminada: baja

- Fuente de datos: eventos CloudTrail de gestión

Este hallazgo le informa de que el registro de acceso al servidor S3 está deshabilitado para un bucket de su AWS entorno. Si está deshabilitado, no se crea ningún registro de solicitudes web para los intentos de acceso al bucket de S3 identificado; sin embargo, se siguen rastreando las llamadas a la API de administración de S3 al bucket [DeleteBucket](#), por ejemplo. Si el registro de eventos de datos de S3 está habilitado CloudTrail para este depósito, se seguirá rastreando las solicitudes web de los objetos incluidos en el depósito. La desactivación del registro es una técnica que suelen utilizar los usuarios no autorizados para evitar que los detecten. Para obtener más información sobre los registros de S3, consulte [Registro de acceso al servidor de S3](#) y [Opciones de registro para S3](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Se ha invocado una API de S3 desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como `PutObject` o `PutObjectAcl`, desde una dirección IP que aparece en una lista de amenazas que ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## UnauthorizedAccess:S3/TorIPCaller

Se ha invocado una API de S3 desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Fuente de datos: eventos CloudTrail de datos para S3

Este resultado le informa de que se ha invocado una operación de la API de S3, como `PutObject` o `PutObjectAcl`, desde una dirección IP de nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Este hallazgo puede indicar un acceso no autorizado a sus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Tipos de resultados de la protección de EKS

Los siguientes resultados son específicos de los recursos de Amazon EKS y tienen un `resource_type` de `EKSCluster`. La gravedad y los detalles de los resultados varían en función del tipo de resultado.



Para todos los resultados del tipo de registros de auditoría de EKS, recomendamos que examine el recurso en cuestión para determinar si la actividad es esperada o potencialmente maliciosa. Para obtener orientación sobre cómo corregir un recurso de registros de auditoría de EKS comprometido identificado mediante un GuardDuty hallazgo, consulte [Corregir los resultados de EKS Protection](#).

 Note

Si se espera la actividad por la que se generan estos resultados, considere agregar [Reglas de supresión en GuardDuty](#) para evitar futuras alertas.

## Temas

- [CredentialAccess:Kubernetes/MaliciousIPCaller](#)
- [CredentialAccess:Kubernetes/MaliciousIPCaller.Custom](#)
- [CredentialAccess:Kubernetes/SuccessfulAnonymousAccess](#)
- [CredentialAccess:Kubernetes/TorIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller](#)
- [DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom](#)
- [DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess](#)
- [DefenseEvasion:Kubernetes/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Impact:Kubernetes/SuccessfulAnonymousAccess](#)
- [Impact:Kubernetes/TorIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller](#)
- [Persistence:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/SuccessfulAnonymousAccess](#)

- [Persistence:Kubernetes/TorIPCaller](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- [CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated](#)
- [Execution:Kubernetes/AnomalousBehavior.ExecInPod](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer](#)
- [Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount](#)
- [Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed](#)
- [PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated](#)
- [Discovery:Kubernetes/AnomalousBehavior.PermissionChecked](#)

#### Note

Antes de la versión 1.14 de Kubernetes, el `system:unauthenticated` grupo estaba asociado a y de forma predeterminada. `system:discovery` `system:basic-user` ClusterRoles Esta asociación puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos. Aunque se haya actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan habilitados. Se recomienda que desasocie estos permisos del grupo `system:unauthenticated`. Para obtener orientación sobre cómo revocar estos permisos, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

## CredentialAccess:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se utiliza habitualmente para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP en una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si

la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## CredentialAccess:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a las credenciales o los secretos de un clúster de Kubernetes desde una dirección IP de un nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de acceso a las credenciales, en las que un adversario intenta recopilar contraseñas, nombres de usuario y claves de acceso de su clúster de Kubernetes. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos del clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## DefenseEvasion:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque

los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para evadir medidas de defensa desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para evadir medidas defensivas.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## DefenseEvasion:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para evadir medidas defensivas desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a las tácticas de evasión de la defensa, en las que un adversario intenta ocultar sus acciones para evitar ser detectado. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Discovery:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes desde una dirección IP.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

### Para el acceso sin autenticar

Los resultados `MaliciousIPCaller` no se generan en caso de acceso sin autenticar.  
Los resultados `SuccessfulAnonymousAccess` no se generan en caso de acceso sin autenticar o anónimo.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un



adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Discovery:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Discovery:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para descubrir recursos en un clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de detección de un ataque, cuando un adversario recopila información sobre el clúster de Kubernetes. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Este tipo de resultado excluye los puntos de conexión de la API de comprobación de estado, como `/healthz`, `/livez`, `/readyz` y `/version`.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Discovery:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para detectar recursos en un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada se suele utilizar en la fase de detección de un ataque, en la que un atacante recopila información para determinar si el clúster de Kubernetes es susceptible a un ataque más amplio. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Execution:Kubernetes/ExecInKubeSystemPod

Se ejecutó un comando dentro de un pod dentro del espacio de nombres del **sistema kube**

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado indica que se ha ejecutado un comando en un pod dentro del espacio de nombres kube-system mediante la API exec de Kubernetes. El espacio de nombres kube-system es un espacio de nombres predeterminado, que se utiliza principalmente para componentes de nivel de sistema, como kube-dns y kube-proxy. Es muy poco común ejecutar comandos dentro de pods o contenedores de un espacio de nombres kube-system, lo que puede indicar una actividad sospechosa.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de identidad de usuario utilizada para ejecutar el comando se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Impact:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para manipular recursos en un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su entorno. AWS

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Impact:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos de su AWS entorno.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario

es un usuario autenticado, investiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Impact:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a la fase de impacto de un ataque, cuando un adversario está manipulando los recursos del clúster. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Impact:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para manipular los recursos de un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de impacto, en las que un adversario intenta manipular, interrumpir o destruir los datos que están dentro de su entorno de AWS. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado al clúster de Kubernetes con la intención de ocultar la verdadera identidad del atacante.

#### Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, invéstiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

### Persistence:Kubernetes/MaliciousIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP maliciosa conocida.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de API desde una dirección IP asociada a una actividad maliciosa conocida. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

#### Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario

es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Persistence:Kubernetes/MaliciousIPCaller.Custom

Se ha invocado una API que se suele utilizar para obtener acceso persistente a un clúster de Kubernetes desde una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una operación de la API desde una dirección IP que aparece en una lista de amenazas que se ha cargado. La lista de amenazas asociada a este resultado aparece enumerada en la sección Información adicional de los detalles del resultado. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso.

Recomendaciones de corrección:

Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, investigúelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Persistence:Kubernetes/SuccessfulAnonymousAccess

Un usuario no autenticado ha invocado una API que se suele utilizar para obtener permisos de nivel superior a un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que el usuario `system:anonymous` ha invocado correctamente una operación de la API. No se han autenticado las llamadas a la API que ha hecho `system:anonymous`. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster e intenta conservar ese acceso. Esta actividad indica que se permite el acceso anónimo o no autenticado a la acción de la API descrita en el resultado y que se puede permitir a otras acciones. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` en su clúster y asegurarse de que todos los permisos sean necesarios. Si los permisos se han concedido por error o de forma maliciosa, debe revocar el acceso del usuario y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Persistence:Kubernetes/TorIPCaller

Se ha invocado una API que se suele utilizar para acceder a un clúster de Kubernetes desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha invocado una API desde una dirección IP de un nodo de salida de Tor. La API observada suele asociarse a tácticas de persistencia, en las que un adversario ha logrado acceder al clúster de Kubernetes e intenta conservar ese acceso. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a tus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:



Si el usuario del que se informa en el resultado de la sección `KubernetesUserDetails` es `system:anonymous`, investigue por qué se permitió al usuario anónimo invocar la API y revoque los permisos, si es necesario, conforme a las instrucciones que aparecen en las [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si el usuario es un usuario autenticado, invéstiguelo para determinar si la actividad fue legítima o maliciosa. Si la actividad fue maliciosa, revoque el acceso del usuario y anule cualquier cambio hecho por un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Policy:Kubernetes/AdminAccessToDefaultServiceAccount

Se concedieron privilegios de administrador en un clúster de Kubernetes a la cuenta de servicio predeterminada.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que se han concedido privilegios de administrador a la cuenta de servicio predeterminada de un espacio de nombres de su clúster de Kubernetes. Kubernetes crea una cuenta de servicio predeterminada para todos los espacios de nombres del clúster. Asigna automáticamente la cuenta de servicio predeterminada como identidad a los pods que no se han asociado explícitamente a otra cuenta de servicio. Si la cuenta de servicio predeterminada tiene privilegios de administrador, es posible que los pods se inicien involuntariamente con privilegios de administrador. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas.

Recomendaciones de corrección:

No debe utilizar la cuenta de servicio predeterminada para conceder permisos a los pods. En su lugar, debe crear una cuenta de servicio dedicada para cada carga de trabajo y conceder el permiso a esa cuenta en función de sus necesidades. Para solucionar este problema, debe crear cuentas de servicio dedicadas para todos sus pods y cargas de trabajo, además de actualizar los pods y las cargas de trabajo para migrarlos de la cuenta de servicio predeterminada a sus cuentas dedicadas. A continuación, debe eliminar el permiso de administrador de la cuenta de servicio predeterminada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Policy:Kubernetes/AnonymousAccessGranted

Al usuario **system:anonymous** se le concedió el permiso de API en un clúster de Kubernetes.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado le informa de que un usuario de su clúster de Kubernetes ha creado correctamente un `ClusterRoleBinding` o `RoleBinding` para enlazar al usuario `system:anonymous` a un rol. Esto permite el acceso no autenticado a las operaciones de la API permitidas por el rol. Si no se espera este comportamiento, puede indicar un error de configuración o que sus credenciales se han visto afectadas

Recomendaciones de corrección:

Debe examinar los permisos que se han otorgado al usuario `system:anonymous` o grupo `system:unauthenticated` en su clúster y revocar el acceso anónimo innecesario. Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon EKS](#) en la Guía del usuario de Amazon EKS. Si los permisos se han concedido de forma maliciosa, debe revocar el acceso del usuario que concedió los permisos y anular cualquier cambio hecho por un adversario en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Policy:Kubernetes/ExposedDashboard

El panel de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubernetes de su clúster a Internet. Un panel expuesto hace que la interfaz de administración del clúster sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubernetes. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Policy:Kubernetes/KubeflowDashboardExposed

La Kubeflow El panel de control de un clúster de Kubernetes estaba expuesto a Internet

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que el servicio de equilibrador de carga ha expuesto el panel de Kubeflow de su clúster a Internet. Un panel de Kubeflow expuesto hace que la interfaz de administración del entorno de Kubeflow sea accesible desde Internet y permite a los adversarios aprovechar cualquier brecha de autenticación y control de acceso que pueda existir.

Recomendaciones de corrección:

Debe asegurarse de que se apliquen una autenticación y una autorización sólidas en el panel de Kubeflow. También debe implementar un control de acceso a la red para restringir el acceso al panel desde direcciones IP específicas.

Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Se invocó de forma anómala una API de Kubernetes utilizada habitualmente para acceder a secretos.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario de Kubernetes del clúster ha invocado una operación anómala de la API para recuperar secretos confidenciales del clúster. La API observada

normalmente se asocia con tácticas de acceso a credenciales que pueden conducir a una escalada de privilegios y a un mayor acceso dentro del clúster. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales de AWS están comprometidas.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de EKS e identifica eventos anómalos asociados a técnicas utilizadas por usuarios no autorizados. El modelo de ML hace un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes en el clúster y asegúrese de que todos estos permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Se creó RoleBinding o ClusterRoleBinding modificó un rol o un espacio de nombres confidencial demasiado permisivo en tu clúster de Kubernetes.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si una RoleBinding o ClusterRoleBinding incluye la tecla o, la ClusterRoles admin gravedad es alta. cluster-admin

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario en el clúster de Kubernetes ha creado un `RoleBinding` o `ClusterRoleBinding` para vincular un usuario a un rol con permisos de administrador o espacios de nombres confidenciales. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales de AWS están comprometidas.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. Además, el modelo de ML realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes. Estos permisos se definen en el rol y los sujetos implicados en `RoleBinding` y `ClusterRoleBinding`. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Execution:Kubernetes/AnomalousBehavior.ExecInPod

Se ejecutó un comando dentro de un pod de forma anómala.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado informa de que se ejecutó un comando en un pod mediante la API `exec` de Kubernetes. La API `exec` de Kubernetes permite ejecutar comandos arbitrarios en un pod. Si este comportamiento no es el esperado para el usuario, el espacio de nombres o el pod, puede indicar un error de configuración o que sus AWS credenciales están comprometidas.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la API observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario dentro

del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. Además, el modelo de ML realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó, el agente de usuario utilizado y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si la ejecución de este comando es inesperada, es posible que las credenciales de la identidad de usuario utilizada para ejecutar el comando se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Se lanzó una carga de trabajo con un contenedor privilegiado de forma anómala.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado informa de que se ha lanzado una carga de trabajo con un contenedor privilegiado en el clúster de Amazon EKS. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los usuarios no autorizados pueden lanzar contenedores privilegiados como una táctica de escalada de privilegios para primero obtener acceso al host y luego comprometerlo.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio

de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

## Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount

Se implementó una carga de trabajo de forma anómala, con una ruta de host confidencial montada dentro de la carga de trabajo.

Gravedad predeterminada: alta

- Característica: registros de auditoría de EKS

Este resultado informa de que se ha lanzado una carga de trabajo con un contenedor que incluía una ruta de host confidencial en la sección `volumeMounts`. Esto potencialmente hace que la ruta confidencial del host sea accesible y que se pueda escribir en esta desde dentro del contenedor. Esta técnica es comúnmente utilizada por usuarios no autorizados para obtener acceso al sistema de archivos del host.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo

de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

## Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Se lanzó una carga de trabajo de forma anómala.

Gravedad predeterminada: baja\*

### Note

La gravedad predeterminada es Baja. Sin embargo, si la carga de trabajo contiene un nombre de imagen potencialmente sospechoso, como una herramienta de prueba de penetración conocida, o un contenedor que ejecuta un comando potencialmente sospechoso al momento del lanzamiento, como comandos de intérprete de comandos inverso, entonces la gravedad de este tipo de resultado se considerará Media.

- Característica: registros de auditoría de EKS



Este resultado informa de que se ha creado o modificado una carga de trabajo de Kubernetes de forma anómala, como una actividad de la API, nuevas imágenes de contenedor o una configuración arriesgada de la carga de trabajo, dentro del clúster de Amazon EKS. Los usuarios no autorizados pueden lanzar contenedores como una táctica para ejecutar código arbitrario para primero obtener acceso al host y luego comprometerlo.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la creación o modificación del contenedor observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario y de la imagen del contenedor dentro del clúster de EKS. Este modelo de ML también identifica eventos anómalos relacionados con las técnicas utilizadas por un usuario no autorizado. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no sean habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Si este lanzamiento de contenedor es inesperado, es posible que las credenciales de la identidad de usuario utilizada para lanzar el contenedor se hayan visto comprometidas. Revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

Si este lanzamiento de contenedor está previsto, se recomienda utilizar una regla de supresión con un criterio de filtro basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe tener el mismo valor que el campo `imagePrefix` especificado en el resultado. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

## PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Un rol muy permisivo o que ClusterRole se creó o modificó de forma anómala.

Gravedad predeterminada: baja

- Característica: registros de auditoría de EKS

Este resultado informa de que un usuario de Kubernetes en el clúster de Amazon EKS ha llamado a una operación de la API anómala para crear un `Role` o `ClusterRole` con permisos excesivos. Los actores pueden utilizar la creación de roles con permisos elevados para evitar el uso de roles predefinidos similares a administradores y evadir la detección. El exceso de permisos puede derivar en la escalada de privilegios, la ejecución remota de código e incluso el control completo de un espacio de nombres o clúster. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales están comprometidas.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó la API observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de Amazon EKS e identifica eventos anómalos asociados a las técnicas utilizadas por usuarios no autorizados. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el agente de usuario utilizado, las imágenes de contenedor observadas en su cuenta y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Examine los permisos definidos en `Role` o `ClusterRole` para asegurarse de que todos los permisos son necesarios y siguen los principios de mínimo privilegio. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Un usuario comprobó su permiso de acceso de forma anómala.

Gravedad predeterminada: baja

- Característica: registros de auditoría de EKS

Este resultado indica que un usuario en el clúster de Kubernetes ha verificado con éxito si están habilitados permisos elevados conocidos, los cuales pueden facilitar la escalada de privilegios y la ejecución remota de código. Por ejemplo, `kubectl auth can-i` es un comando común utilizado

para comprobar los permisos de un usuario. Si este comportamiento no es el esperado, puede indicar un error de configuración o que las credenciales se han visto comprometidas.

El modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías identificó la API observada como anómala. El modelo de ML evalúa toda la actividad de la API del usuario dentro del clúster de Amazon EKS e identifica eventos anómalos asociados a las técnicas utilizadas por usuarios no autorizados. El modelo de ML también realiza un seguimiento de múltiples factores de la operación de la API, como el usuario que realiza la solicitud, la ubicación desde la que se realizó la solicitud, el permiso que se comprueba y el espacio de nombres que el usuario operó. Puedes encontrar los detalles de la solicitud de API que no son habituales en el panel de detalles de búsqueda de la GuardDuty consola.

Recomendaciones de corrección:

Examine los permisos concedidos al usuario de Kubernetes para asegurarse de que todos los permisos son necesarios. Si los permisos se concedieron por error o de forma malintencionada, revoque el acceso del usuario y revierta cualquier cambio realizado por un usuario no autorizado en el clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si sus AWS credenciales están comprometidas, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## GuardDuty Tipos de búsqueda de Runtime Monitoring

Amazon GuardDuty genera los siguientes resultados de Runtime Monitoring para indicar posibles amenazas en función del comportamiento a nivel del sistema operativo de los hosts y contenedores de Amazon EC2 en sus clústeres de Amazon EKS, las cargas de trabajo de Fargate y Amazon ECS y las instancias de Amazon EC2.

### Note

Los tipos de resultados de la Supervisión en tiempo de ejecución se obtienen según los registros de tiempo de ejecución recopilados de los hosts. Los registros contienen campos, como las rutas de los archivos, que puede controlar un agente malicioso. Estos campos también se incluyen en los resultados para proporcionar un contexto de tiempo de ejecución GuardDuty. Al procesar los resultados de Runtime Monitoring fuera de la GuardDuty consola, debe desinfectar los campos de búsqueda. Por ejemplo, puede codificar en HTML los campos de resultado cuando los muestre en una página web.

## Temas

- [CryptoCurrency:Runtime/BitcoinTool.B](#)
- [Backdoor:Runtime/C&CActivity.B](#)
- [UnauthorizedAccess:Runtime/TorRelay](#)
- [UnauthorizedAccess:Runtime/TorClient](#)
- [Trojan:Runtime/BlackholeTraffic](#)
- [Trojan:Runtime/DropPoint](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [UnauthorizedAccess:Runtime/MetadataDNSRebind](#)
- [Execution:Runtime/NewBinaryExecuted](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [PrivilegeEscalation:Runtime/RuncContainerEscape](#)
- [PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified](#)
- [DefenseEvasion:Runtime/ProcessInjection.Proc](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [DefenseEvasion:Runtime/FilelessExecution](#)
- [Impact:Runtime/CryptoMinerExecuted](#)

- [Execution:Runtime/NewLibraryLoaded](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/UserfaultfdUsage](#)
- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/MaliciousFileExecuted.Custom](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)
- [Discovery:Runtime/SuspiciousCommand](#)
- [Persistence:Runtime/SuspiciousCommand](#)
- [PrivilegeEscalation:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/KernelModuleLoaded](#)

## CryptoCurrency:Runtime/BitcoinTool.B

Una instancia o un contenedor de Amazon EC2 está consultando una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se estaba ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando una dirección IP que está asociada con una actividad relacionada con criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente GuardDuty de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de

hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o un contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado `CryptoCurrency:Runtime/BitcoinTool.B` podría representar la actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:Runtime/BitcoinTool.B`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Backdoor:Runtime/C&CActivity.B

Una instancia o un contenedor de Amazon EC2 está consultando una IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 mostrados en el entorno de AWS consultan una dirección IP asociada a un servidor de comando y control (C&C) conocido. La instancia o el contenedor que aparecen en la lista podrían estar potencialmente afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de

la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

 Note

Si la IP consultada está relacionada con log4j, los campos del hallazgo asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName` = Amazon
- `service.additionalInfo.threatName` = Log4j Related

El agente de GuardDuty tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## UnauthorizedAccess:Runtime/TorRelay

La instancia o contenedor de Amazon EC2 está estableciendo conexiones a una red de Tor como relé de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo indica que un proceso que se ejecuta en la instancia EC2 de la lista o en un contenedor de su AWS entorno se conecta a una red Tor de una manera que sugiere que actúa como un repetidor de Tor. Tor es un software que permite la comunicación anónima. Tor incrementa el anonimato en la comunicación, ya que reenvía el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

El agente GuardDuty de ejecución monitorea los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## UnauthorizedAccess:Runtime/TorClient

La instancia o el contenedor de Amazon EC2 está estableciendo conexiones con un nodo Authority o Guard de Tor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia EC2 de la lista o en un contenedor de su AWS entorno se está conectando a un nodo de Tor Guard o Authority. Tor es un software que permite la comunicación anónima. Los nodos Guard y Authority de Tor actúan como puertas de enlace a una red de Tor. Este tráfico puede indicar que esta instancia o el contenedor de EC2 se han visto afectados y están actuando como clientes en una red de Tor. Este hallazgo puede indicar un acceso no autorizado a tus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.



### Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/BlackholeTraffic

Una instancia o un contenedor de Amazon EC2 intenta comunicarse con una dirección IP de un host remoto que es un agujero negro conocido.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo indica que un proceso que se ejecuta en la instancia EC2 de la lista o en un contenedor de su AWS entorno podría estar en peligro porque intenta comunicarse con la dirección IP de un agujero negro (o sumidero). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

### Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/DropPoint

Una instancia o un contenedor de Amazon EC2 está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia EC2 de la lista o en un contenedor de su AWS entorno está intentando comunicarse con una dirección IP de un host remoto del que se sabe que guarda credenciales y otros datos robados capturados por software malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## CryptoCurrency:Runtime/BitcoinTool.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio asociado con una actividad de criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está consultando un nombre de dominio que está asociado con actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de los recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado CryptoCurrency:Runtime/BitcoinTool.B!DNS podría representar la actividad esperada

para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtrado. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad de criptomonedas o cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Backdoor:Runtime/C&CActivity.B!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que está asociado a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio asociado con un servidor de comando y control (C&C) conocido. La instancia o el contenedor de EC2 de la lista podrían haberse visto afectados. Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet (que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas) que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función de la finalidad y la estructura del botnet, el servidor de C&C también puede emitir comandos para comenzar un ataque de denegación de servicio distribuida (DDoS).

### Note

Si el nombre de dominio consultado está relacionado con log4j, los campos del hallazgo asociado incluirán los siguientes valores:

- `service.additionalInfo.threatListName = Amazon`

- `service.additionalInfo.threatName = Log4j Related`

#### Note

Para comprobar cómo se GuardDuty genera este tipo de hallazgo, puedes realizar una solicitud de DNS desde tu instancia (digpara Linux o nslookup Windows) para compararla con un dominio de prueba. `guardduty2activityb.com`

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/BlackholeTraffic!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectado, ya que está consultando un nombre de dominio que se está redireccionando a una dirección IP de agujero negro. Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de

la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/DropPoint!DNS

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de un host remoto que se conoce que conservar credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia EC2 de la lista o en un contenedor de su AWS entorno está consultando el nombre de dominio de un host remoto del que se sabe que contiene credenciales y otros datos robados capturados por software malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/DGADomainRequest.C!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios generados mediante algoritmo. El malware suele utilizar dichos dominios y podría indicar que una instancia o un contenedor de EC2 se han visto afectados.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS está intentando consultar dominios de algoritmos de generación de dominios (DGA). Es posible que su recurso se haya visto afectado.

Los dominios DGA se utilizan para generar de forma periódica una gran cantidad de nombres de dominio que se pueden usar como puntos de encuentro con sus servidores de comando y control (C&C). Los servidores de comando y control son equipos que envían comandos a los miembros de un botnet, que es una colección de dispositivos conectados a Internet que están infectados y son controlados por un tipo común de malware. El gran número de posibles puntos de encuentro dificulta un apagado eficaz de los botnets, ya que los equipos infectados intentan ponerse en contacto con algunos de estos nombres de dominio cada día para recibir actualizaciones o comandos.

#### Note

Este hallazgo se basa en dominios de DGA conocidos procedentes de fuentes de inteligencia sobre GuardDuty amenazas.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/DriveBySourceTraffic!DNS

Una instancia o un contenedor de Amazon EC2 consulta el nombre de dominio de un host remoto que es una fuente conocida de ataques de Drive-By descarga.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa que un proceso que se está ejecutando en la instancia o el contenedor de EC2 que aparece en la lista del entorno de AWS podría haberse visto afectada, ya que está

consultando un nombre de dominio de un host remoto que es un origen conocido de ataques de descargas Drive-By. Se trata de descargas no intencionadas de software informático desde Internet que pueden iniciar la instalación automática de un virus, spyware o malware.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Trojan:Runtime/PhishingDomainRequest!DNS

Una instancia o un contenedor de Amazon EC2 está consultando dominios implicados en ataques de suplantación de identidad.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en una instancia o un contenedor de EC2 en el entorno de AWS está intentando consultar un dominio implicado en ataques de suplantación de identidad. Los dominios de suplantación de identidad los configura alguien que se presenta como una institución legítima para inducir a las personas a proporcionar información confidencial, como información de identificación personal, datos bancarios y de tarjetas de crédito, y contraseñas. Es posible que su instancia o contenedor de EC2 esté intentando recuperar información confidencial almacenados en un sitio web de suplantación de identidad o que esté intentando configurar un sitio web de este tipo. Su instancia o contenedor de EC2 podrían haberse visto afectados.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Impact:Runtime/AbusedDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios que se sabe que se han utilizado indebidamente.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP de los que se sabe que se ha utilizado indebidamente. Algunos ejemplos de dominios utilizados indebidamente son los nombres de dominio de nivel superior (TLD) y los nombres de dominio de segundo nivel (2LD), que proporcionan registros de subdominios gratuitos, así como proveedores de DNS dinámicos. Los actores de amenazas suelen utilizar estos servicios para registrar dominios de forma gratuita o a un bajo costo. Los dominios de baja reputación de esta categoría también pueden ser dominios caducados que se resuelven en la dirección IP de estacionamiento de un registrador y, por lo tanto, es posible que ya no estén activos. Una IP de estacionamiento es el lugar al que un registrador dirige el tráfico de dominios que no se han vinculado a ningún servicio. La instancia o el contenedor de Amazon EC2 que aparece en la lista pueden haberse visto afectados, ya que los actores de amenazas suelen utilizar estos registradores o servicios para la distribución de C&C y malware.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).



## Impact:Runtime/BitcoinDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a la actividad relacionada con la criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio que está asociado a actividades relacionadas con Bitcoin u otras criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si utiliza esta instancia o el contenedor de EC2 para extraer o administrar criptomonedas, o si cualquiera de estos está involucrado de otra manera en la actividad de cadena de bloques, el resultado podría representar la actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `Impact:Runtime/BitcoinDomainRequest.Reputation`. El segundo criterio de filtro debe ser el ID de instancia de la instancia o el ID de imagen de contenedor del contenedor implicado en una actividad relacionada con las criptomonedas o las cadenas de bloques. Para obtener más información, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Impact:Runtime/MaliciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que está asociado a dominios maliciosos conocidos.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación asociado a dominios o direcciones IP maliciosos conocidos. Por ejemplo, los dominios pueden estar asociados a una dirección IP conocida como oculta. Los dominios ocultos son aquellos que anteriormente estaban controlados por un agente de amenazas y las solicitudes que se les hagan pueden indicar que la instancia se ha visto afectada. Estos dominios también pueden estar correlacionados con campañas o algoritmos de generación de dominios maliciosos conocidos.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Impact:Runtime/SuspiciousDomainRequest.Reputation

Una instancia o un contenedor de Amazon EC2 está consultando un nombre de dominio de baja reputación que resulta sospechoso por naturaleza debido a su antigüedad o a su baja popularidad.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que un proceso que se está ejecutando en el contenedor o la instancia de EC2 que aparece en la lista dentro del entorno de AWS está consultando un nombre de dominio de baja reputación que se sospecha puede ser malicioso. Las características observadas de este dominio coincidían con las de dominios maliciosos observados anteriormente. Sin embargo, nuestro modelo de reputación no pudo relacionarlo definitivamente con una amenaza conocida. Por lo general, estos dominios se han detectado recientemente o reciben poco tráfico.

Los dominios de baja reputación se basan en un modelo de puntuación de reputación. Este modelo evalúa y clasifica las características de un dominio para determinar su probabilidad de ser malicioso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## UnauthorizedAccess:Runtime/MetadataDNSRebind

Una instancia o un contenedor de Amazon EC2 hace búsquedas de DNS que se resuelven en el servicio de metadatos de instancia.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

### Note

Actualmente, este tipo de resultados solo se admite para la arquitectura AMD64.

Este resultado le informa de que un proceso que se ejecuta en la instancia de EC2 de la lista o en un contenedor de su AWS entorno está consultando un dominio que se resuelve en la dirección IP de los metadatos de EC2 (169.254.169.254). Una consulta de DNS de este tipo puede indicar que la instancia es el objetivo de una técnica de reenlace de DNS. Esta técnica se puede utilizar para

obtener metadatos de una instancia de EC2, que incluye las credenciales de IAM asociadas a la instancia.

El reenlace de DNS implica engañar a una aplicación que se ejecuta en la instancia de EC2 para que cargue datos devueltos desde una URL, de tal forma que el nombre de dominio de la URL se resuelve en la dirección IP de metadatos de EC2 (169.254.169.254). Esto hace que la aplicación obtenga acceso a los metadatos de EC2 y, posiblemente, los ponga a disposición del atacante.

Solo se puede obtener acceso a los metadatos de EC2 mediante el reenlace de DNS si la instancia de EC2 ejecuta una aplicación vulnerable que permite la inserción de URL o si un usuario obtiene acceso a la URL en un navegador web que se ejecuta en la instancia de EC2.

El GuardDuty agente de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

En respuesta a este resultado, es importante evaluar si hay alguna aplicación vulnerable que se esté ejecutando en la instancia o en el contenedor de EC2 o si un usuario ha utilizado un navegador para acceder al dominio identificado en el resultado. Si la causa raíz es una aplicación vulnerable, corrija la vulnerabilidad. Si un usuario ha navegado por el dominio identificado, bloquee el dominio o impida que los usuarios puedan acceder a él. Si determina que el resultado está relacionado con cualquiera de los casos anteriores, debe [revocar la sesión asociada a la instancia de EC2](#).

Algunos AWS clientes asignan intencionadamente la dirección IP de los metadatos a un nombre de dominio de sus servidores DNS autorizados. Si este es el caso en su entorno de , le recomendamos que configure una regla de supresión para este resultado. La regla de supresión debe constar de dos criterios de filtro. El primer criterio de filtro debe utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. El segundo criterio de filtro debe ser el Dominio de la solicitud de DNS o el ID de imagen de contenedor del contenedor. El valor Dominio de la solicitud DNS debe coincidir con el dominio que ha asignado a la dirección IP de metadatos (169.254.169.254). Para obtener información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/NewBinaryExecuted

Se ha ejecutado un archivo binario recién creado o que se ha modificado recientemente en un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un archivo binario recién creado o modificado en un contenedor. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. Este comportamiento indica que un actor malicioso que ha obtenido acceso al contenedor ha descargado y ejecutado malware u otro software como parte del comprometimiento potencial. Aunque este tipo de actividad podría ser un indicio de un comprometimiento, también se trata de un patrón de uso habitual. Por lo tanto, GuardDuty utiliza mecanismos para identificar los casos sospechosos de esta actividad y genera este tipo de hallazgos solo para los casos sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. Para identificar el proceso de modificación y el nuevo binario, consulte los detalles del Proceso de modificación y los detalles del Proceso

Los detalles del proceso de modificación se incluyen en el campo `service.runtimeDetails.context.modifyingProcess` del JSON del resultado, o en Proceso de modificación en el panel de detalles del resultado. Para este tipo de resultado, el proceso de modificación es `/usr/bin/dpkg`, como se identifica en el campo `service.runtimeDetails.context.modifyingProcess.executablePath` del JSON del resultado, o como parte del Proceso de modificación en el panel de detalles del resultado.

Los detalles del binario nuevo o modificado ejecutado se incluyen en el `service.runtimeDetails.process` del JSON del resultado, o en la sección Proceso bajo Detalles de tiempo de ejecución. Para este tipo de resultado, el binario nuevo o modificado es `/usr/bin/python3.8`, como se indica en el campo `service.runtimeDetails.process.executablePath` (Ruta ejecutable).

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/DockerSocketAccessed

Un proceso dentro de un contenedor se comunica con el daemon de Docker mediante un socket de Docker.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

El socket de Docker es un socket de dominio Unix que el daemon de Docker (`dockerd`) utiliza para comunicarse con sus clientes. Un cliente puede llevar a cabo diversas acciones, como crear contenedores al comunicarse con el daemon de Docker a través del socket de Docker. Es sospechoso que un proceso de contenedor acceda al socket de Docker. Un proceso de contenedor puede escapar del contenedor y obtener acceso de host al comunicarse con el socket de Docker y crear un contenedor privilegiado.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/RuncContainerEscape

Se detectó un intento de escape del contenedor a través de `runC`.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

`RunC` es el tiempo de ejecución de contenedores de bajo nivel que los tiempos de ejecución de contenedores de alto nivel, como Docker y Containerd utilizan para generar y ejecutar contenedores.

RunC siempre se ejecuta con privilegios de raíz porque necesita realizar la tarea de bajo nivel de crear un contenedor. Un actor que represente una amenaza puede obtener acceso a nivel de host ya sea al modificar o explotar una vulnerabilidad en el binario de runC.

Este resultado detecta la modificación del binario de runC y posibles intentos de explotar las siguientes vulnerabilidades de runC:

- [CVE-2019-5736](#): la explotación de CVE-2019-5736 implica sobrescribir el binario de runC desde dentro de un contenedor. Este resultado se invoca cuando un proceso dentro de un contenedor modifica el binario de runC.
- [CVE-2024-21626](#): la explotación de CVE-2024-21626 implica establecer el directorio de trabajo actual (CWD) o un contenedor en un descriptor de archivo abierto `/proc/self/fd/FileDescriptor`. Este resultado se invoca cuando se detecta un proceso de contenedor con un directorio de trabajo actual bajo `/proc/self/fd/`, por ejemplo, `/proc/self/fd/7`.

Este resultado puede indicar que un actor malicioso ha intentado realizar una explotación en uno de los siguientes tipos de contenedores:

- Un contenedor nuevo con una imagen controlada por un atacante.
- Un contenedor existente al que el actor tenía acceso con permisos de escritura en el binario de runC a nivel de host.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Se detectó un intento de escape de un contenedor a través del agente de liberación de CGroups.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha detectado un intento de modificar el archivo de agente de lanzamiento de un grupo de control (cgroup). Linux utiliza grupos de control (cgroups) para limitar, contabilizar y aislar el uso de recursos de un conjunto de procesos. Cada cgroup tiene un archivo de agente de lanzamiento (`release_agent`), un script que Linux ejecuta cuando termina cualquier proceso dentro del cgroup. El archivo de agente de lanzamiento debe ejecutarse siempre en el host. Un actor de amenazas dentro de un contenedor puede escapar al host mediante la escritura de comandos arbitrarios en el archivo de agente de lanzamiento que pertenece a un cgroup. Cuando termina un proceso dentro de ese cgroup, se ejecutan los comandos escritos por el actor.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/ProcessInjection.Proc

Se ha detectado una inyección de proceso mediante el sistema de archivos `proc` en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. El sistema de archivos `proc` (`procfs`) es un sistema de archivos especial de Linux que presenta la memoria virtual del proceso como un archivo. La ruta de ese archivo es `/proc/PID/mem`, donde PID es el ID único del proceso. Un actor de amenazas puede escribir en este archivo para inyectar código en el proceso. Este resultado identifica los posibles intentos de escritura en este archivo.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.



### Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/ProcessInjection.Ptrace

Se ha detectado una inyección de proceso mediante una llamada al sistema ptrace en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso puede utilizar la llamada al sistema ptrace para inyectar código en otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema ptrace.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

### Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Se ha detectado una inyección de proceso mediante una escritura directa en la memoria virtual en un contenedor o en una instancia de Amazon EC2.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

La inyección de procesos es una técnica que los actores de amenazas utilizan para inyectar código en los procesos a fin de evadir las defensas y, potencialmente, aumentar sus privilegios. Un proceso

puede utilizar una llamada al sistema como `process_vm_writev` para inyectar código directamente en la memoria virtual de otro proceso. Este resultado identifica un posible intento de inyectar código en un proceso mediante la llamada al sistema para escribir en la memoria virtual del proceso.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/ReverseShell

Un proceso en un contenedor o en una instancia de Amazon EC2 ha creado un intérprete de comandos inverso.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Un intérprete de comandos inverso es una sesión de intérprete de comandos que se crea en una conexión que se ha iniciado del host de destino al host del actor. Esto es lo opuesto a un intérprete de comandos normal que se inicia desde el host del actor hasta el host de destino. Los actores de amenazas crean un intérprete de comandos inverso para ejecutar comandos en el objetivo tras obtener el acceso inicial a este. Este resultado indica conexiones de intérprete de comandos inverso que son potencialmente sospechosas.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución y genera este tipo de hallazgo solo cuando se descubre que la actividad y el contexto asociados son inusuales o sospechosos. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

El agente GuardDuty de seguridad monitorea los eventos desde múltiples fuentes. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de búsqueda de la GuardDuty consola.

Si esta actividad es inesperada, es posible que su tipo de recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/FilelessExecution

Un proceso en un contenedor o en una instancia de Amazon EC2 ejecuta código desde la memoria.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa cuando se ejecuta un proceso mediante un archivo ejecutable en memoria en el disco. Se trata de una técnica de evasión de defensa habitual que impide escribir el ejecutable malicioso en el disco para evitar la detección basada en el análisis del sistema de archivos. Si bien el malware utiliza esta técnica, también tiene algunos casos de uso legítimos. Uno de los ejemplos es un compilador Just-in-time (JIT) que escribe código compilado en la memoria y lo ejecuta desde ahí.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Impact:Runtime/CryptoMinerExecuted

Una instancia o un contenedor de Amazon EC2 ejecuta un archivo binario asociado con una actividad de extracción de criptomonedas.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia o contenedor de EC2 de la lista en su AWS entorno está ejecutando un archivo binario asociado a una actividad de minería

de criptomonedas. Los actores de las amenazas pueden intentar tomar el control de recursos de computación para reutilizarlos maliciosamente para la extracción no autorizada de criptomonedas.

El agente GuardDuty de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en el panel de hallazgos de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola y consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/NewLibraryLoaded

Un proceso ha cargado una biblioteca recién creada o modificada recientemente dentro de un contenedor.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este resultado le informa de que se ha creado una biblioteca o que esta se ha modificado dentro de un contenedor durante el tiempo de ejecución y que un proceso que se ejecuta dentro del contenedor la ha cargado. Se recomienda mantener los contenedores inmutables durante el tiempo de ejecución y los archivos binarios, scripts o bibliotecas no deben crearse ni modificarse durante la vida útil del contenedor. La carga de una biblioteca recién creada o modificada en un contenedor puede indicar actividad sospechosa. Este comportamiento indica la posibilidad de que un actor malicioso haya accedido al contenedor, haya descargado y ejecutado malware u otro software como parte de una posible amenaza. Aunque este tipo de actividad podría ser un indicio de un comprometimiento, también se trata de un patrón de uso habitual. Por lo tanto, GuardDuty utiliza mecanismos para identificar los casos sospechosos de esta actividad y genera este tipo de hallazgo solo para los casos sospechosos.

El agente GuardDuty de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Un proceso dentro de un contenedor ha montado un sistema de archivos de host durante el tiempo de ejecución.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Varias técnicas de escape de contenedores implican montar un sistema de archivos de host dentro de un contenedor durante el tiempo de ejecución. Este resultado indica que un proceso dentro de un contenedor podría intentar montar un sistema de archivos de host, lo que podría indicar un intento de escape al host.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/UserfaultfdUsage

Un proceso ha utilizado llamadas al sistema **userfaultfd** para gestionar los errores de página en el espacio de usuario.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Por lo general, los errores de página los gestiona el kernel en el espacio del kernel. Sin embargo, la llamada al sistema `userfaultfd` permite que un proceso gestione los errores de página en

un sistema de archivos del espacio de usuario. Esta es una característica útil que permite la implementación de sistemas de archivos en el espacio de usuario. Por otro lado, también puede ser utilizada por un proceso potencialmente malicioso para interrumpir el funcionamiento del kernel desde el espacio de usuario. Interrumpir el kernel mediante una llamada al sistema `userfaultfd` es una técnica de explotación común para ampliar los intervalos de carrera cuando se explotan las condiciones de carrera del kernel. El uso de `userfaultfd` puede indicar una actividad sospechosa en la instancia de Amazon Elastic Compute Cloud (Amazon EC2).

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/SuspiciousTool

Un contenedor o una instancia de Amazon EC2 está ejecutando un archivo binario o un script que se utiliza con frecuencia en escenarios de seguridad ofensiva, como pruebas de penetración.

Gravedad predeterminada: variable

La gravedad de este resultado puede ser alta o baja, según si la herramienta sospechosa detectada se considera de doble uso o es de uso exclusivamente ofensivo.

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado una herramienta sospechosa en una instancia o contenedor de EC2 de su AWS entorno. Esto incluye las herramientas utilizadas en las actividades de pruebas de penetración, también conocidas como herramientas de puerta trasera, analizadores de red y rastreadores de red. Todas estas herramientas se pueden utilizar en contextos benignos, pero también las utilizan con frecuencia los actores de amenazas con intenciones maliciosas. Si se observan herramientas de seguridad ofensivas, podría ser un indicio de que la instancia de EC2 o el contenedor asociados se han visto comprometidos.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o un contenedor que es indicativo de un comprometimiento.

Gravedad predeterminada: variable

Según el impacto del patrón malicioso observado, la gravedad de este tipo de resultado podría ser baja, media o alta.

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado un comando sospechoso e indica que una instancia de Amazon EC2 o un contenedor de su AWS entorno se han visto comprometidos. Esto puede significar que se ha descargado un archivo de una fuente sospechosa y luego se ha ejecutado, o que un proceso en ejecución muestra un patrón malicioso conocido en su línea de comandos. Esto indica además la presencia de malware en ejecución en el sistema.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

 Note

Los argumentos de la línea de comandos del proceso pueden contener datos confidenciales. Para proteger los datos confidenciales, los resultados de la supervisión del GuardDuty tiempo de ejecución no incluyen los argumentos completos de la línea de comandos. En su lugar, `Service.RuntimeDetails.Context.CommandLineExample` proporciona un ejemplo representativo del patrón de línea de comandos que generó el hallazgo.

## DefenseEvasion:Runtime/SuspiciousCommand

Se ha ejecutado un comando en la instancia de Amazon EC2 o en un contenedor de la lista, intenta modificar o desactivar un mecanismo de defensa de Linux, como el firewall o los servicios esenciales del sistema.

Gravedad predeterminada: variable

Según el mecanismo de defensa que se haya modificado o desactivado, la gravedad de este tipo de resultado puede ser alta, media o baja.

- Característica: supervisión en tiempo de ejecución

Este resultado informa de que se ha ejecutado un comando que intenta ocultar un ataque a los servicios de seguridad del sistema local. Esto incluye acciones como desactivar el firewall de Unix, modificar las tablas de IP locales, eliminar entradas crontab, desactivar un servicio local o asumir la función de `LDPreload`. Cualquier modificación es altamente sospechosa y un indicador potencial de comprometimiento. Por lo tanto, estos mecanismos detectan que el sistema está comprometido o impiden que se comprometa aún más.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución, de modo que solo genera este hallazgo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en los detalles de los resultados



de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/PtraceAntiDebugging

Un proceso en un contenedor o una instancia de Amazon EC2 ha ejecutado una medida antidepuración mediante la llamada al sistema ptrace.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este resultado muestra que un proceso que se ejecuta en la instancia de Amazon EC2 que se encuentra en la lista o un contenedor dentro del entorno de AWS ha utilizado la llamada al sistema ptrace con la opción PTRACE\_TRACEME. Esta actividad provocaría que un depurador asociado se separara del proceso en ejecución. Si no hay ningún depurador asociado, no se producirá ningún efecto. Sin embargo, la actividad en sí misma suscita sospechas. Esto podría ser indicio de la presencia de malware en ejecución en el sistema. El malware utiliza con frecuencia técnicas antidepuración para eludir los análisis, y estas técnicas se pueden detectar en tiempo de ejecución.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/MaliciousFileExecuted

Se ha ejecutado un archivo ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que se ha ejecutado un ejecutable malicioso conocido en una instancia de Amazon EC2 o en un contenedor de su AWS entorno. Se trata de un sólido indicio de que la instancia o el contenedor se han visto potencialmente comprometidos y de que se ha ejecutado malware.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados para generar este hallazgo solo cuando la actividad y el contexto asociados son potencialmente sospechosos.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/MaliciousFileExecuted.Custom

Se ha ejecutado un archivo ejecutable malicioso de una lista de amenazas personalizada en una instancia de Amazon EC2 o en un contenedor.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un archivo ejecutable que está incluido en una lista de entidades de amenazas que ha cargado y activado se ha ejecutado en una instancia de Amazon EC2 o en un

contenedor de su AWS entorno. En GuardDuty, una lista de entidades de amenazas puede incluir direcciones IP, dominios y hashes de SHA-256 archivos maliciosos conocidos. GuardDuty genera resultados en función de la actividad asociada a la lista de entidades de amenazas cargada. Puede ver el nombre de la lista de entidades amenazantes en los detalles de la búsqueda.

Nota: Este hallazgo solo se activa cuando se ejecuta un archivo ejecutable cuyo hash estaba incluido en la lista de entidades de amenaza.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Execution:Runtime/SuspiciousShellCreated

Un servicio de red o un proceso al que se puede acceder a través de la red en una instancia de Amazon EC2 o en un contenedor ha iniciado un proceso de intérprete de comandos interactivo.

Gravedad predeterminada: baja

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un servicio accesible a la red en una instancia de Amazon EC2 o en un contenedor de AWS su entorno ha lanzado un shell interactivo. En determinadas circunstancias, este escenario podría ser indicio de un comportamiento posterior a la explotación. Los intérpretes de comandos interactivos permiten a los atacantes ejecutar comandos arbitrarios en una instancia o contenedor comprometidos.

El agente GuardDuty de ejecución monitorea los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación. Puede ver la información del proceso al que se puede acceder a través de la red en los detalles del proceso principal.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/ElevationToRoot

Un proceso que se ejecuta en la instancia o contenedor de Amazon EC2 que aparece en la lista ha asumido privilegios de raíz.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en el Amazon EC2 de la lista o en el contenedor de su AWS entorno ha asumido privilegios de root mediante una ejecución `setuid` binaria inusual o sospechosa. Esto indica que un proceso en ejecución ha sido potencialmente comprometido, para la instancia de EC2 a través de un exploit, o a través de la explotación `setuid`. Al utilizar los privilegios de raíz, el atacante puede potencialmente ejecutar comandos en la instancia o el contenedor.

Si bien GuardDuty está diseñado para no generar este tipo de hallazgo para actividades que impliquen el uso regular del `sudo` comando, generará este hallazgo cuando identifique la actividad como inusual o sospechosa.

GuardDuty examina la actividad y el contexto relacionados con el tiempo de ejecución y genera este tipo de hallazgo solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

El agente GuardDuty de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Discovery:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo que permite al atacante obtener información sobre el sistema local, la AWS infraestructura circundante o la infraestructura del contenedor.

Gravedad predeterminada: baja

Característica: supervisión en tiempo de ejecución

Este resultado informa de que un proceso que se está ejecutando en la instancia o contenedor de Amazon EC2 listados en el entorno de AWS han ejecutado un comando que podría proporcionar información crucial a un atacante para posibles avances en su cometido. Es posible que se haya recuperado la siguiente información:

- Sistema local, como la configuración del usuario o de la red,
- Otros AWS recursos y permisos disponibles, o
- Infraestructura de Kubernetes, como servicios y pods.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente GuardDuty de tiempo de ejecución supervisa los eventos de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Puede encontrar los detalles sobre el comando sospechoso en el campo `service.runtimeDetails.context` del JSON del resultado. El contexto adicional, incluida la información sobre el proceso y el linaje del proceso, está disponible en el resultado para una mayor investigación.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Persistence:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo que permite a un atacante conservar el acceso y el control de su AWS entorno.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia de Amazon EC2 de la lista o en un contenedor de su AWS entorno ha ejecutado un comando sospechoso. El comando instala un método de persistencia que permite al malware ejecutarse ininterrumpidamente, o permite a un atacante acceder continuamente al tipo de recurso de instancia o contenedor potencialmente comprometido. Esto podría significar que se ha instalado o modificado un servicio del sistema, se ha modificado el `crontab` o se ha añadido un nuevo usuario a la configuración del sistema.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados y genera este tipo de hallazgo solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente GuardDuty de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso potencialmente comprometido, consulta el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Puede encontrar los detalles sobre el comando sospechoso en el campo `service.runtimeDetails.context` del JSON del resultado. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## PrivilegeEscalation:Runtime/SuspiciousCommand

Se ha ejecutado un comando sospechoso en una instancia de Amazon EC2 o en un contenedor, lo cual permite a un atacante escalar privilegios.

Gravedad predeterminada: media

- Característica: supervisión en tiempo de ejecución

Este hallazgo le informa de que un proceso que se ejecuta en la instancia de Amazon EC2 de la lista o en un contenedor de su AWS entorno ha ejecutado un comando sospechoso. El comando intenta realizar una escalada de privilegios, lo que permite a un adversario realizar tareas de alto privilegio.

GuardDuty examina la actividad y el contexto del tiempo de ejecución relacionados y genera este tipo de hallazgo solo cuando la actividad y el contexto asociados son inusuales o sospechosos.

Es posible que la instancia de Amazon EC2 o el contenedor que aparece en los detalles del resultado se hayan visto comprometidos.

El agente GuardDuty de ejecución supervisa los eventos desde varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## DefenseEvasion:Runtime/KernelModuleLoaded

Se cargó un módulo de kernel en una instancia de Amazon EC2, lo que indica un intento de obtener acceso a nivel de kernel.

Gravedad predeterminada: alta

- Característica: supervisión en tiempo de ejecución

Este resultado indica que se cargó un módulo del núcleo en la instancia de EC2 mostrada. Dado que los módulos del núcleo tienen los privilegios más altos por sistema (anillo 0), esto podría indicar que

un agente de amenazas ha obtenido acceso del núcleo. Este nivel de acceso permite un control total del sistema.

El agente GuardDuty de ejecución supervisa los eventos de varios recursos. Para identificar el recurso afectado, consulte el tipo de recurso en los detalles de los resultados de la GuardDuty consola. Cuando proceda, hay contexto adicional, incluida la información sobre el proceso y el linaje del proceso, en los resultados para seguir investigando.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el recurso se haya visto afectado. Para obtener más información, consulte [Corregir los resultados de la Supervisión en tiempo de ejecución](#).

## Tipos de resultados de la protección contra malware para EC2

GuardDuty Malware Protection for EC2 proporciona una única protección contra malware para EC2 que detecta todas las amenazas detectadas durante el análisis de una instancia de EC2 o una carga de trabajo de contenedor. El resultado incluye el número total de detecciones hechas durante el análisis y, en función de la gravedad, proporciona detalles sobre las 32 amenazas principales que detecta. A diferencia de otros GuardDuty hallazgos, los de Malware Protection for EC2 no se actualizan cuando se vuelve a escanear la misma instancia de EC2 o carga de trabajo del mismo contenedor.

Se genera un nuevo resultado de protección contra malware para EC2 por cada análisis que detecta malware. Los hallazgos de Malware Protection for EC2 incluyen información sobre el análisis correspondiente que produjo el hallazgo, así como el GuardDuty hallazgo que lo inició. Esto facilita la correlación entre el comportamiento sospechoso y el malware detectado.

### Note

Cuando GuardDuty detecta actividad maliciosa en la carga de trabajo de un contenedor, Malware Protection for EC2 no genera una detección de nivel EC2.

Los siguientes hallazgos son específicos de GuardDuty Malware Protection for EC2.

### Temas

- [Execution:EC2/MaliciousFile](#)



- [Execution:ECS/MaliciousFile](#)
- [Execution:Kubernetes/MaliciousFile](#)
- [Execution:Container/MaliciousFile](#)
- [Execution:EC2/SuspiciousFile](#)
- [Execution:ECS/SuspiciousFile](#)
- [Execution:Kubernetes/SuspiciousFile](#)
- [Execution:Container/SuspiciousFile](#)

## Execution:EC2/MaliciousFile

Se ha detectado un archivo malicioso en una instancia de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este hallazgo indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos maliciosos en la instancia de EC2 de la lista en su entorno. AWS La instancia que aparece en la lista podría haberse visto afectada. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Execution:ECS/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este hallazgo indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de

ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el contenedor que pertenece al clúster de ECS se haya visto afectado. Para obtener más información, consulte [Corregir un clúster de ECS potencialmente comprometido](#).

## Execution:Kubernetes/MaliciousFile

Se ha detectado un archivo malicioso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este hallazgo indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos maliciosos en una carga de trabajo de contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster administrado por EKS, los detalles de los resultados proporcionarán información adicional sobre el recurso de EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Execution:Container/MaliciousFile

Se ha detectado un archivo malicioso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este hallazgo indica que el análisis de GuardDuty Malware Protection for EC2 detectó uno o más archivos maliciosos en la carga de trabajo de un contenedor y no se identificó información sobre el clúster. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir un contenedor independiente potencialmente comprometido](#).

## Execution:EC2/SuspiciousFile

Se ha detectado un archivo sospechoso en una instancia de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este hallazgo indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos sospechosos en una instancia de EC2. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera ver el archivo detectado en su AWS entorno. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Execution:ECS/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de ECS.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de ECS. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su AWS entorno. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que el contenedor que pertenece al clúster de ECS se haya visto afectado. Para obtener más información, consulte [Corregir un clúster de ECS potencialmente comprometido](#).

## Execution:Kubernetes/SuspiciousFile

Se ha detectado un archivo sospechoso en un clúster de Kubernetes.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos sospechosos en un contenedor que pertenece a un clúster de Kubernetes. Si se trata de un clúster administrado por EKS, los detalles de los resultados proporcionarán información adicional sobre el EKS afectado. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes

los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su entorno. AWS Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Execution:Container/SuspiciousFile

Se ha detectado un archivo sospechoso en un contenedor independiente.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: protección contra malware de EBS

Este resultado indica que el análisis de GuardDuty Malware Protection for EC2 ha detectado uno o más archivos sospechosos en un contenedor sin información de clúster. Para obtener más información, consulte la sección Amenazas detectadas en los detalles de los resultados.

Las detecciones de tipo SuspiciousFile indican la presencia de programas potencialmente no deseados, como adware, spyware o herramientas de doble uso, en un recurso afectado. Estos programas podrían tener un impacto negativo en sus recursos. También es posible que los atacantes los utilicen con fines maliciosos. Por ejemplo, los adversarios pueden utilizar las herramientas de red de forma legítima o maliciosa como herramientas de hackeo para intentar afectar los recursos.

Cuando se detecte un archivo sospechoso, evalúe si espera verlo en su AWS entorno. Si el archivo es inesperado, siga las recomendaciones de corrección que se indican en la siguiente sección.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la carga de trabajo del contenedor se haya visto afectada. Para obtener más información, consulte [Corregir un contenedor independiente potencialmente comprometido](#).

# Tipo de resultado de la protección contra malware para S3

GuardDuty genera un hallazgo solo cuando detecta una posible amenaza de seguridad en su interior Cuenta de AWS. Un resultado de la protección contra malware para S3 indica que el objeto cargado que inició el análisis de malware contiene un archivo potencialmente malicioso.

Para GuardDuty que Amazon genere un hallazgo en su cuenta Cuenta de AWS, habilite GuardDuty tanto Malware Protection for S3. La mejor práctica es activar primero la protección contra malware para S3 GuardDuty y, a continuación, activarla. Si este orden es diferente en tu caso, asegúrate de activarlo GuardDuty antes de que se cargue un objeto de S3 en tu depósito protegido.

## Note

GuardDuty no puede generar una búsqueda para un objeto de S3 que se escaneó antes de activarlo GuardDuty. Para analizar un objeto de S3 existente, puede cargarlo de nuevo.

## Object:S3/MaliciousFile

Se ha detectado un archivo malicioso en un objeto de S3 analizado.

Gravedad predeterminada: alta

- Característica: protección contra malware para S3

Este resultado indica que un análisis de malware ha detectado que el objeto de S3 enumerado es malicioso. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si este resultado fue inesperado, el objeto de S3 es potencialmente malicioso. Para obtener información sobre los pasos de corrección recomendados, consulte [Corregir un objeto de S3 potencialmente malicioso](#).

## Tipos de búsqueda de Malware Protection for Backup

GuardDuty Malware Protection for Backup proporciona una búsqueda única de todas las amenazas detectadas durante el análisis del recurso solicitado. El resultado incluye el número total de

detecciones hechas durante el análisis y, en función de la gravedad, proporciona detalles sobre las 32 amenazas principales que detecta. A diferencia de otros GuardDuty hallazgos, los hallazgos de Malware Protection for Backup no se actualizan cuando se vuelve a escanear el mismo recurso. Se genera un nuevo hallazgo de Malware Protection for Backup para cada análisis que detecte malware.

Los siguientes hallazgos son específicos de GuardDuty Malware Protection for Backup.

#### Temas

- [Execution:EC2/MaliciousFile!Snapshot](#)
- [Execution:EC2/MaliciousFile!AMI](#)
- [Execution:EC2/MaliciousFile!RecoveryPoint](#)
- [Execution:S3/MaliciousFile!RecoveryPoint](#)

## Execution:EC2/MaliciousFile!Snapshot

Se ha detectado un archivo malicioso en una instantánea de EBS.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: Protección contra malware para Backup

Este hallazgo indica que un análisis de GuardDuty Malware Protection for Backup ha detectado uno o más archivos maliciosos en una instantánea de EBS de su entorno. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si esto es inesperado, es posible que la instantánea se haya visto afectada. Para obtener más información, consulte [Corregir una instantánea de EBS potencialmente comprometida](#).

## Execution:EC2/MaliciousFile!AMI

Se ha detectado un archivo malintencionado en una AMI de EC2.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: Protección contra malware para Backup

Este hallazgo indica que un análisis de GuardDuty Malware Protection for Backup ha detectado uno o más archivos maliciosos en una AMI de su entorno. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si esto es inesperado, es posible que la AMI se haya visto afectada. Para obtener más información, consulte [Corregir una AMI de EC2 potencialmente comprometida](#).

## Execution:EC2/MaliciousFile!RecoveryPoint

Se ha detectado un archivo malicioso en un punto de recuperación EC2 de AWS Backup.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: Protección contra malware para Backup

Este hallazgo indica que un análisis de GuardDuty Malware Protection for Backup ha detectado uno o más archivos maliciosos en un punto de recuperación de EC2 de su entorno. El punto de recuperación afectado podría ser una instantánea de EBS o una AMI de EC2. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si esto es inesperado, es posible que el punto de recuperación de EC2 se haya visto afectado. Para obtener más información, consulte [Corregir un punto de recuperación de EC2 potencialmente comprometido](#).

## Execution:S3/MaliciousFile!RecoveryPoint

Se ha detectado un archivo malicioso en un punto de recuperación AWS de Backup S3.

Gravedad predeterminada: varía en función de la amenaza detectada.

- Característica: Protección contra malware para Backup



Este hallazgo indica que un análisis de GuardDuty Malware Protection for Backup ha detectado uno o más objetos maliciosos en un punto de recuperación de S3 de su entorno. Para obtener más información, consulte la sección Amenazas detectadas en el panel de detalles del resultado.

Recomendaciones de corrección:

Si esto es inesperado, es posible que el punto de recuperación de S3 se haya visto afectado. Para obtener más información, consulte [Corregir un punto de recuperación de S3 potencialmente comprometido](#).

## GuardDuty Tipos de búsqueda de RDS Protection

GuardDuty RDS Protection detecta un comportamiento de inicio de sesión anómalo en su instancia de base de datos. Los siguientes resultados son específicos de [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) y tendrán un Tipo de recurso de RDSDBInstance o RDSLimitlessDB. La gravedad y los detalles de los resultados variarán en función del tipo de resultado.

### Temas

- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.FailedLogin](#)
- [CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce](#)
- [CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/MaliciousIPCaller.FailedLogin](#)
- [Discovery:RDS/MaliciousIPCaller](#)
- [CredentialAccess:RDS/TorIPCaller.SuccessfulLogin](#)
- [CredentialAccess:RDS/TorIPCaller.FailedLogin](#)
- [Discovery:RDS/TorIPCaller](#)

## CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta de forma anómala.

Gravedad predeterminada: variable

 Note

Según el comportamiento anómalo asociado a este resultado, la gravedad predeterminada puede ser baja, media y alta.

- Baja: si el nombre de usuario asociado a este resultado inició sesión desde una dirección IP asociada a una red privada.
- Media: si el nombre de usuario asociado a este resultado inició sesión desde una dirección IP pública.
- Alto: si hay un patrón constante de intentos de inicio de sesión fallidos desde direcciones IP públicas, lo que indica que las políticas de acceso son demasiado permisivas.

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo le informa de que se observó un inicio de sesión anómalo correcto en una base de datos de RDS de su entorno. AWS Esto puede indicar que un usuario anteriormente invisible inició sesión en una base de datos de RDS por primera vez. Un escenario común es el de un usuario interno que inicia sesión en una base de datos a la que acceden mediante programación las aplicaciones y no los usuarios individuales.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó este inicio de sesión correcto como anómalo. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre los eventos de inicio de sesión que son potencialmente inusuales, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, se recomienda cambiar la contraseña del usuario de la base de datos asociada y revisar los registros de auditoría disponibles para ver si hay actividad hecha por el usuario anómalo. Los resultados de gravedad media y alta pueden indicar que existe una política de acceso demasiado permisiva a la base de datos y que las credenciales de los usuarios pueden haber quedado expuestas o haberse visto afectadas. Se

recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

## CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Se observaron uno o más intentos de inicio de sesión fallidos inusuales en una base de datos de RDS de su cuenta.

Gravedad predeterminada: baja

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo le informa de que se observaron uno o más inicios de sesión erróneos anómalos en una base de datos de RDS de su entorno. AWS Un intento de inicio de sesión fallido desde direcciones IP públicas puede indicar que la base de datos de RDS de su cuenta ha sido objeto de un intento de ataque de fuerza bruta por parte de un actor potencialmente malicioso.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó estos inicios de sesión fallidos como anómalos. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que la base de datos está expuesta públicamente o que existe una política de acceso demasiado permisiva a la base de datos. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

## CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP pública de forma anómala tras un patrón constante de intentos de inicio de sesión fallidos e inusuales.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo le informa de que se ha observado un inicio de sesión anómalo, indicativo de una fuerza bruta correcta, en una base de datos de RDS de su entorno. AWS Antes de iniciar sesión correctamente de forma anómala, se observaba un patrón constante de intentos de inicio de sesión fallidos inusuales. Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta se hayan visto afectados y que un actor potencialmente malicioso haya accedido a la base de datos de RDS.

El modelo de aprendizaje automático (ML) con detección de GuardDuty anomalías identificó este inicio de sesión exitoso por fuerza bruta como anómalo. El modelo de ML evalúa todos los eventos de inicio de sesión a la base de datos en su [Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles](#) e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. El modelo de ML rastrea varios factores de la actividad de inicio de sesión en RDS, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y los detalles específicos de la conexión a la base de datos que se utilizaron. Para obtener información sobre la actividad de inicio de sesión en RDS que puede ser inusual, consulte [Anomalías basadas en la actividad de inicio de sesión en RDS](#).

Recomendaciones de corrección:

Esta actividad indica que las credenciales de la base de datos pueden estar expuestas o que se hayan visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario potencialmente afectado. Un patrón constante de intentos de inicio de sesión fallidos inusuales es indicador de una política de acceso demasiado permisiva a la base de datos o que la base de datos también puede haber estado expuesta al público. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

## CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP maliciosa conocida.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo indica que se ha producido una actividad de inicio de sesión correcta en el RDS desde una dirección IP asociada a una actividad maliciosa conocida en su entorno. AWS Esto indica que es posible que el usuario y la contraseña asociados a la base de datos de RDS de su cuenta se hayan visto afectados y que un actor potencialmente malicioso haya accedido a la base de datos de RDS.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden estar expuestas o haberse visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario afectado. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

## CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión sin éxito en una base de datos de RDS de su cuenta.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo le informa de que una dirección IP asociada a una actividad maliciosa conocida intentó iniciar sesión en una base de datos de RDS de su AWS entorno, pero no proporcionó el nombre de

usuario o la contraseña correctos. Esto indica que un actor potencialmente malicioso podría estar intentando afectar a la base de datos de RDS de su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

## Discovery:RDS/MaliciousIPCaller

Una dirección IP asociada a una actividad maliciosa conocida ha sondeado una base de datos de RDS de su cuenta; no se ha llevado a cabo ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo indica que una dirección IP asociada a una actividad maliciosa conocida ha explorado una base de datos de RDS de su AWS entorno, aunque no se ha realizado ningún intento de inicio de sesión. Esto puede indicar que un actor potencialmente malicioso está intentando buscar una infraestructura de acceso público.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

## CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Un usuario ha iniciado sesión correctamente en una base de datos de RDS de su cuenta desde una dirección IP de nodo de salida de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado le informa de que un usuario ha iniciado sesión correctamente en una base de datos de RDS de su entorno de AWS desde una dirección IP de nodo de salida de Tor. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del usuario anónimo.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, puede indicar que las credenciales del usuario pueden estar expuestas o haberse visto afectadas. Se recomienda cambiar la contraseña del usuario de la base de datos asociado y revisar los registros de auditoría disponibles para ver la actividad que ha llevado a cabo el usuario afectado. Esta actividad también puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#).

## CredentialAccess:RDS/TorIPCaller.FailedLogin

Una dirección IP de Tor intentó iniciar sesión sin éxito en una base de datos de RDS de su cuenta.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este hallazgo indica que una dirección IP del nodo de salida de Tor intentó iniciar sesión en una base de datos de RDS de su AWS entorno, pero no proporcionó el nombre de usuario o la contraseña correctos. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del usuario anónimo.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

## Discovery:RDS/TorIPCaller

Una dirección IP de nodo de salida de Tor ha sondeado una base de datos de RDS de su cuenta, pero no se ha llevado a cabo ningún intento de autenticación.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de inicio de sesión de RDS

Este resultado indica que una dirección IP de nodo de salida de Tor ha sondeado una base de datos de RDS de su entorno de AWS , aunque no se ha llevado a cabo ningún intento de inicio de sesión. Esto puede indicar que un actor potencialmente malicioso está intentando buscar una infraestructura de acceso público. Tor es un software que permite las comunicaciones anónimas. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de red. El último nodo de Tor se denomina nodo de salida. Esto puede indicar un acceso no autorizado a los recursos de RDS de su cuenta con la intención de ocultar la verdadera identidad del actor potencialmente malicioso.

Recomendaciones de corrección:

Si esta actividad es inesperada para la base de datos asociada, esto puede indicar que existe una política de acceso demasiado permisiva a la base de datos o que la base de datos está expuesta públicamente. Se recomienda colocar la base de datos en una VPC privada y limitar las reglas del



grupo de seguridad para permitir el tráfico únicamente desde los orígenes necesarios. Para obtener más información, consulte [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#).

## Tipos de resultados de la protección de Lambda

En esta sección se describen los tipos de búsqueda que son específicos de sus AWS Lambda recursos y que resourceType figuran como Lambda. Para todos los resultados de Lambda, se recomienda examinar el recurso en cuestión y determinar si se comporta de la manera esperada. Si la actividad está autorizada, puede utilizar [reglas de supresión](#) o [listas de IP confiables y de amenazas](#) para evitar las notificaciones de falsos positivos de ese recurso.

Si la actividad es inesperada, la práctica recomendada de seguridad consiste en suponer que Lambda posiblemente se ha visto afectado y seguir las recomendaciones de corrección.

### Temas

- [Backdoor:Lambda/C&CActivity.B](#)
- [CryptoCurrency:Lambda/BitcoinTool.B](#)
- [Trojan:Lambda/BlackholeTraffic](#)
- [Trojan:Lambda/DropPoint](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:Lambda/TorClient](#)
- [UnauthorizedAccess:Lambda/TorRelay](#)

### Backdoor:Lambda/C&CActivity.B

Una función de Lambda está consultando una dirección IP que está asociada a un servidor de comando y control conocido.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda incluida en su AWS entorno está consultando una dirección IP asociada a un servidor de comando y control (C&C) conocido. La función de

Lambda asociada al resultado generado se ha visto potencialmente afectada. Los servidores C&C son equipos que envían comandos a los miembros de un botnet.

Un botnet es una colección de dispositivos conectados a Internet, que pueden incluir PC, servidores, dispositivos móviles y dispositivos de Internet de las cosas, que están infectados y controlados por un tipo común de malware. A menudo, los botnets se utilizan para distribuir malware y recopilar información obtenida de forma indebida, como números de tarjetas de crédito. En función del propósito y la estructura del botnet, el servidor C&C también puede enviar comandos para comenzar una denegación de servicio distribuida.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## CryptoCurrency:Lambda/BitcoinTool.B

Una función de Lambda consulta una dirección IP asociada con una actividad relacionada con una criptomoneda.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que la función Lambda que aparece en su AWS entorno consulta una dirección IP asociada a una actividad relacionada con Bitcoin u otra actividad relacionada con criptomonedas. Los actores de las amenazas pueden intentar tomar el control de las funciones de Lambda para reutilizarlas maliciosamente para la extracción no autorizada de criptomonedas.

Recomendaciones de corrección:

Si utiliza esta función de Lambda para extraer o administrar criptomonedas, o esta función está involucrada de otra manera en la actividad de cadena de bloques, esto podría representar una actividad esperada para su entorno. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. El primer criterio debe utilizar el atributo de tipo de resultado con un valor CryptoCurrency:Lambda/BitcoinTool.B. El segundo criterio de filtro debe ser el nombre de la función de Lambda de la función implicada en la actividad de la cadena de bloques. Para obtener información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## Trojan:Lambda/BlackholeTraffic

Una función de Lambda está intentando comunicarse con una dirección IP de un host remoto que es una dirección IP de agujero negro conocida.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda incluida en la lista de su AWS entorno está intentando comunicarse con la dirección IP de un agujero negro (o sumidero). Los agujeros negros hacen referencia a lugares de la red donde el tráfico entrante o saliente se descarta silenciosamente sin informar al origen de que los datos no llegaron a su destinatario esperado. Una dirección IP de agujero negro especifica una máquina host que no se está ejecutando o una dirección a la que no se le ha asignado ningún host. La función de Lambda que aparece en la lista se ha visto potencialmente afectada.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## Trojan:Lambda/DropPoint

Una función de Lambda está intentando comunicarse con una dirección IP de un host remoto que se sabe que conserva credenciales y otros datos robados capturados por malware.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda incluida en la lista de su AWS entorno está intentando comunicarse con una dirección IP de un host remoto del que se sabe que contiene credenciales y otros datos robados capturados por el malware.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Una función de Lambda lleva a cabo conexiones a una dirección IP de una lista de amenazas personalizada.

Gravedad predeterminada: media

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda de su AWS entorno se está comunicando con una dirección IP incluida en una lista de amenazas que ha cargado. En GuardDuty, una [lista de amenazas](#) consta de direcciones IP maliciosas conocidas. GuardDuty genera resultados a partir de las listas de amenazas cargadas. Puede ver los detalles de la lista de amenazas en los detalles de búsqueda de la GuardDuty consola.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## UnauthorizedAccess:Lambda/TorClient

Una función de Lambda está llevando a cabo conexiones con un nodo Authority o Guard de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda de su AWS entorno está realizando conexiones a un nodo de Tor Guard o Authority. Tor es un software que permite la comunicación anónima. Los nodos Authority y Guard de Tor actúan como puertas de enlace iniciales a una red de Tor. Este tráfico puede indicar que esta función de Lambda se ha visto potencialmente afectada. Ahora actúa como cliente en una red de Tor.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## UnauthorizedAccess:Lambda/TorRelay

Una función de Lambda está estableciendo conexiones a una red de Tor como relé de Tor.

Gravedad predeterminada: alta

- Característica: supervisión de la actividad de la red de Lambda

Este hallazgo le informa de que una función Lambda en su AWS entorno está haciendo conexiones a una red Tor de una manera que sugiere que actúa como un repetidor Tor. Tor es un software que permite la comunicación anónima. Tor habilita la comunicación anónima al reenviar el tráfico potencialmente ilícito del cliente de un relé de Tor a otro.

## Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que su función de Lambda se haya visto afectada. Para obtener más información, consulte [Corregir una función de Lambda potencialmente comprometida](#).

## Tipos de resultados retirados

Un resultado es una notificación que contiene detalles sobre un problema potencial de seguridad descubierto por GuardDuty . Para obtener información sobre los cambios importantes en los tipos de GuardDuty hallazgos, incluidos los tipos de hallazgos recién agregados o retirados, consulte [Historial de documentos de Amazon GuardDuty](#).

Los siguientes tipos de búsqueda se retiran y ya no los genera GuardDuty.

### Important

No puedes reactivar los tipos de GuardDuty búsqueda retirados.

## Temas

- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Exfiltration:S3/ObjectRead.Unusual](#)
- [Impact:S3/PermissionsModification.Unusual](#)
- [Impact:S3/ObjectDelete.Unusual](#)
- [Discovery:S3/BucketEnumeration.Unusual](#)
- [Persistence:IAMUser/NetworkPermissions](#)
- [Persistence:IAMUser/ResourcePermissions](#)
- [Persistence:IAMUser/UserPermissions](#)
- [PrivilegeEscalation:IAMUser/AdministrativePermissions](#)
- [Recon:IAMUser/NetworkPermissions](#)
- [Recon:IAMUser/ResourcePermissions](#)
- [Recon:IAMUser/UserPermissions](#)
- [ResourceConsumption:IAMUser/ComputeResources](#)
- [Stealth:IAMUser/LoggingConfigurationModified](#)
- [UnauthorizedAccess:IAMUser/ConsoleLogin](#)
- [UnauthorizedAccess:EC2/TorIPCaller](#)
- [Backdoor:EC2/XORDDOS](#)
- [Behavior:IAMUser/InstanceLaunchUnusual](#)
- [CryptoCurrency:EC2/BitcoinTool.A](#)
- [UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

## PrivilegeEscalation:Kubernetes/PrivilegedContainer

Se ha lanzado un contenedor privilegiado con acceso a nivel raíz en su clúster de Kubernetes.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado le informa de que se ha lanzado un contenedor privilegiado en su clúster de Kubernetes mediante una imagen que nunca antes se había utilizado para lanzar contenedores privilegiados en su clúster. Un contenedor privilegiado tiene acceso de nivel raíz al host. Los adversarios pueden lanzar contenedores privilegiados como una táctica de derivación de privilegios para acceder al host y, posteriormente, ponerlo en peligro.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

## Persistence:Kubernetes/ContainerWithSensitiveMount

Se ha lanzado un contenedor con una ruta de host externa confidencial montada en su interior.

Gravedad predeterminada: media

- Característica: registros de auditoría de EKS

Este resultado indica que se ha lanzado un contenedor con una configuración que incluía una ruta de host confidencial con acceso de escritura en la sección `volumeMounts`. Esto hace que la ruta confidencial del host sea accesible y se pueda sobrescribir desde el interior del contenedor. Los adversarios suelen utilizar esta técnica para acceder al sistema de archivos del host.

Recomendaciones de corrección:

Si el lanzamiento de este contenedor es inesperado, es posible que las credenciales de identidad de usuario utilizadas para lanzarlo se hayan visto afectadas. Revoque el acceso del usuario y anule cualquier cambio que haya hecho un adversario en su clúster. Para obtener más información, consulte [Corregir los resultados de EKS Protection](#).

Si el lanzamiento de este contenedor es esperado, se recomienda utilizar una regla de supresión que consista en un criterio de filtrado basado en el campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. En los criterios de filtrado, el campo `imagePrefix` debe ser el mismo que el `imagePrefix`

especificado en el resultado. Para obtener más información sobre la creación de reglas de supresión, consulte [Reglas de supresión](#).

## Exfiltration:S3/ObjectRead.Unusual

Una entidad de IAM ha invocado una API de S3 de forma sospechosa.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

- Fuente de datos: eventos CloudTrail de datos para S3

Este hallazgo le informa de que una entidad de IAM de su AWS entorno está realizando llamadas a la API que involucren un bucket de S3 y que difieren de la línea base establecida por esa entidad. La llamada a la API utilizada en esta actividad está asociada a la fase de exfiltración de un ataque, en la que un atacante intenta recopilar datos. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Impact:S3/PermissionsModification.Unusual

Una entidad de IAM ha invocado una API para modificar los permisos en uno o más recursos de S3.

Gravedad predeterminada: media\*



 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este resultado le informa de que una entidad de IAM está haciendo llamadas a la API diseñadas para modificar los permisos en uno o más buckets u objetos de su entorno de AWS . Es posible que un atacante lleve a cabo esta acción para permitir que la información se comparta fuera de la cuenta. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Impact:S3/ObjectDelete.Unusual

Una entidad de IAM ha invocado una API que se utiliza para eliminar datos en un bucket de S3.

Gravedad predeterminada: media\*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo le informa de que una entidad de IAM específica de su AWS entorno está realizando llamadas a la API diseñadas para eliminar los datos del depósito de S3 de la lista mediante la eliminación del propio depósito. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

## Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Discovery:S3/BucketEnumeration.Unusual

Una entidad de IAM ha invocado una API de S3 que se utiliza para detectar los buckets de S3 dentro de la red.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este resultado le informa de que una entidad de IAM ha invocado una API de S3 para detectar los buckets de S3 en su entorno, como, por ejemplo, `ListBuckets`. Este tipo de actividad está asociada a la fase de descubrimiento de un ataque, en la que un atacante recopila información para determinar si su AWS entorno es susceptible a un ataque más amplio. Esta actividad es sospechosa porque la entidad de IAM invocó la API de una forma inusual. Por ejemplo, esta entidad de IAM no tenía antecedentes de haber invocado este tipo de API o se ha invocado la API desde una ubicación inusual.

## Recomendaciones de corrección:

Si esta actividad es inesperada para la entidad principal asociada, puede indicar que las credenciales han quedado expuestas o que sus permisos de S3 no son lo suficientemente restrictivos. Para obtener más información, consulte [Corregir un bucket de S3 potencialmente comprometido](#).

## Persistence:IAMUser/NetworkPermissions

Una entidad de IAM invocó una API que se utiliza habitualmente para cambiar los permisos de acceso a la red de los grupos de seguridad, las rutas y las ACL de su AWS account.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo indica que un director específico (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario) de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando los ajustes de configuración de la red se modifican en circunstancias sospechosas, como cuando una entidad principal invoca la API de `CreateSecurityGroup` sin antecedentes de haberlo hecho. A menudo, los atacantes intentan cambiar los grupos de seguridad para permitir que cierta cantidad de tráfico entre en varios puertos a fin de mejorar su capacidad para obtener acceso a una instancia de EC2.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Persistence:IAMUser/ResourcePermissions

Un director invocó una API que se usa comúnmente para cambiar las políticas de acceso de seguridad de varios recursos de su Cuenta de AWS.

Gravedad predeterminada: media\*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si se invoca la API con AWS credenciales temporales que se crearon en una instancia, la gravedad del hallazgo es alta.

Este hallazgo indica que un director específico (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario) de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había invocado esta API.

Este hallazgo se activa cuando se detecta un cambio en las políticas o los permisos asociados a AWS los recursos, por ejemplo, cuando un director de su AWS entorno invoca la PutBucketPolicy API sin tener antecedentes de hacerlo. Algunos servicios, como Amazon S3, tienen permisos asociados a recursos que conceden a una o más entidades principales acceso a dicho recurso. Con las credenciales robadas, los atacantes pueden cambiar las políticas asociadas a un recurso para obtener acceso a dicho recurso.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Persistence:IAMUser/UserPermissions

Un director invocó una API que se utiliza habitualmente para añadir, modificar o eliminar usuarios, grupos o políticas de IAM en su AWS account.

Gravedad predeterminada: media\*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo indica que un director específico (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario) de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había invocado esta API.

Este hallazgo se debe a cambios sospechosos en los permisos relacionados con los usuarios de su AWS entorno, por ejemplo, cuando un director de su AWS entorno invoca la `AttachUserPolicy` API sin tener antecedentes de hacerlo. Los atacantes pueden utilizar credenciales robadas para crear nuevos usuarios, agregar políticas de acceso a los usuarios existentes o crear claves de acceso para maximizar su acceso a una cuenta, incluso si su punto de acceso original está cerrado. Por ejemplo, el propietario de la cuenta podría darse cuenta del robo de una contraseña o un usuario de IAM en concreto y eliminarlos de la cuenta. Sin embargo, es posible que no eliminen a otros usuarios que hayan sido creados por un administrador principal creado de forma fraudulenta, dejando su AWS cuenta accesible al atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## PrivilegeEscalation:IAMUser/AdministrativePermissions

Una entidad principal ha intentado asignarse una política excesivamente permisiva.

Gravedad predeterminada: baja\*

### Note

La gravedad de este resultado es baja si no se consigue completar el intento de escalado de privilegios o media si el intento se lleva a cabo con éxito.

Este hallazgo indica que una entidad de IAM específica de su AWS entorno presenta un comportamiento que puede ser indicativo de un ataque de escalada de privilegios. Este resultado se desencadena cuando un rol o un usuario de IAM intentan asignarse una política excesivamente permisiva. Si el usuario o el rol en cuestión no debe tener privilegios administrativos, puede que las credenciales del usuario estén en riesgo o que los permisos del rol no se hayan configurado correctamente.

Los atacantes utilizarán credenciales robadas para crear nuevos usuarios, agregar políticas de acceso a los usuarios existentes o crear claves de acceso para maximizar su acceso a una cuenta

incluso si su punto de acceso original está cerrado. Por ejemplo, el propietario de la cuenta podría percatarse de que le han robado una credencial de inicio de sesión de un usuario de IAM específico y eliminarla de la cuenta. Sin embargo, es posible que no elimine otros usuarios creados por la entidad principal de administración creada de forma fraudulenta, lo que aún dejaría su cuenta de AWS accesible para el atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/NetworkPermissions

Un director invocó una API que se suele utilizar para cambiar los permisos de acceso a la red para los grupos de seguridad, las rutas y las ACL de su AWS account.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo indica que un director específico (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario) de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad principal invoca la API `DescribeInstances` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/ResourcePermissions

Un director invocó una API que se utiliza habitualmente para cambiar las políticas de seguridad y acceso de varios recursos de su AWS account.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo indica que un director específico (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario) de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había invocado esta API.

Este resultado se desencadena cuando se sondean los permisos de acceso a recursos de su cuenta de AWS en circunstancias sospechosas. Por ejemplo, si una entidad principal invoca la API `DescribeInstances` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Recon:IAMUser/UserPermissions

Un director invocó una API que se utiliza habitualmente para añadir, modificar o eliminar usuarios, grupos o políticas de IAM en su AWS account.

Gravedad predeterminada: media\*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este hallazgo se activa cuando se comprueban los permisos de usuario de su AWS entorno en circunstancias sospechosas. Por ejemplo, si una entidad principal (Usuario raíz de la cuenta de AWS, rol de IAM o usuario de IAM) invoca la API `ListInstanceProfilesForRole` cuando no tiene antecedentes de haberlo hecho. Un atacante podría utilizar credenciales robadas para realizar este tipo de reconocimiento de sus AWS recursos con el fin de encontrar credenciales más valiosas o determinar las capacidades de las credenciales que ya tiene.

Este hallazgo indica que un director específico de su AWS entorno presenta un comportamiento diferente del punto de referencia establecido. Esta entidad principal no tiene historial previo de invocación de esta API de esta manera.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## ResourceConsumption:IAMUser/ComputeResources

Una entidad principal ha invocado una API que suele utilizarse para lanzar recursos de computación como instancias EC2.

Gravedad predeterminada: media\*

 Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este resultado se desencadena cuando se lanzan instancias de EC2, que aparecen en la cuenta mostrada en la lista, dentro de su entorno de AWS en circunstancias sospechosas. Este resultado



indica que un director específico de su AWS entorno presenta un comportamiento diferente del valor de referencia establecido; por ejemplo, si un director (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario de IAM) ha invocado la RunInstances API sin antecedentes de haberlo hecho. Esto podría ser señal de que un atacante está utilizando credenciales robadas para robar tiempo de computación (posiblemente para minería de criptomoneda o violación de contraseñas). También puede indicar que un atacante ha utilizado una instancia EC2 de su AWS entorno y sus credenciales para mantener el acceso a su cuenta.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## Stealth:IAMUser/LoggingConfigurationModified

Un director invocó una API que se utiliza habitualmente para detener el CloudTrail registro, eliminar los registros existentes y eliminar cualquier rastro de actividad en su AWS account.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este resultado se desencadena cuando se modifica la configuración de registro de la cuenta de AWS , que aparece en la lista, en circunstancias sospechosas. Este hallazgo indica que un director específico de su AWS entorno presenta un comportamiento diferente del valor de referencia establecido; por ejemplo, si un director (Usuario raíz de la cuenta de AWS un rol de IAM o un usuario de IAM) ha invocado la StopLogging API sin antecedentes de haberlo hecho. Esto puede ser señal de que un atacante está intentando cubrir sus huellas eliminando cualquier rastro de su actividad.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:IAMUser/ConsoleLogin

Un inicio de sesión inusual en la consola realizado por un director de su AWS se observó la cuenta.

Gravedad predeterminada: media\*

### Note

La gravedad predeterminada de este resultado es media. Sin embargo, si la API se invoca con AWS credenciales temporales que se crean en una instancia, la gravedad del hallazgo es alta.

Este resultado se desencadena cuando se detecta un inicio de sesión en la consola en circunstancias sospechosas. Por ejemplo, si un director sin antecedentes de hacerlo invocó la ConsoleLogin API desde un cliente que nunca había utilizado antes o desde una ubicación inusual. Esto podría indicar que se han utilizado credenciales robadas para acceder a tu AWS cuenta o que un usuario válido ha accedido a la cuenta de forma no válida o menos segura (por ejemplo, no a través de una VPN aprobada).

Este hallazgo le informa de que un director específico de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Esta entidad principal nunca antes había iniciado sesión con esta aplicación cliente desde esta ubicación específica.

Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## UnauthorizedAccess:EC2/TorIPCaller

La instancia EC2 recibe conexiones entrantes de un nodo de salida Tor.

Gravedad predeterminada: media

Este hallazgo le informa de que una instancia EC2 de su AWS entorno recibe conexiones entrantes desde un nodo de salida de Tor. Tor es un software que permite la comunicación anónima. Cifra y hace rebotar de forma aleatoria las comunicaciones a través de relés entre una serie de nodos de

red. El último nodo de Tor se denomina nodo de salida. Este hallazgo puede indicar un acceso no autorizado a tus AWS recursos con la intención de ocultar la verdadera identidad del atacante.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Backdoor:EC2/XORDDOS

Una instancia de EC2 está intentando comunicarse con una dirección IP asociada con malware XOR DDoS.

Gravedad predeterminada: alta

Este hallazgo le informa de que una instancia EC2 de su AWS entorno está intentando comunicarse con una dirección IP asociada al malware XOR DDoS. Esta instancia de EC2 podría estar comprometida. XOR DDoS es malware troyano que secuestra sistemas Linux. En un intento de obtener acceso al sistema, lanza un ataque de fuerza bruta para descubrir la contraseña a los servicios de Secure Shell (SSH) en Linux. Después de haber adquirido las credenciales de SSH y haber llevado a cabo correctamente el inicio de sesión, utiliza privilegios de usuario raíz para ejecutar un script que descarga e instala XOR DDoS. A continuación, este malware se utiliza como parte de un botnet para lanzar ataques de denegación de servicio distribuida (DDoS) contra otros destinos.

Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## Behavior:IAMUser/InstanceLaunchUnusual

Un usuario ha lanzado una instancia de EC2 de un tipo inusual.

Gravedad predeterminada: alta

Este hallazgo le informa de que un usuario específico de su AWS entorno presenta un comportamiento diferente al de referencia establecido. Este usuario no tiene historial previo de lanzamientos de una instancia de EC2 de este tipo. Sus credenciales de inicio de sesión podrían haberse visto afectadas.

### Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## CryptoCurrency:EC2/BitcoinTool.A

La instancia EC2 se está comunicando con grupos de minería de Bitcoin.

Gravedad predeterminada: alta

Este hallazgo le informa de que una instancia de EC2 de su AWS entorno se está comunicando con los grupos de minería de Bitcoin. En el campo de la minería de criptomonedas, un grupo de minería es la agrupación de recursos de mineros que comparten potencia de procesamiento a través de una red para dividir la compensación en función de la cantidad de trabajo con la que han contribuido para resolver un bloque. A menos que utilice esta instancia de EC2 para la minería de Bitcoin, dicha instancia podría estar comprometida.

### Recomendaciones de corrección:

Si esta actividad es inesperada, es posible que la instancia se haya visto afectada. Para obtener más información, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## UnauthorizedAccess:IAMUser/UnusualASNCaller

Se ha invocado una API desde una dirección IP de una red inusual.

Gravedad predeterminada: alta

Este resultado le informa que se ha invocado cierta actividad desde una dirección IP de una red inusual. Esta red no se ha observado nunca en todo el historial de uso de AWS del usuario descrito. Esta actividad puede incluir un inicio de sesión en la consola, un intento de lanzar una instancia de EC2, la creación de un nuevo usuario de IAM, la modificación de sus privilegios de AWS , etc. Esto puede indicar un acceso no autorizado a sus AWS recursos.

### Recomendaciones de corrección:

Si esta actividad es inesperada, sus credenciales pueden verse afectadas. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).

## GuardDuty buscar tipos por recursos potencialmente afectados

Las siguientes páginas se clasifican según el tipo de recurso potencialmente afectado asociado a un GuardDuty hallazgo:

- [Tipos de resultados de EC2](#)
- [Tipos de resultados de IAM](#)
- [Tipos de resultados de secuencias de ataque](#)
- [Tipos de resultados de la S3 Protection](#)
- [Tipos de resultados de la protección de EKS](#)
- [Tipos de resultados de la supervisión en tiempo de ejecución](#)
- [Tipos de resultados de la protección contra malware para EC2](#)
- [Tipo de resultado de la protección contra malware para S3](#)
- [Tipos de búsqueda de Malware Protection for Backup](#)
- [Tipos de resultados de la protección de RDS](#)
- [Tipos de resultados de la protección de Lambda](#)

## GuardDuty tipos de búsqueda activos

En la siguiente tabla, se muestran todos los tipos de resultados activos ordenados por el origen de datos o la característica fundamental, según corresponda. En la siguiente tabla, algunos de los resultados tienen los valores de la columna Gravedad del resultado marcados con un asterisco (\*) o un signo más (+):

\* Estos tipos de resultados tienen una gravedad variable. Un resultado de un tipo concreto puede tener una gravedad diferente según el contexto específico del resultado. Para obtener más información sobre un tipo de resultado, consulte su descripción detallada.

+ Los resultados de EC2 que utilizan registros de flujo de VPC como origen de datos no admiten el tráfico IPv6.

| Tipo de resultado                                        | Tipo de recurso | Datos fundamentales source/Feature  | Gravedad del resultado |
|----------------------------------------------------------|-----------------|-------------------------------------|------------------------|
| <a href="#">Discovery:S3/AnomalousBehavior</a>           | Amazon S3       | CloudTrail eventos de datos para S3 | Bajo                   |
| <a href="#">Discovery:S3/MaliciousIPCaller</a>           | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Discovery:S3/MaliciousIPCaller.Custom</a>    | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Discovery:S3/TorIPCaller</a>                 | Amazon S3       | CloudTrail eventos de datos para S3 | Medio                  |
| <a href="#">Exfiltration:S3/AnomalousBehavior</a>        | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Exfiltration:S3/MaliciousIPCaller</a>        | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Custom</a> | Amazon EC2      | Registros de DNS                    | Medio                  |
| <a href="#">Impact:S3/AnomalousBehavior.Delete</a>       | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Impact:S3/AnomalousBehavior.Permission</a>   | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">Impact:S3/AnomalousBehavior.Write</a>        | Amazon S3       | CloudTrail eventos de datos para S3 | Medio                  |
| <a href="#">Impact:S3/MaliciousIPCaller</a>              | Amazon S3       | CloudTrail eventos de datos para S3 | Alto                   |
| <a href="#">PenTest:S3/KaliLinux</a>                     | Amazon S3       | CloudTrail eventos de datos para S3 | Medio                  |

| Tipo de resultado                                               | Tipo de recurso | Datos fundamentales source/Feature                                  | Gravedad del resultado |
|-----------------------------------------------------------------|-----------------|---------------------------------------------------------------------|------------------------|
| <a href="#">PenTest:S3/ParrotLinux</a>                          | Amazon S3       | CloudTrail eventos de datos para S3                                 | Medio                  |
| <a href="#">PenTest:S3/PentoolLinux</a>                         | Amazon S3       | CloudTrail eventos de datos para S3                                 | Medio                  |
| <a href="#">UnauthorizedAccess:S3/TorIPCaller</a>               | Amazon S3       | CloudTrail eventos de datos para S3                                 | Alto                   |
| <a href="#">UnauthorizedAccess:S3/MaliciousIPCaller.Custom</a>  | Amazon S3       | CloudTrail eventos de datos para S3                                 | Alto                   |
| <a href="#">CredentialAccess:IAMUser/AnomalousBehavior</a>      | IAM             | CloudTrail eventos de gestión                                       | Medio                  |
| <a href="#">CredentialAccess:IAMUser/CompromisedCredentials</a> | IAM             | CloudTrail eventos de gestión o eventos CloudTrail de datos para S3 | Alto                   |
| <a href="#">DefenseEvasion:IAMUser/AnomalousBehavior</a>        | IAM             | CloudTrail eventos de gestión                                       | Medio                  |
| <a href="#">DefenseEvasion:IAMUser/BedrockLoggingDisabled</a>   | IAM             | CloudTrail eventos de gestión                                       | Medio                  |
| <a href="#">Discovery:IAMUser/AnomalousBehavior</a>             | IAM             | CloudTrail eventos de gestión                                       | Bajo                   |
| <a href="#">Exfiltration:IAMUser/AnomalousBehavior</a>          | IAM             | CloudTrail eventos de gestión                                       | Alto                   |

| Tipo de resultado                                                                   | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado         |
|-------------------------------------------------------------------------------------|-----------------|------------------------------------|--------------------------------|
| <a href="#">Impact:IAMUser/AnomalousBehavior</a>                                    | IAM             | CloudTrail eventos de gestión      | Alto                           |
| <a href="#">InitialAccess:IAMUser/AnomalousBehavior</a>                             | IAM             | CloudTrail eventos de gestión      | Medio                          |
| <a href="#">PenTest:IAMUser/KaliLinux</a>                                           | IAM             | CloudTrail eventos de gestión      | Medio                          |
| <a href="#">PenTest:IAMUser/ParrotLinux</a>                                         | IAM             | CloudTrail eventos de gestión      | Medio                          |
| <a href="#">PenTest:IAMUser/PentooLinux</a>                                         | IAM             | CloudTrail eventos de gestión      | Medio                          |
| <a href="#">Persistence:IAMUser/AnomalousBehavior</a>                               | IAM             | CloudTrail eventos de gestión      | Medio                          |
| <a href="#">Stealth:IAMUser/PasswordPolicyChange</a>                                | IAM             | CloudTrail eventos de gestión      | Bajo <sup>*</sup> <sub>—</sub> |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS</a> | IAM             | CloudTrail eventos de gestión      | Alto <sup>*</sup> <sub>—</sub> |
| <a href="#">Policy:S3/BucketBlockPublicAccessDisabled</a>                           | Amazon S3       | CloudTrail eventos de gestión      | Bajo                           |
| <a href="#">Policy:S3/BucketAnonymousAccessGranted</a>                              | Amazon S3       | CloudTrail eventos de gestión      | Alto                           |



| Tipo de resultado                                                | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado |
|------------------------------------------------------------------|-----------------|------------------------------------|------------------------|
| <a href="#">Policy:S3/BucketBlockPublicAccessDisabled</a>        | Amazon S3       | CloudTrail eventos de gestión      | Bajo                   |
| <a href="#">Policy:S3/BucketPublicAccessGranted</a>              | Amazon S3       | CloudTrail eventos de gestión      | Alto                   |
| <a href="#">PrivilegeEscalation:IAMUser/AnomalousBehavior</a>    | IAM             | CloudTrail eventos de gestión      | Medio                  |
| <a href="#">Recon:IAMUser/MaliciousIPCaller</a>                  | IAM             | CloudTrail eventos de gestión      | Medio                  |
| <a href="#">Recon:IAMUser/MaliciousIPCaller.Custom</a>           | IAM             | CloudTrail eventos de gestión      | Medio                  |
| <a href="#">Recon:IAMUser/TorIPCaller</a>                        | IAM             | CloudTrail eventos de gestión      | Medio                  |
| <a href="#">Stealth:IAMUser/CloudTrailLoggingDisabled</a>        | IAM             | CloudTrail eventos de gestión      | Bajo                   |
| <a href="#">Stealth:S3/ServerAccessLoggingDisabled</a>           | Amazon S3       | CloudTrail eventos de gestión      | Bajo                   |
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B</a> | IAM             | CloudTrail eventos de gestión      | Medio                  |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller</a>     | IAM             | CloudTrail eventos de gestión      | Medio                  |

| Tipo de resultado                                                                    | Tipo de recurso | Datos fundamentales source/Feature                                  | Gravedad del resultado |
|--------------------------------------------------------------------------------------|-----------------|---------------------------------------------------------------------|------------------------|
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom</a>                  | IAM             | CloudTrail eventos de gestión                                       | Medio                  |
| <a href="#">UnauthorizedAccess:IAMUser/TorIPCaller</a>                               | IAM             | CloudTrail eventos de gestión                                       | Medio                  |
| <a href="#">Policy:IAMUser/RootCredentialUsage</a>                                   | IAM             | CloudTrail eventos de gestión o eventos CloudTrail de datos para S3 | Bajo                   |
| <a href="#">Policy:IAMUser/ShortTermRootCredentialUsage</a>                          | IAM             | CloudTrail eventos de gestión o eventos CloudTrail de datos para S3 | Bajo                   |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</a> | IAM             | CloudTrail eventos de gestión o eventos CloudTrail de datos para S3 | Alto                   |
| <a href="#">UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS</a> | IAM             | CloudTrail eventos de gestión o eventos CloudTrail de datos para S3 | Alto                   |

| Tipo de resultado                                                | Tipo de recurso                                  | Datos fundamentales source/Feature                                                                                                                                                                                                                                                                                                                                                                 | Gravedad del resultado |
|------------------------------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#"><u>AttackSequence:EKS/CompromisedCluster</u></a>     | Recursos involucrados en una secuencia de ataque | <ul style="list-style-type: none"> <li>• Eventos de registro de auditoría de EKS</li> <li>• Runtime Monitoring de Amazon EKS</li> <li>• Detección de malware de Amazon EKS para Amazon EC2</li> <li>• AWS CloudTrail eventos de datos para S3</li> <li>• AWS CloudTrail eventos de gestión</li> <li>• Logs de flujo de VPC</li> <li>• Registros de consultas de DNS de Route53 Resolver</li> </ul> | Critico                |
| <a href="#"><u>AttackSequence:IAM/CompromisedCredentials</u></a> | Recursos involucrados en la secuencia de ataque  | CloudTrail eventos de gestión                                                                                                                                                                                                                                                                                                                                                                      | Critico                |
| <a href="#"><u>AttackSequence:S3/CompromisedData</u></a>         | Recursos involucrados en la secuencia de ataque  | CloudTrail eventos de gestión y eventos CloudTrail de datos para S3                                                                                                                                                                                                                                                                                                                                | Critico                |

| Tipo de resultado                                           | Tipo de recurso                                 | Datos fundamentales source/Feature                                                                                                                                                                                                                    | Gravedad del resultado |
|-------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| <a href="#">AttackSequence:ECS/CompromisedCluster</a>       | Recursos involucrados en la secuencia de ataque | <ul style="list-style-type: none"> <li>• AWS Deteccion es en tiempo de ejecución de Amazon ECS (Fargate)</li> <li>• AWS Deteccion es en tiempo de ejecución de Amazon ECS (instancias de Amazon EC2)</li> <li>• AWS Detecciones de malware</li> </ul> | Critico                |
| <a href="#">AttackSequence:EC2/CompromisedInstanceGroup</a> | Recursos involucrados en la secuencia de ataque | <ul style="list-style-type: none"> <li>• AWS Deteccion es en tiempo de ejecución de Amazon EC2</li> <li>• AWS Detecciones de malware</li> <li>• Logs de flujo de VPC</li> <li>• Registros de consultas de DNS de Route53 Resolver</li> </ul>          | Critico                |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B!DNS</a>          | Amazon EC2                                      | Registros de DNS                                                                                                                                                                                                                                      | Alto                   |
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B!DNS</a>        | Amazon EC2                                      | Registros de DNS                                                                                                                                                                                                                                      | Alto                   |

| Tipo de resultado                                             | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado |
|---------------------------------------------------------------|-----------------|------------------------------------|------------------------|
| <a href="#">Impact:EC2/AbusedDomainRequest.Reputation</a>     | Amazon EC2      | Registros de DNS                   | Medio                  |
| <a href="#">Impact:EC2/BitcoinDomainRequest.Reputation</a>    | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Reputation</a>  | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Impact:EC2/SuspiciousDomainRequest.Reputation</a> | Amazon EC2      | Registros de DNS                   | Bajo                   |
| <a href="#">Trojan:EC2/BlackholeTraffic!DNS</a>               | Amazon EC2      | Registros de DNS                   | Medio                  |
| <a href="#">Trojan:EC2/DGADomainRequest.B</a>                 | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Trojan:EC2/DGADomainRequest.C!DNS</a>             | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Trojan:EC2/DNSDataExfiltration</a>                | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Trojan:EC2/DriveBySourceTraffic!DNS</a>           | Amazon EC2      | Registros de DNS                   | Alto                   |
| <a href="#">Trojan:EC2/DropPoint!DNS</a>                      | Amazon EC2      | Registros de DNS                   | Medio                  |

| Tipo de resultado                                        | Tipo de recurso | Datos fundamentales source/Feature                | Gravedad del resultado                   |
|----------------------------------------------------------|-----------------|---------------------------------------------------|------------------------------------------|
| <a href="#">Trojan:EC2/PhishingDomainRequest!DNS</a>     | Amazon EC2      | Registros de DNS                                  | Alto                                     |
| <a href="#">UnauthorizedAccess:EC2/MetadataDNSRebind</a> | Amazon EC2      | Registros de DNS                                  | Alto                                     |
| <a href="#">Execution:Container/MaliciousFile</a>        | Container       | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:Container/SuspiciousFile</a>       | Container       | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:EC2/MaliciousFile</a>              | Amazon EC2      | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:EC2/SuspiciousFile</a>             | Amazon EC2      | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:ECS/MaliciousFile</a>              | ECS             | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:ECS/SuspiciousFile</a>             | ECS             | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:Kubernetes/MaliciousFile</a>       | Kubernetes      | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:Kubernetes/SuspiciousFile</a>      | Kubernetes      | Protección contra malware de EBS                  | Varía en función de la amenaza detectada |
| <a href="#">Execution:EC2/MaliciousFile!Snapshot</a>     | Amazon EBS      | Protección contra malware para copia de seguridad | Varía en función de la amenaza detectada |

| Tipo de resultado                                                             | Tipo de recurso | Datos fundamentales source/Feature                | Gravedad del resultado                   |
|-------------------------------------------------------------------------------|-----------------|---------------------------------------------------|------------------------------------------|
| <a href="#">Execution:EC2/MaliciousFile!AMI</a>                               | Amazon EC2      | Protección contra malware para copia de seguridad | Varía en función de la amenaza detectada |
| <a href="#">Execution:EC2/MaliciousFile!RecoveryPoint</a>                     | AWS Backup      | Protección contra malware para copia de seguridad | Varía en función de la amenaza detectada |
| <a href="#">Execution:S3/MaliciousFile!RecoveryPoint</a>                      | AWS Backup      | Protección contra malware para copia de seguridad | Varía en función de la amenaza detectada |
| <a href="#">CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed</a> | Kubernetes      | Registros de auditoría de EKS                     | Medio                                    |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCcaller</a>                | Kubernetes      | Registros de auditoría de EKS                     | Alto                                     |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCcaller.Custom</a>         | Kubernetes      | Registros de auditoría de EKS                     | Alto                                     |
| <a href="#">CredentialAccess:Kubernetes/SuccessfulAnonymousAccess</a>         | Kubernetes      | Registros de auditoría de EKS                     | Alto                                     |
| <a href="#">CredentialAccess:Kubernetes/TorIPCcaller</a>                      | Kubernetes      | Registros de auditoría de EKS                     | Alto                                     |
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCcaller</a>                  | Kubernetes      | Registros de auditoría de EKS                     | Alto                                     |

| Tipo de resultado                                                        | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado |
|--------------------------------------------------------------------------|-----------------|------------------------------------|------------------------|
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom</a>       | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess</a>      | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">DefenseEvasion:Kubernetes/TorIPCaller</a>                    | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Discovery:Kubernetes/AnomalousBehavior.PermissionChecked</a> | Kubernetes      | Registros de auditoría de EKS      | Bajo                   |
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller</a>                   | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller.Custom</a>            | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Discovery:Kubernetes/SuccessfulAnonymousAccess</a>           | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Discovery:Kubernetes/TorIPCaller</a>                         | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Execution:Kubernetes/ExecInKubeSystemPod</a>                 | Kubernetes      | Registros de auditoría de EKS      | Medio                  |



| Tipo de resultado                                                       | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado |
|-------------------------------------------------------------------------|-----------------|------------------------------------|------------------------|
| <a href="#">Execution:Kubernetes/AnomalousBehavior.ExecInPod</a>        | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed</a> | Kubernetes      | Registros de auditoría de EKS      | Bajo                   |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller</a>                     | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller.Custom</a>              | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Impact:Kubernetes/SuccessfulAnonymousAccess</a>             | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Impact:Kubernetes/TorIPCaller</a>                           | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller</a>                | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller.Custom</a>         | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Persistence:Kubernetes/SuccessfulAnonymousAccess</a>        | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Persistence:Kubernetes/TorIPCaller</a>                      | Kubernetes      | Registros de auditoría de EKS      | Medio                  |

| Tipo de resultado                                                                                     | Tipo de recurso | Datos fundamentales source/Feature | Gravedad del resultado |
|-------------------------------------------------------------------------------------------------------|-----------------|------------------------------------|------------------------|
| <a href="#">Policy:Kubernetes/AdminAccessToDefaultServiceAccount</a>                                  | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Policy:Kubernetes/AnonymousAccessGranted</a>                                              | Kubernetes      | Registros de auditoría de EKS      | Alto                   |
| <a href="#">Policy:Kubernetes/KubeflowDashboardExposed</a>                                            | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">Policy:Kubernetes/ExposedDashboard</a>                                                    | Kubernetes      | Registros de auditoría de EKS      | Medio                  |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated</a>                   | Kubernetes      | Registros de auditoría de EKS      | Medio <sup>*</sup>     |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated</a>                          | Kubernetes      | Registros de auditoría de EKS      | Bajo                   |
| <a href="#">Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount</a> | Kubernetes      | Registros de auditoría de EKS      | Alto                   |

| Tipo de resultado                                                                                     | Tipo de recurso | Datos fundamentales source/Feature           | Gravedad del resultado |
|-------------------------------------------------------------------------------------------------------|-----------------|----------------------------------------------|------------------------|
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer</a> | Kubernetes      | Registros de auditoría de EKS                | Alto                   |
| <a href="#">Backdoor:Lambda/C&amp;CActivity.B</a>                                                     | Lambda          | Supervisión de la actividad de red de Lambda | Alto                   |
| <a href="#">CryptoCurrency:Lambda/BitcoinTool.B</a>                                                   | Lambda          | Supervisión de la actividad de red de Lambda | Alto                   |
| <a href="#">Trojan:Lambda/BlackholeTraffic</a>                                                        | Lambda          | Supervisión de la actividad de red de Lambda | Medio                  |
| <a href="#">Trojan:Lambda/DropPoint</a>                                                               | Lambda          | Supervisión de la actividad de red de Lambda | Medio                  |
| <a href="#">UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom</a>                                    | Lambda          | Supervisión de la actividad de red de Lambda | Medio                  |
| <a href="#">UnauthorizedAccess:Lambda/TorClient</a>                                                   | Lambda          | Supervisión de la actividad de red de Lambda | Alto                   |
| <a href="#">UnauthorizedAccess:Lambda/TorRelay</a>                                                    | Lambda          | Supervisión de la actividad de red de Lambda | Alto                   |
| <a href="#">Object:S3/MaliciousFile</a>                                                               | S3Object        | Protección contra malware para S3            | Alto                   |

| Tipo de resultado                                                           | Tipo de recurso                                                                             | Datos fundamentales source/Feature                     | Gravedad del resultado             |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------|
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.FailedLogin</a>          | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Bajo                               |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce</a> | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Alto                               |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin</a>      | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Variable <sup>*</sup> <sub>_</sub> |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.FailedLogin</a>          | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Medio                              |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin</a>      | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Alto                               |
| <a href="#">CredentialAccess:RDS/TorIPCaller.FailedLogin</a>                | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Medio                              |
| <a href="#">CredentialAccess:RDS/TorIPCaller.SuccessfulLogin</a>            | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Alto                               |

| Tipo de resultado                                         | Tipo de recurso                                                                             | Datos fundamentales source/Feature                     | Gravedad del resultado |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------|------------------------|
| <a href="#">Discovery:RDS/MaliciousIPCaller</a>           | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Medio                  |
| <a href="#">Discovery:RDS/TorIPCaller</a>                 | <a href="#">Bases de datos ilimitadas de Amazon Aurora, Amazon RDS y Aurora compatibles</a> | Supervisión de la actividad de inicio de sesión de RDS | Medio                  |
| <a href="#">Backdoor:Runtime/C&amp;CAActivity.B</a>       | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Alto                   |
| <a href="#">Backdoor:Runtime/C&amp;CAActivity.B!DNS</a>   | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Alto                   |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B</a>      | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Alto                   |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B!DNS</a>  | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Alto                   |
| <a href="#">DefenseEvasion:Runtime/FilelessExecution</a>  | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Medio                  |
| <a href="#">DefenseEvasion:Runtime/KernelModuleLoaded</a> | Instancia, clúster de EKS, clúster de ECS o contenedor                                      | Supervisión en tiempo de ejecución                     | Alto                   |

| Tipo de resultado                                                          | Tipo de recurso                                        | Datos fundamentales source/Feature | Gravedad del resultado |
|----------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------|------------------------|
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Proc</a>               | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Ptrace</a>             | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite</a> | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">DefenseEvasion:Runtime/PtraceAntiDebugging</a>                 | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Bajo                   |
| <a href="#">DefenseEvasion:Runtime/SuspiciousCommand</a>                   | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Discovery:Runtime/SuspiciousCommand</a>                        | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Bajo                   |
| <a href="#">Execution:Runtime/MaliciousFileExecuted</a>                    | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Execution:Runtime/MaliciousFileExecuted.Custom</a>             | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Execution:Runtime/NewBinaryExecuted</a>                        | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |

| Tipo de resultado                                                | Tipo de recurso                                        | Datos fundamentales source/Feature | Gravedad del resultado |
|------------------------------------------------------------------|--------------------------------------------------------|------------------------------------|------------------------|
| <a href="#">Execution:Runtime/NewLibraryLoaded</a>               | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Execution:Runtime/SuspiciousCommand</a>              | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Variable               |
| <a href="#">Execution:Runtime/SuspiciousShellCreated</a>         | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Bajo                   |
| <a href="#">Execution:Runtime/SuspiciousTool</a>                 | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Variable               |
| <a href="#">Execution:Runtime/ReverseShell</a>                   | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Impact:Runtime/AbusedDomainRequest.Reputation</a>    | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Impact:Runtime/BitcoinDomainRequest.Reputation</a>   | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Impact:Runtime/CryptoMinerExecuted</a>               | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Impact:Runtime/MaliciousDomainRequest.Reputation</a> | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |

| Tipo de resultado                                                        | Tipo de recurso                                        | Datos fundamentales source/Feature | Gravedad del resultado |
|--------------------------------------------------------------------------|--------------------------------------------------------|------------------------------------|------------------------|
| <a href="#">Impact:Runtime/SuspiciousDomainRequest.Reputation</a>        | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Bajo                   |
| <a href="#">Persistence:Runtime/SuspiciousCommand</a>                    | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified</a>  | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">PrivilegeEscalation:Runtime/ContainerMountsHostDirectory</a> | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">PrivilegeEscalation:Runtime/DockerSocketAccessed</a>         | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">PrivilegeEscalation:Runtime/ElevationToRoot</a>              | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">PrivilegeEscalation:Runtime/RuncContainerEscape</a>          | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">PrivilegeEscalation:Runtime/SuspiciousCommand</a>            | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">PrivilegeEscalation:Runtime/UserfaultfdUsage</a>             | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |



| Tipo de resultado                                            | Tipo de recurso                                        | Datos fundamentales source/Feature | Gravedad del resultado |
|--------------------------------------------------------------|--------------------------------------------------------|------------------------------------|------------------------|
| <a href="#">Trojan:Runtime/BlackholeTraffic</a>              | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Trojan:Runtime/BlackholeTraffic!DNS</a>          | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Trojan:Runtime/DropPoint</a>                     | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Trojan:Runtime/DGA DomainRequest.C!DNS</a>       | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Trojan:Runtime/DriveBySourceTraffic!DNS</a>      | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">Trojan:Runtime/DropPoint!DNS</a>                 | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Medio                  |
| <a href="#">Trojan:Runtime/PhishingDomainRequest!DNS</a>     | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">UnauthorizedAccess:Runtime/MetadataDNSRebind</a> | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |
| <a href="#">UnauthorizedAccess:Runtime/TorClient</a>         | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución | Alto                   |

| Tipo de resultado                                            | Tipo de recurso                                        | Datos fundamentales source/Feature     | Gravedad del resultado |
|--------------------------------------------------------------|--------------------------------------------------------|----------------------------------------|------------------------|
| <a href="#">UnauthorizedAccess:Runtime/TorRelay</a>          | Instancia, clúster de EKS, clúster de ECS o contenedor | Supervisión en tiempo de ejecución     | Alto                   |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B</a>               | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/DenialOfService.Dns</a>             | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/DenialOfService.Tcp</a>             | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/DenialOfService.Udp</a>             | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/DenialOfService.UdpOnTcpPorts</a>   | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/DenialOfService.UnusualProtocol</a> | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Alto                   |
| <a href="#">Backdoor:EC2/SpamBot</a>                         | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Medio                  |
| <a href="#">Behavior:EC2/NetworkPortUnusual</a>              | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Medio                  |
| <a href="#">Behavior:EC2/TrafficVolumeUnusual</a>            | Amazon EC2                                             | Registros de flujo de VPC <sup>±</sup> | Medio                  |

| Tipo de resultado                                     | Tipo de recurso | Datos fundamentales source/Feature     | Gravedad del resultado |
|-------------------------------------------------------|-----------------|----------------------------------------|------------------------|
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B</a>      | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Alto                   |
| <a href="#">DefenseEvasion:EC2/UnusualDNSResolver</a> | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">DefenseEvasion:EC2/UnusualDoHActivity</a> | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">DefenseEvasion:EC2/UnusualDoTActivity</a> | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">Impact:EC2/PortSweep</a>                  | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Alto                   |
| <a href="#">Impact:EC2/WinRMBruteForce</a>            | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Bajo <sup>*</sup>      |
| <a href="#">Recon:EC2/PortProbeEMRUnprotectedPort</a> | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Alto                   |
| <a href="#">Recon:EC2/PortProbeUnprotectedPort</a>    | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Bajo <sup>*</sup>      |
| <a href="#">Recon:EC2/Portscan</a>                    | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">Trojan:EC2/BlackholeTraffic</a>           | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">Trojan:EC2/DropPoint</a>                  | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |

| Tipo de resultado                                               | Tipo de recurso | Datos fundamentales source/Feature     | Gravedad del resultado |
|-----------------------------------------------------------------|-----------------|----------------------------------------|------------------------|
| <a href="#">UnauthorizedAccess:EC2/MaliciousIPCaller.Custom</a> | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Medio                  |
| <a href="#">UnauthorizedAccess:EC2/RDPBruteForce</a>            | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Bajo <sup>*</sup>      |
| <a href="#">UnauthorizedAccess:EC2/SSHBruteForce</a>            | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Bajo <sup>*</sup>      |
| <a href="#">UnauthorizedAccess:EC2/TorClient</a>                | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Alto                   |
| <a href="#">UnauthorizedAccess:EC2/TorRelay</a>                 | Amazon EC2      | Registros de flujo de VPC <sup>+</sup> | Alto                   |

# Comprender y generar los GuardDuty hallazgos de Amazon

Un GuardDuty hallazgo representa un posible problema de seguridad detectado en Cuentas de AWS las cargas de trabajo y los datos. GuardDuty genera un hallazgo cada vez que detecta una actividad inesperada y potencialmente maliciosa en su AWS entorno.

Puede ver y gestionar sus GuardDuty hallazgos en la página Hallazgos de la GuardDuty consola o mediante las AWS CLI operaciones de la API. Para obtener información sobre cómo gestionar GuardDuty los hallazgos, consulte [Gestión de los GuardDuty hallazgos de Amazon](#).

Temas:

## [GuardDuty formato de búsqueda](#)

Comprenda el formato de los tipos de GuardDuty búsqueda y los diferentes propósitos de amenazas que GuardDuty rastrea.

## [Ejemplos de hallazgos](#)

Genere ejemplos de resultados en la GuardDuty consola o mediante la GuardDuty API o AWS CLI los comandos. Los resultados de las muestras generadas incluyen detalles ficticios para ayudarle a comprender los detalles de los hallazgos asociados a cada GuardDuty hallazgo. Estos resultados llevan el prefijo [MUESTRA].

## [Pruebe GuardDuty los resultados en cuentas dedicadas](#)

Puede probar GuardDuty hallazgos específicos en su entorno. Ejecute el script `guardduty-tester` en una Cuenta de AWS dedicada que no sea de producción. GuardDuty Para detectar y simular los hallazgos, desplegará ciertos recursos en su entorno. Esta experiencia es diferente de la generación de resultados de muestra.

## [Visualización de los hallazgos generados en la consola GuardDuty](#)

Aprenda a revisar los hallazgos generados en la GuardDuty consola.

## [Niveles de gravedad de GuardDuty los hallazgos](#)

Cada GuardDuty hallazgo tiene un nivel de gravedad asociado que refleja el riesgo potencial en su AWS entorno. En esta sección se explica el significado de cada nivel de gravedad.

## [Detalles de los resultados](#)

Obtén información sobre los detalles relacionados con GuardDuty los hallazgos que se generan en tu cuenta. En este tema se incluyen los detalles relacionados con la detección básica de amenazas, la detección ampliada de amenazas y los planes de protección dedicados. GuardDuty

## [GuardDuty encontrar agregación](#)

Obtenga información sobre cómo GuardDuty se gestionan varias incidencias del mismo tipo de hallazgo. Al agregar los mismos tipos de hallazgos detectados, GuardDuty actualiza el tipo de hallazgo original con los detalles más recientes.

## [GuardDuty buscar tipos](#)

En esta sección se enumeran los tipos de GuardDuty búsqueda por el o asociado [Orígenes de datos fundamentales](#). [Función mapeada GuardDuty](#) Para obtener más información sobre cada tipo de resultado, selecciónelo para obtener más detalles, como su descripción y las posibles medidas para corregirlo.

# GuardDuty formato de búsqueda

Cuando GuardDuty detecta un comportamiento sospechoso o inesperado en su AWS entorno, genera un hallazgo. Un hallazgo es una notificación que contiene los detalles sobre un posible problema de seguridad que se GuardDuty descubre. [Visualización de los hallazgos generados en la consola GuardDuty](#) Incluyen información sobre lo que ocurrió, qué AWS recursos estuvieron involucrados en la actividad sospechosa, cuándo tuvo lugar esta actividad e información relacionada que puede ayudarle a entender la causa raíz.

Uno de los datos más útiles de los detalles de los resultados es el tipo de resultado. El objetivo del tipo de resultado es proporcionar una descripción concisa pero comprensible del posible problema de seguridad. Por ejemplo, el tipo de GuardDuty Recon:EC2/PortProbeUnprotectedPort hallazgo le informa rápidamente de que, en algún lugar de su AWS entorno, una instancia EC2 tiene un puerto desprotegido que un posible atacante está investigando.

GuardDuty utiliza el siguiente formato para nombrar los distintos tipos de hallazgos que genera:

ThreatPurpose:ResourceTypeAffected/ThreatFamilyName.DetectionMechanism! Artefacto

Cada parte de este formato representa un aspecto de un tipo de resultado. Estos aspectos tienen las siguientes explicaciones:

- **ThreatPurpose**- describe el objetivo principal de una amenaza, el tipo de ataque o la fase de un posible ataque. Consulte la siguiente sección para obtener una lista completa de los propósitos de las GuardDuty amenazas.
- **ResourceTypeAffected**- describe qué tipo de AWS recurso se identifica en este hallazgo como el objetivo potencial de un adversario. Actualmente, GuardDuty puede generar resultados para los tipos de recursos que se enumeran en el [GuardDuty tipos de búsqueda activos](#).
- **ThreatFamilyName**- describe la amenaza general o la posible actividad maliciosa que GuardDuty se está detectando. Por ejemplo, un valor de `NetworkPortUnusual` indica que una instancia de EC2 identificada en el GuardDuty hallazgo no tiene un historial previo de comunicaciones en un puerto remoto concreto que también esté identificado en el hallazgo.
- **DetectionMechanism**- describe el método con el que GuardDuty se detectó el hallazgo. Se puede usar para indicar una variación de un tipo de hallazgo común o un hallazgo que GuardDuty utilizó un mecanismo específico para detectarlo. Por ejemplo, `Backdoor:EC2/DenialOfService.Tcp` indica que se detectó una denegación de servicio (DoS) a través de TCP. La variante UDP es `Backdoor:EC2/DenialOfService.Udp`.

Un valor de `.Custom` indica que GuardDuty se detectó el hallazgo en función de sus listas de amenazas personalizadas. Para obtener más información, consulte [Listas de entidades y listas de direcciones IP](#).

Un valor de `.Reputation` indica que GuardDuty se detectó el hallazgo mediante un modelo de puntuación de reputación de dominio. Para obtener más información, consulte [Cómo AWS rastrea las principales amenazas de seguridad de la nube y ayuda a eliminarlas](#).

- **Artefacto**: describe un recurso específico que es propiedad de una herramienta que se utiliza en la actividad maliciosa. Por ejemplo, el DNS del tipo de búsqueda [CryptoCurrency:EC2/BitcoinTool.B!DNS](#) indica que una instancia de Amazon EC2 se está comunicando con un dominio conocido Bitcoin-related .

#### Note

El artefacto es opcional y puede que no esté disponible para todos los tipos de GuardDuty búsqueda.

## Propósitos de amenaza

En GuardDuty una amenaza, el propósito describe el objetivo principal de una amenaza, un tipo de ataque o la fase de un posible ataque. Por ejemplo, algunos propósitos de amenaza, como Backdoor, indican un tipo de ataque. Sin embargo, algunos propósitos de amenaza, como Impact, se alinean con las [tácticas de MITRE ATT&CK](#). Las tácticas de MITRE ATT&CK indican distintas fases del ciclo de ataque del adversario. En la versión actual de GuardDuty, ThreatPurpose puede tener los siguientes valores:

### Backdoor

Este valor indica que un adversario ha puesto en peligro un AWS recurso y lo ha modificado para que pueda ponerse en contacto con su servidor de comando y control (C&C) local y recibir más instrucciones sobre una actividad maliciosa.

### Comportamiento

Este valor indica que GuardDuty ha detectado una actividad o patrones de actividad diferentes de la línea base establecida para los AWS recursos involucrados.

### CredentialAccess

Este valor indica que GuardDuty ha detectado patrones de actividad que un adversario podría utilizar para robar credenciales, como contraseñas, nombres de usuario y claves de acceso, de su entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

### Cryptocurrency

Este valor indica que GuardDuty ha detectado que un AWS recurso de su entorno aloja software asociado a criptomonedas (por ejemplo, Bitcoin).

### DefenseEvasion

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para evitar ser detectado mientras se infiltra en su entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

### Discovery

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para ampliar su conocimiento de sus sistemas y redes internas. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).



## Execution

Este valor indica que GuardDuty ha detectado que un adversario puede intentar ejecutar o ya ha ejecutado un código malicioso para explorar el AWS entorno o robar datos. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## Exfiltration

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar al intentar robar datos de su entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## Impact

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que sugieren que un adversario está intentando manipular, interrumpir o destruir sus sistemas y datos. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## InitialAccess

Este valor generalmente se asocia con la etapa de acceso inicial de un ataque cuando un adversario intenta establecer acceso al entorno. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## Pentest

A veces, los propietarios de AWS los recursos o sus representantes autorizados realizan pruebas intencionadas en las AWS aplicaciones para detectar vulnerabilidades, como grupos de seguridad abiertos o claves de acceso demasiado permisivas. Estas pruebas de intrusión son un intento de identificar y bloquear los recursos vulnerables antes de que los descubran los adversarios. Sin embargo, algunas de las herramientas que se utilizan para las pruebas de intrusión autorizadas están disponibles de forma gratuita y, por tanto, los usuarios no autorizados o los adversarios pueden utilizarlas para llevar a cabo pruebas de sondeo. Si bien no GuardDuty puede identificar el verdadero propósito de dicha actividad, el valor de Pentest indica que GuardDuty se está detectando dicha actividad, que es similar a la que generan las conocidas herramientas de prueba con lápiz óptico y que podría indicar que se está realizando un sondeo malintencionado de la red.

## Persistencia

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar para intentar mantener el acceso a sus sistemas aunque su ruta de acceso inicial esté cortada. Por ejemplo, esto podría incluir la creación de un nuevo usuario de

IAM después de obtener acceso a través de las credenciales afectadas de un usuario existente. Cuando se eliminan las credenciales del usuario existente, el adversario retendrá el acceso al nuevo usuario que no se haya detectado como parte del evento original. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## Política

Este valor indica que su Cuenta de AWS comportamiento va en contra de las mejores prácticas de seguridad recomendadas. Por ejemplo, la modificación no intencionada de las políticas de permisos asociadas a los recursos o el entorno de AWS , y el uso de cuentas privilegiadas cuyo uso debería ser escaso o nulo.

## PrivilegeEscalation

Este valor le informa de que la entidad principal implicada dentro de su entorno de AWS presenta un comportamiento que un adversario podría utilizar para obtener permisos de nivel superior para acceder a su red. Este propósito de amenaza se basa en las [tácticas de MITRE ATT&CK](#).

## Recon

Este valor indica que GuardDuty ha detectado actividad o patrones de actividad que un adversario podría utilizar al realizar un reconocimiento de su entorno para determinar cómo puede ampliar su acceso o utilizar sus recursos. Por ejemplo, esta actividad puede incluir la búsqueda de vulnerabilidades en el entorno de AWS mediante el sondeo de puertos, la realización de llamadas a API, la enumeración de usuarios y la enumeración de tablas de bases de datos, entre otras cosas.

## Stealth

Este valor indica que un adversario está intentando ocultar sus acciones de forma activa. Por ejemplo, podrían utilizar un servidor proxy anonimizador, lo que dificultaría enormemente evaluar la verdadera naturaleza de la actividad.

## Trojan

Este valor indica que un ataque está utilizando programas troyanos que llevan a cabo actividad maliciosa sigilosamente. En ocasiones, este software tiene el aspecto de un programa legítimo. A veces, los usuarios ejecutan accidentalmente este software. Otras veces, este software puede ejecutarse automáticamente mediante la explotación de una vulnerabilidad.

## UnauthorizedAccess

Este valor indica que GuardDuty se está detectando una actividad sospechosa o un patrón de actividad sospechoso por parte de una persona no autorizada.

# GuardDuty motor de escaneo de detección de malware

Amazon GuardDuty tiene un motor de escaneo creado y administrado internamente y un [proveedor externo](#). Ambos utilizan indicadores de compromiso (IoCs) procedentes de varios canales internos que permiten ver los distintos tipos de malware a los que pueden dirigirse AWS. GuardDuty también incluye definiciones de detección basadas en las reglas de YARA añadidas por nuestros ingenieros de seguridad, y detecciones basadas en modelos heurísticos y de aprendizaje automático (ML). Al escanear objetos de Amazon S3, GuardDuty Malware Protection produce resultados consistentes al escanear el mismo objeto varias veces con las mismas definiciones y motores de escaneo. Signature-based La detección no solo incluye la coincidencia de bytes, sino también un fragmento de código potencialmente complejo, y el escáner puede analizar el contenido y tomar decisiones.

El motor de análisis de malware no realiza análisis de comportamiento en vivo, en los que la detonación de malware supervisa la muestra mientras se ejecuta en un sistema real. La GuardDuty solución consiste principalmente en una detección basada en archivos. Para detectar malware sin archivos, GuardDuty proporciona una solución basada en agentes, como Amazon EKS, [Supervisión en tiempo de ejecución](#) Amazon EC2 y Amazon ECS (incluidas). AWS Fargate

Sin restricciones en cuanto a los formatos de archivo que GuardDuty escanean en busca de malware, los motores de escaneo que utiliza pueden detectar diferentes tipos de malware, como los criptomneros, el ransomware y los webshells. El motor de GuardDuty análisis, totalmente gestionado, actualiza continuamente la lista de firmas de malware cada 15 minutos.

El motor de escaneo forma parte del sistema de inteligencia de GuardDuty amenazas que utiliza un componente interno de detonación de malware. Esto permite generar nueva inteligencia sobre amenazas mediante la recopilación autónoma de muestras de malware y archivos benignos provenientes de diversos orígenes. El tipo de IoC de hash de archivo del sistema de inteligencia de amenazas se integra además con el motor de análisis de malware para detectar malware basado en hashes de archivos maliciosos conocidos.

## Generación de hallazgos de muestra en GuardDuty

Amazon le GuardDuty ayuda a generar muestras de resultados para visualizar y comprender los distintos tipos de hallazgos que puede generar. Al generar muestras de resultados, GuardDuty rellena la lista de hallazgos actual con una muestra por cada tipo de hallazgo admitido, incluidos los tipos de búsqueda de secuencias de ataques.

Las muestras generadas son aproximaciones rellenas con valores de marcador de posición. Es posible que estas muestras tengan un aspecto diferente al de los resultados reales de su entorno, pero puede utilizarlas para probar distintas configuraciones GuardDuty, como los EventBridge eventos o los filtros. Para consultar la lista de valores disponibles para los tipos de resultados, consulte la tabla [GuardDuty buscar tipos](#).

## Generar ejemplos de resultados a través de la GuardDuty consola o la API

Elija el método de acceso que prefiera para generar resultados de muestra.

### Note

La GuardDuty consola le ayuda a generar uno para cada tipo de hallazgo. Para generar uno o más tipos de búsqueda específicos, lleve a cabo los API/CLI pasos correspondientes.

### Console

Use el procedimiento siguiente para generar resultados de muestra. Este proceso genera un hallazgo de muestra para cada tipo de GuardDuty hallazgo.

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Configuración.
3. En la página Settings, en Sample findings, elija Generate sample findings.
4. En el panel de navegación, seleccione Resultados. Los resultados de muestra se muestran en la página Resultados actuales con el prefijo [SAMPLE].

### API/CLI

Puede generar una única búsqueda de muestra que coincida con cualquiera de los tipos de GuardDuty búsqueda a través de la [CreateSampleFindings](#) API; los valores disponibles para los tipos de búsqueda se muestran en [GuardDuty buscar tipos](#) la tabla.

Esto resulta útil para probar las reglas de los CloudWatch eventos o para automatizarlas en función de los resultados. En el siguiente ejemplo, se muestra cómo generar un solo resultado de muestra del tipo `Backdoor:EC2/DenialOfService.Tcp` con la AWS CLI.

Para encontrar los detectorId correspondientes a tu cuenta y a la región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
--finding-types Backdoor:EC2/DenialOfService.Tcp
```

El título de los resultados de muestra generados mediante estos métodos siempre comienza con [SAMPLE] en la consola. Los resultados de muestra tienen un valor "sample": true en la sección additionalInfo de los detalles de los resultados de JSON.

Para comprender los detalles del resultado, como la gravedad del resultado y el recurso potencialmente comprometido, asociados a los resultados generados, consulte [Niveles de gravedad de GuardDuty los hallazgos](#) y [Detalles de los resultados](#).

Para obtener algunos resultados comunes basados en una actividad simulada en un entorno específico y aislado Cuenta de AWS , consulte [Pruebe GuardDuty los resultados en cuentas dedicadas](#).

## Pruebe GuardDuty los resultados en cuentas dedicadas

Utilice este documento para ejecutar un script de prueba que genere GuardDuty resultados a partir de los recursos de prueba que se desplegarán en su Cuenta de AWS ordenador. Puede realizar estos pasos si desea comprender y obtener información sobre determinados tipos de GuardDuty hallazgos y cómo los detalles de los hallazgos buscan los recursos reales de su cuenta. Esta experiencia es diferente a la de generar [Ejemplos de hallazgos](#). Para obtener más información sobre la experiencia de probar GuardDuty los resultados, consulte [Consideraciones](#).

### Contenido

- [Consideraciones](#)
- [GuardDuty hallazgos que el script del probador puede generar](#)
- [Paso 1: Requisitos previos](#)
- [Paso 2: Despliegue AWS los recursos](#)
- [Paso 3: Ejecute los scripts de la herramienta de pruebas](#)
- [Paso 4: Limpiar los recursos AWS de prueba](#)
- [Solución de problemas comunes de](#)

## Consideraciones

Antes de continuar, tenga en cuenta las siguientes consideraciones:

- GuardDuty recomienda implementar el comprobador en un lugar dedicado que no sea Cuenta de AWS de producción. Este enfoque garantizará que pueda identificar adecuadamente los GuardDuty hallazgos generados por el evaluador. Además, el GuardDuty evaluador despliega una variedad de recursos que pueden requerir permisos de IAM más allá de lo permitido en otras cuentas. Al utilizar una cuenta dedicada, se garantiza que los permisos se puedan delimitar correctamente con un límite de cuenta claro.
- El script del evaluador genera más de 100 GuardDuty resultados con diferentes combinaciones de recursos. AWS Actualmente, esto no incluye todos los [GuardDuty buscar tipos](#). Para obtener una lista de los tipos de resultados que puede generar con este script de la herramienta de pruebas, consulte [GuardDuty hallazgos que el script del probador puede generar](#).

### Nota

Para visualizar los tipos de búsqueda de secuencias de ataque, el script del probador genera solo [AttackSequence:EKS/CompromisedCluster](#) y [AttackSequence:S3/CompromisedData](#). Para visualizar y comprender las [AttackSequence:IAM/CompromisedCredentials](#), puedes generar los [Ejemplos de hallazgos](#) en su cuenta.

- Para que el GuardDuty evaluador funcione como se espera, GuardDuty debe estar habilitado en la cuenta en la que se despliegan los recursos del evaluador. En función de las pruebas que se ejecuten, el evaluador evalúa si los planes de GuardDuty protección adecuados están habilitados o no. En el caso de cualquier plan de protección que no esté activado, GuardDuty solicitará permiso para activar los planes de protección necesarios durante el tiempo suficiente GuardDuty para realizar las pruebas que generen resultados. Más adelante, GuardDuty desactivará el plan de protección una vez que se hayan completado las pruebas.

Habilitando GuardDuty por primera vez

Cuando GuardDuty se active en tu cuenta dedicada por primera vez en una región específica, tu cuenta se inscribirá automáticamente en una prueba gratuita de 30 días.

GuardDuty ofrece planes de protección opcionales. En el momento de la activación GuardDuty, algunos planes de protección también se habilitan y se incluyen en la prueba gratuita de GuardDuty 30 días. Para obtener más información, consulte [Uso de una GuardDuty prueba gratuita de 30 días](#).

GuardDuty ya estaba activado en su cuenta antes de ejecutar el script de prueba

Cuando ya GuardDuty esté activado, el script del comprobador comprobará, en función de los parámetros, el estado de la configuración de determinados planes de protección y otros ajustes a nivel de cuenta necesarios para generar los resultados.

Al ejecutar este script de la herramienta de pruebas, es posible que ciertos planes de protección se habiliten por primera vez en la cuenta dedicada en una región. Esto iniciará la prueba gratuita de 30 días para ese plan de protección. Para obtener información sobre la prueba gratuita asociada a cada plan de protección, consulte [Uso de una GuardDuty prueba gratuita de 30 días](#).

- Mientras la infraestructura del GuardDuty comprobador esté implementada, es posible que ocasionalmente reciba [UnauthorizedAccess:EC2/TorClient](#) los resultados de la PenTest instancia.

## GuardDuty hallazgos que el script del probador puede generar

Actualmente, el script de la herramienta de pruebas genera los siguientes tipos de resultados relacionados con los registros de auditoría de Amazon EC2, Amazon EKS, Amazon S3, IAM y EKS:

- [AttackSequence:EKS/CompromisedCluster](#)
- [AttackSequence:S3/CompromisedData](#)
- [Backdoor:EC2/C&CActivity.B!DNS](#)
- [Backdoor:EC2/DenialOfService.Dns](#)
- [Backdoor:EC2/DenialOfService.Udp](#)
- [CryptoCurrency:EC2/BitcoinTool.B!DNS](#)
- [Impact:EC2/AbusedDomainRequest.Reputation](#)
- [Impact:EC2/BitcoinDomainRequest.Reputation](#)
- [Impact:EC2/MaliciousDomainRequest.Reputation](#)
- [Impact:EC2/SuspiciousDomainRequest.Reputation](#)
- [Recon:EC2/Portscan](#)
- [Trojan:EC2/BlackholeTraffic!DNS](#)
- [Trojan:EC2/DGADomainRequest.C!DNS](#)
- [Trojan:EC2/DNSDataExfiltration](#)
- [Trojan:EC2/DriveBySourceTraffic!DNS](#)

- [Trojan:EC2/DropPoint!DNS](#)
- [Trojan:EC2/PhishingDomainRequest!DNS](#)
- [UnauthorizedAccess:EC2/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:EC2/RDPBruteForce](#)
- [UnauthorizedAccess:EC2/SSHBruteForce](#)
- [PenTest:IAMUser/KaliLinux](#)
- [Recon:IAMUser/MaliciousIPCaller.Custom](#)
- [Recon:IAMUser/TorIPCaller](#)
- [Stealth:IAMUser/CloudTrailLoggingDisabled](#)
- [Stealth:IAMUser/PasswordPolicyChange](#)
- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)
- [UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:IAMUser/TorIPCaller](#)
- [Discovery:Kubernetes/MaliciousIPCaller.Custom](#)
- [Discovery:Kubernetes/SuccessfulAnonymousAccess](#)
- [Discovery:Kubernetes/TorIPCaller](#)
- [Execution:Kubernetes/ExecInKubeSystemPod](#)
- [Impact:Kubernetes/MaliciousIPCaller.Custom](#)
- [Persistence:Kubernetes/ContainerWithSensitiveMount](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [PrivilegeEscalation:Kubernetes/PrivilegedContainer](#)
- [UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom](#)
- [Discovery:S3/MaliciousIPCaller.Custom](#)
- [Discovery:S3/TorIPCaller](#)
- [PenTest:S3/KaliLinux](#)
- [Policy:S3/AccountBlockPublicAccessDisabled](#)
- [Policy:S3/BucketAnonymousAccessGranted](#)
- [Policy:S3/BucketBlockPublicAccessDisabled](#)



- [Policy:S3/BucketPublicAccessGranted](#)
- [Stealth:S3/ServerAccessLoggingDisabled](#)
- [UnauthorizedAccess:S3/MaliciousIPCaller.Custom](#)
- [UnauthorizedAccess:S3/TorIPCaller](#)
- [Backdoor:Runtime/C&CActivity.B!DNS](#)
- [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
- [DefenseEvasion:Runtime/ProcessInjection.Ptrace](#)
- [DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite](#)
- [Execution:Runtime/ReverseShell](#)
- [Impact:Runtime/AbusedDomainRequest.Reputation](#)
- [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
- [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
- [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
- [PrivilegeEscalation:Runtime/ContainerMountsHostDirectory](#)
- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#)
- [Trojan:Runtime/BlackholeTraffic!DNS](#)
- [Trojan:Runtime/DGADomainRequest.C!DNS](#)
- [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
- [Trojan:Runtime/DropPoint!DNS](#)
- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

## Paso 1: Requisitos previos

Para preparar el entorno de prueba, necesitará los siguientes elementos:

- Git: instale la herramienta de línea de comandos git en función del sistema operativo que utilice.

Esto se necesita para clonar el [repositorio de amazon-guardduty-tester](#).

- AWS Command Line Interface— Una herramienta de código abierto que permite interactuar con ella Servicios de AWS mediante comandos de la consola de la línea de comandos. Para obtener más información, consulte [Introducción a AWS CLI](#) en la Guía del usuario de AWS Command Line Interface .

- AWS Systems Manager— Para iniciar sesiones del administrador de sesiones con los nodos gestionados mediante el uso, AWS CLI debe instalar el complemento del administrador de sesiones en su máquina local. Para obtener más información, consulte [Instalar el complemento del Administrador de sesiones para AWS CLI](#) en la Guía del usuario de AWS Systems Manager
- Administrador de paquetes de nodos (NPM): instale el NPM para instalar todas las dependencias.
- Docker: debe tener Docker instalado. Para obtener instrucciones de instalación, consulte el [sitio web de Docker](#).

Para verificar que Docker ha sido instalado, ejecute el siguiente comando y confirme que hay una salida similar a la siguiente:

```
$ docker --version
Docker version 19.03.1
```

- Suscríbase a la imagen de [Kali Linux](#) en el AWS Marketplace.

## Paso 2: Despliegue AWS los recursos

Esta sección proporciona una lista de conceptos clave y los pasos para implementar determinados recursos de AWS en la cuenta dedicada.

### Conceptos

En la siguiente lista se ofrecen conceptos clave relacionados con los comandos que sirven para implementar los recursos:

- AWS Cloud Development Kit (AWS CDK)— CDK es un marco de desarrollo de software de código abierto para definir la infraestructura de la nube en el código y aprovisionarla mediante ella. CloudFormation CDK admite un par de lenguajes de programación para definir componentes en la nube reutilizables conocidos como constructos. Puedes combinarlos en pilas y aplicaciones. Luego, puede implementar sus aplicaciones de CDK para aprovisionar o CloudFormation actualizar sus recursos. Para obtener más información, consulte [¿Qué es? AWS CDK](#) en la Guía para AWS Cloud Development Kit (AWS CDK) desarrolladores.
- Bootstrapping: es el proceso de preparar el AWS entorno para su uso con. AWS CDK Antes de implementar una pila de CDK en un AWS entorno, primero se debe iniciar el entorno. Este proceso de aprovisionamiento de AWS los recursos específicos de su entorno que AWS CDK utiliza forma parte de los pasos que realizará en la siguiente sección: [Pasos para implementar los recursos AWS](#)

Para obtener más información sobre cómo funciona el arranque, consulte [Arranque](#) en la Guía del desarrollador de AWS Cloud Development Kit (AWS CDK) .

## Pasos para implementar los recursos AWS

Siga los siguientes pasos para comenzar a implementar los recursos:

1. Configure su cuenta y región AWS CLI predeterminadas, a menos que las variables de región de la cuenta dedicada se configuren manualmente en el `bin/cdk-gd-tester.ts` archivo. Para obtener más información, consulte [Entornos](#) en la Guía para desarrolladores de AWS Cloud Development Kit (AWS CDK) .
2. Ejecute los siguientes comandos para implementar los recursos:

```
git clone https://github.com/aws-labs/amazon-guardduty-tester && cd amazon-guardduty-tester
npm install
cdk bootstrap
cdk deploy
```

El último comando (`cdk deploy`) crea una CloudFormation pila en tu nombre. El nombre de esta pila es `GuardDutyTesterStack`.

Como parte de este script, GuardDuty crea nuevos recursos para generar GuardDuty resultados en tu cuenta. Además, agrega el siguiente par de clave y valor de etiqueta a las instancias de Amazon EC2:

`CreatedBy:GuardDuty Test Script`

Las instancias de Amazon EC2 también incluyen las instancias de EC2 que alojan nodos de EKS y clústeres de ECS.

### Tipos de instancias

GuardDuty está diseñado para utilizar tipos de instancias rentables que proporcionen el rendimiento mínimo necesario para llevar a cabo las pruebas satisfactoriamente. Debido a los requisitos de vCPU, el grupo de nodos de Amazon EKS requiere `t3.medium`, y debido al aumento de la capacidad de red requerida para las pruebas de resultados de DenialOfService, el nodo controlador requiere `m6i.large`. Para todas las demás

pruebas, GuardDuty utiliza el tipo de `t3.micro` instancia. Para obtener más información sobre los tipos de instancias, consulte [Tamaños disponibles](#) en la Guía de tipos de instancias de Amazon EC2.

## Paso 3: Ejecute los scripts de la herramienta de pruebas

Se trata de un proceso de dos pasos en el que primero hay que iniciar una sesión con el controlador de prueba y, a continuación, ejecutar los scripts para generar GuardDuty resultados con combinaciones de recursos específicas.

### Parte A: Iniciar una sesión con el controlador de la prueba

1. Una vez implementados los recursos, guarde el código de la región en una variable de la sesión de terminal actual. Usa el siguiente comando y `us-east-1` sustitúyelo por el código de región en el que desplegaste los recursos:

```
$ REGION=us-east-1
```

2. El script de prueba solo está disponible a través de AWS Systems Manager (SSM). Para iniciar un shell interactivo en la instancia host del probador, consulte el host. `InstanceId`
3. Utilice el siguiente comando para iniciar la sesión para el script de la herramienta de pruebas:

```
aws ssm start-session
  --region $REGION
  --document-name AWS-StartInteractiveCommand
  --parameters command="cd /home/ssm-user/py_tester && bash -l"
  --target $(aws ec2 describe-instances
    --region $REGION
    --filters "Name=tag:Name,Values=Driver-GuardDutyTester"
    --query "Reservations[].Instances[?State.Name=='running'].InstanceId"
    --output text)
```

### Parte B: Generar resultados

El script del probador es un Python-based programa que crea dinámicamente un script bash para generar resultados a partir de los datos introducidos. Tiene la flexibilidad de generar conclusiones en función de uno o más tipos de AWS recursos, planes de GuardDuty protección [Propósitos de](#)

[amenaza](#) (tácticas) o. [Orígenes de datos fundamentales](#) the section called “GuardDuty hallazgos que el script del probador puede generar”

Utilice los siguientes ejemplos de comandos como referencia y ejecute uno o varios comandos para generar los resultados que desee explorar:

```
python3 guardduty_tester.py
python3 guardduty_tester.py --all
python3 guardduty_tester.py --s3
python3 guardduty_tester.py --tactics discovery
python3 guardduty_tester.py --ec2 --eks --tactics backdoor policy execution
python3 guardduty_tester.py --eks --runtime only
python3 guardduty_tester.py --ec2 --runtime only --tactics impact
python3 guardduty_tester.py --log-source dns vpc-flowlogs
python3 guardduty_tester.py --finding 'CryptoCurrency:EC2/BitcoinTool.B!DNS'
```

Para obtener más información sobre los parámetros válidos, puede ejecutar el siguiente comando de ayuda:

```
python3 guardduty_tester.py --help
```

## Parte C: Revise los resultados generados

Elija el método que prefiera para ver los resultados generados en la cuenta.

### GuardDuty console

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Resultados.
3. En la tabla de resultados, seleccione el resultado del que desea ver los detalles. Se abrirá el panel de detalles del resultado. Para obtener información, consulte [Comprender y generar los GuardDuty hallazgos de Amazon](#).
4. Si desea filtrar estos resultados, utilice la clave y el valor de la etiqueta del recurso. Por ejemplo, para filtrar los resultados generados para las instancias de Amazon EC2, utilice el par de clave y valor de etiqueta CreatedBy:GuardDuty Test Script para la Clave de etiqueta de instancia y Clave de etiqueta de instancia.

## API

- Corre [ListFindings](#) para ver los resultados de un ID de detector específico. Puede especificar parámetros para filtrar resultados.

Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

## AWS CLI

- Ejecuta el siguiente AWS CLI comando para ver los resultados generados `us-east-1` y sustitúyelos `12abc34d567e8fa901bc2d34EXAMPLE` por los valores adecuados:

```
aws guardduty list-findings --region us-east-1 --detector-id 12abc34d567e8fa901bc2d34EXAMPLE
```

Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

Para obtener más información sobre los parámetros que puede utilizar para filtrar los resultados, consulte [list-findings](#) en la Referencia de comandos de AWS CLI .

## Paso 4: Limpiar los recursos AWS de prueba

La configuración a nivel de cuenta y otras actualizaciones del estado de la configuración realizadas durante [Paso 3: Ejecute los scripts de la herramienta de pruebas](#) vuelven al estado original cuando finaliza el script de la herramienta de pruebas.

Después de ejecutar el script del probador, puede optar por limpiar los recursos de la AWS prueba. Para ello, puede optar por uno de los siguientes métodos:

- Use el siguiente comando:

```
cdk destroy
```

- Elimine la CloudFormation pila con el nombre `GuardDutyTesterStack`. Para obtener información sobre los pasos, consulte [Eliminar una pila en la CloudFormation consola](#).

## Solución de problemas comunes de

GuardDuty ha identificado los problemas más comunes y recomienda los siguientes pasos para solucionarlos:

- `Cloud assembly schema version mismatch`— Actualice la AWS CDK CLI a una versión compatible con la versión de ensamblaje en la nube requerida o a la última versión disponible. Para obtener más información, consulte [Compatibilidad de la CLI con AWS CDK](#).
- `Docker permission denied`: agregue el usuario de la cuenta dedicada a los docker o docker-users de modo que la cuenta dedicada pueda ejecutar los comandos. Para obtener más información sobre los pasos, consulte la [opción de socket Daemon](#).
- `Your requested instance type is not supported in your requested Availability Zone`: algunas zonas de disponibilidad no admiten determinados tipos de instancias. Para identificar qué zonas de disponibilidad son compatibles con el tipo de instancia que prefiera y volver a intentar implementar AWS los recursos, lleve a cabo los siguientes pasos:
  1. Elija el método que prefiera para determinar qué zonas de disponibilidad admiten el tipo de instancia:

### Console

Para identificar las zonas de disponibilidad que admiten el tipo de instancia de su preferencia

1. Inicie sesión en la consola Amazon EC2 Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/ec2/>
2. Con el selector de AWS regiones situado en la esquina superior derecha de la página, elija la región en la que desee lanzar la instancia.
3. En el panel de navegación, en Instancias, seleccione Tipos de instancias.
4. Elija el tipo de instancia de su preferencia de la tabla Tipos de instancias.
5. En Redes, consulte las regiones enumeradas en Zonas de disponibilidad.

Según esta información, es posible que tenga que elegir una nueva región en la que implementar los recursos.

### AWS CLI

Ejecute el siguiente comando para ver una lista de las zonas de disponibilidad. Asegúrese de especificar el tipo de instancia que prefiera y la región (*us-east-1*).

```
aws ec2 describe-instance-type-offerings --location-type availability-zone --  
filters Name=instance-type,Values=Preferred instance type --region us-east-1 --  
output table
```

Para obtener más información sobre este comando, consulte [describe-instance-type-offerings](#) en la Referencia de comandos de la AWS CLI .

Al ejecutar este comando, si se produce un error, asegúrese de que utiliza la versión más reciente de la AWS CLI. Para obtener más información, consulte [Solución de problemas](#) en la Guía del usuario de AWS Command Line Interface .

2. Intente volver a implementar los AWS recursos y especifique una zona de disponibilidad que sea compatible con el tipo de instancia que prefiera.

Para volver a intentar implementar AWS los recursos

1. Configure la región predeterminada en el archivo `bin/cdk-gd-tester.ts`.
2. Para especificar la zona de disponibilidad, abra el archivo `amazon-guardduty-tester/lib/common/network/vpc.ts`.
3. En este archivo, sustituya `maxAzs: 2`, por `availabilityZones: ['us-east-1a', 'us-east-1c']`, donde debe especificar las zonas de disponibilidad para el tipo de instancia.
4. Continúe con los pasos restantes en [Pasos para implementar los recursos AWS](#).

## Visualización de los hallazgos generados en la consola GuardDuty

Cuando GuardDuty detecta una actividad que coincide con el patrón de un problema de seguridad, GuardDuty genera un hallazgo. Este resultado está asociado a un tipo de recurso que puede haberse visto comprometido durante esta actividad. Puede ver los detalles asociados a cada hallazgo que se GuardDuty genere.

Si utiliza una cuenta de GuardDuty administrador, puede ver los resultados generados en nombre de las cuentas de los miembros. Sin embargo, una cuenta de miembro puede ver los resultados generados en su propia cuenta. Una cuenta de miembro no puede ver los resultados generados por otras cuentas de miembro.



## Pasos para ver los resultados en la GuardDuty consola

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Resultados.

GuardDuty muestra los resultados en formato tabular. De forma predeterminada, esta tabla se ordena en orden decreciente según el valor de la columna Vista por última vez y muestra los resultados más recientes en la parte superior.

Los resultados con el icono de una espada



representan un resultado de la secuencia de ataque.

3. Para ver los detalles asociados a un resultado, seleccione su título. Se abrirá el panel lateral de detalles del resultado. Para los resultados de una secuencia de ataque, este panel lateral incluye una versión resumida de la secuencia de ataque y, para ampliar esta vista, seleccione Ver detalles.

Para obtener información acerca de los campos que aparecen en este panel lateral, consulte [Detalles de los resultados](#).

4. (Opcional) para descargar resultados JSON
  - a. Seleccione el resultado y, a continuación, elija el menú Acciones.
  - b. En el menú Acciones, elija Exportar.
  - c. En la ventana Resultados JSON, seleccione Descargar.

### Note

En algunos casos, GuardDuty se da cuenta de que algunos resultados son falsos positivos una vez generados. GuardDuty proporciona un campo de confianza en el JSON del hallazgo y establece su valor en cero. De esta GuardDuty forma, sabrá que puede ignorar estos hallazgos de forma segura.

Los resultados sin el campo Confianza no se consideran falsos positivos.

## Navegación en la página Resultados

Esta sección proporciona información clave sobre varios elementos de la página Resultados. Esto le ayudará a analizar los resultados generados para analizar las amenazas y responder a ellas.

En la siguiente lista se explican los elementos de la página Resultados que le ayudarán a comprender mejor los resultados generados:

- Tipo de amenaza:

El tipo de amenaza incluye GuardDuty los hallazgos individuales y los hallazgos de la secuencia de ataque. De forma predeterminada, la página muestra Todos los resultados.

Para filtrar la vista de la tabla de resultados, en el menú Tipo de amenaza, seleccione una de las opciones: Solo resultados de la secuencia de ataque o Solo resultados individuales.

- Columnas de recursos y recuento:

La columna Recursos de la tabla de hallazgos muestra el nombre del AWS recurso potencialmente comprometido. Para encontrar una secuencia de ataque, esta columna muestra la cantidad de AWS recursos potencialmente comprometidos. Para ver los nombres de los recursos, seleccione el número que aparece en la columna Recurso.

La columna Recuento indica el número de veces GuardDuty que se observa un hallazgo específico. Cuando GuardDuty detecta que una actividad coincide con un problema de seguridad identificado anteriormente, aumenta el recuento de ese hallazgo específico. En el caso de un resultado de la secuencia de un ataque, el valor de esta columna indica el número total de señales y resultados involucrados en la generación del resultado.

- Clasificación de los resultados por columnas de la tabla:

Si hay una flecha junto al encabezado de una columna, puede ordenar la tabla de resultados en función de la columna. Seleccione el encabezado de la columna para ordenar los resultados en orden creciente o decreciente según el valor de esa columna.

- Filtrado de resultados:

En función de atributos de propiedad específicos, como Account ID y Resource type, puede filtrar aún más la tabla de resultado. Para obtener más información sobre los tipos de filtros que puede utilizar, consulte [Filtrar GuardDuty los hallazgos](#).

- Reglas de estado y guardadas:

El menú Estado incluye dos valores: Actual y Archivado. La vista predeterminada es resultados actuales en la tabla.

Cuando ya no desee GuardDuty generar un resultado que coincida con un criterio específico, puede suprimirlo. GuardDuty archiva ese hallazgo. Cuando vuelva a GuardDuty detectar este hallazgo, no se le notificará esta observación. Para ver específicamente los resultados archivados, en el menú de estado, seleccione Archivado.

Las reglas guardadas son una característica que le ayuda a filtrar automáticamente los resultados que coinciden con un criterio específico y a tomar medidas al respecto. Las acciones pueden incluir archivar los resultados o suprimirlos de futuras notificaciones.

Para obtener más información, consulte [Reglas de supresión](#).

## Niveles de gravedad de GuardDuty los hallazgos

Cada GuardDuty hallazgo tiene un nivel de gravedad y un valor asignados que reflejan el riesgo potencial que el hallazgo podría suponer para su entorno, según lo determinen nuestros ingenieros de seguridad. El valor de la gravedad puede estar comprendido en cualquier lugar dentro del intervalo de 1,0 a 10,0, donde los valores superiores indican un mayor riesgo de seguridad. Para ayudarlo a determinar la respuesta a un posible problema de seguridad que se destaque en un hallazgo, GuardDuty desglosa este rango en niveles de gravedad crítica, alta, media y baja.

Un resultado de un tipo concreto puede tener una gravedad diferente según el contexto específico del resultado. Para ver una lista consolidada de los niveles de gravedad predeterminados para todos los tipos de GuardDuty hallazgos, consulte [GuardDuty tipos de búsqueda activos](#).

En las siguientes secciones se explican los niveles de gravedad definidos para los GuardDuty hallazgos.

### Temas

- [Gravedad crítica](#)
- [Gravedad alta](#)
- [Gravedad media](#)
- [Gravedad baja](#)

## Gravedad crítica

Rango de valores: 9,0 - 10,0

Descripción: un nivel de gravedad crítico indica que una secuencia de ataque puede estar en curso o haber ocurrido recientemente. Uno o más AWS recursos, como las credenciales de inicio de sesión de los usuarios de IAM y el bucket de Amazon S3, pueden estar en peligro o ya lo están.

Recomendación: GuardDuty recomienda priorizar la clasificación y la corrección de todos los hallazgos de gravedad crítica, ya que estos problemas pueden ser parte de un ataque de ransomware y agravarse en cualquier momento. Consulte los detalles sobre los recursos involucrados y comience a abordar los problemas de seguridad. Para obtener más información, consulte [Corrección de resultados](#).

## Gravedad alta

Rango de valores: 7,0 - 8,9

Descripción: un nivel de seguridad alto indica que el recurso en cuestión (una instancia de Amazon EC2 o un conjunto de credenciales de inicio de sesión de usuarios de IAM) está en peligro y que se está utilizando activamente para fines no autorizados.

Recomendación: le GuardDuty recomienda que dé prioridad a cualquier problema de seguridad grave relacionado con la detección de problemas de seguridad y que tome medidas correctivas de inmediato para evitar un mayor uso no autorizado de sus recursos. Por ejemplo, limpie la instancia de Amazon EC2 o termínela, o rote las credenciales de IAM. Siga los pasos que se indican [Corrección de resultados](#) para corregir el resultado.

## Gravedad media

Rango de valores: 4,0 - 6,9

Descripción: un nivel de gravedad mediano indica una actividad sospechosa que se desvía del comportamiento observado normalmente y, en función de su caso de uso, puede ser indicativo de un peligro para los recursos.

Recomendación: GuardDuty recomienda investigar el recurso potencialmente afectado lo antes posible. Los pasos de corrección variarán según el recurso y la familia de resultados. Un enfoque establecido consiste en confirmar que la actividad está autorizada y es coherente con su caso de

uso. Si no puede identificar la causa o confirmar que la actividad está autorizada, debería considerar el recurso como afectado. Siga los pasos que se indican [Corrección de resultados](#) para corregir el resultado.

Estas son algunas cosas a tener en cuenta al revisar un resultado de nivel mediano:

- Compruebe si un usuario autorizado ha instalado nuevo software que haya cambiado el comportamiento de un recurso (por ejemplo, permitir un tráfico superior al normal o habilitar la comunicación en un nuevo puerto).
- Verifique si un usuario autorizado cambió la configuración del plano de control; por ejemplo, si modificó la configuración de un grupo de seguridad.
- Ejecute un examen antivirus en el recurso implicado para detectar software no autorizado.
- Verifique los permisos asociados al rol de IAM, usuario, grupo o conjunto de credenciales implicados. Tal vez sea necesario cambiarlos o moverlos.

## Gravedad baja

Rango de valores: 1,0 - 3,9

Descripción: un nivel de gravedad bajo indica un intento de actividad sospechosa que no puso en peligro el entorno; por ejemplo, un análisis de puerto o un intento fallido de intrusión.

Recomendación: no hay ninguna acción recomendada inmediata, pero vale la pena tomar nota de esta información ya que puede indicar que alguien busca puntos débiles en el entorno.

## Detalles de los resultados

En la GuardDuty consola de Amazon, puedes ver los detalles de búsqueda en la sección de resumen de búsquedas. Los detalles de los resultados varían según el tipo de resultado.

Hay dos detalles principales que determinarán qué tipo de información está disponibles para cualquier resultado. El primero es el tipo de recurso, que puede ser Instance, AccessKey, S3Bucket, S3Object, Kubernetes cluster, ECS cluster, Container, RDSDBInstance, RDSLimitlessDB o Lambda. El segundo detalle que determina la información de los resultados es el rol del recurso. El rol del recurso puede ser Target, lo que significa que el recurso fue el blanco de una actividad sospechosa. En el caso de resultados por tipo de instancia, el rol del recurso también puede ser Actor, lo que significa que el recurso fue el actor que ha llevado a cabo la

actividad sospechosa. En este tema, se describen algunos de los detalles de los resultados que se encuentran disponibles con más frecuencia. Para [the section called “Tipos de resultados de la supervisión en tiempo de ejecución”](#) y [Tipo de resultado de la protección contra malware para S3](#), no se ha completado el rol del recurso.

## Temas

- [Información general de los resultados](#)
- [Recurso](#)
- [Detalles de los resultados de la secuencia de ataque](#)
- [Detalles de usuario de la base de datos \(DB\) de RDS](#)
- [Detalles del resultado de la supervisión en tiempo de ejecución](#)
- [Detalles del análisis de volúmenes de EBS](#)
- [Detalles de los resultados de Malware Protection for EC2](#)
- [Detalles de los resultados de la protección contra malware para S3](#)
- [Action](#)
- [Actor u objetivo](#)
- [Detalles de geolocalización](#)
- [Información adicional](#)
- [Evidencia](#)
- [Comportamiento anómalo](#)

## Información general de los resultados

La sección Información general de un resultado contiene las características identificativas más básicas del resultado, incluida la siguiente información:

- ID de cuenta: el ID de la AWS cuenta en la que se llevó GuardDuty a cabo la actividad que provocó la generación de este hallazgo.
- Recuento: el número de veces que GuardDuty se ha agregado una actividad que coincide con este patrón con este identificador de búsqueda.
- Hora de creación: fecha y hora en que se ha creado este resultado por primera vez. Si este valor difiere de Hora de actualización, indica que la actividad se ha producido varias veces y es un problema continuo.

 Note

Las marcas de tiempo de las búsquedas en la GuardDuty consola aparecen en la zona horaria local, mientras que las exportaciones de JSON y las salidas de CLI muestran las marcas de tiempo en UTC.

- ID de resultado: un identificador único para este tipo de resultado y conjunto de parámetros. Las nuevas ocurrencias de actividad que coincidan con este patrón se añadirán al mismo ID.
- Tipo de resultado: una cadena formateada que representa el tipo de actividad que ha desencadenado el resultado. Para obtener más información, consulte [GuardDuty formato de búsqueda](#).
- Región: la AWS región en la que se generó el hallazgo. Para obtener más información acerca de las regiones admitidas, consulte [Regiones y puntos de conexión](#).
- ID de recurso: el ID del AWS recurso con el que se llevó GuardDuty a cabo la actividad que provocó la generación de este hallazgo.
- ID de escaneo: se aplica a los hallazgos cuando la protección contra GuardDuty malware para EC2 está habilitada y es un identificador del análisis de malware que se ejecuta en los volúmenes de EBS conectados a la carga de trabajo de la instancia de EC2 o del contenedor potencialmente comprometida. Para obtener más información, consulte [Detalles de los resultados de Malware Protection for EC2](#).
- Gravedad: un nivel de gravedad crítica, alta, mediana o baja asignado al resultado. Para obtener más información, consulte [Niveles de gravedad de los resultados](#).
- Actualizado el: la última vez que se actualizó este hallazgo con una nueva actividad que coincidía con el patrón que llevó GuardDuty a generarlo.

## Recurso

El recurso afectado proporciona detalles sobre el AWS recurso al que se dirigió la actividad iniciadora. La información disponible variará según el tipo de recurso y el tipo de acción.

Función de recurso: la función del AWS recurso que inició la búsqueda. Este valor puede ser TARGET o ACTOR y representa si su recurso era el objetivo de la actividad sospechosa o si era el actor que ha llevado a cabo la actividad sospechosa, respectivamente.

Tipo de recurso: el tipo del recurso afectado. Si estuvieron involucrados varios recursos, un resultado puede incluir varios tipos de recursos. Los tipos de recursos son Instance, S3Bucket AccessKey, S3Object, ECSCluster, Container KubernetesCluster, RDSDBInstance, RDSLimitlessDB y Lambda. En función del tipo de recurso, habrá distintos detalles disponibles sobre el resultado. Seleccione una pestaña de opciones de recurso para obtener información sobre los detalles disponibles de ese recurso.

## Instance

Detalles de la instancia:

### Note

Es posible que falten algunos detalles de la instancia si esta ya se ha detenido o si la invocación a la API subyacente se ha originado en una instancia de EC2 en una región diferente al hacer una llamada a la API entre regiones.

- ID de instancia: el ID de la instancia de EC2 implicada en la actividad que provocó la generación del hallazgo. GuardDuty
- Tipo de instancia: el tipo de instancia de EC2 implicada en el resultado.
- Hora de lanzamiento: la fecha y hora en que se lanzó la instancia.
- Outpost ARN: el nombre del recurso de Amazon (ARN) de. AWS Outposts Solo se aplica a las instancias. AWS Outposts Para obtener más información, consulte [¿Qué es AWS Outposts?](#) en la Guía del usuario de bastidores Outposts.
- Nombre del grupo de seguridad: el nombre del grupo de seguridad asociado a la instancia en cuestión.
- ID del grupo de seguridad: el ID del grupo de seguridad asociado a la instancia en cuestión.
- Estado de la instancia: el estado actual de la instancia afectada.
- Zona de disponibilidad: la zona de disponibilidad de la región de AWS en la que se encuentra la instancia en cuestión.
- ID de imagen: el ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.
- Descripción de la imagen: una descripción del ID de la imagen de máquina de Amazon utilizada para crear la instancia implicada en la actividad.



- Etiquetas: una lista de etiquetas adjuntas a este recurso, enumeradas en el formato de key-value.

## AccessKey

Detalles de la clave de acceso:

- ID de clave de acceso: ID de clave de acceso del usuario que participó en la actividad GuardDuty que provocó la generación del hallazgo.
- ID principal: el ID principal del usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo.
- Tipo de usuario: el tipo de usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo. Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).
- Nombre de usuario: el nombre del usuario que participó en la actividad que provocó GuardDuty la generación del hallazgo.

## S3Bucket

Detalles del bucket de Amazon S3:

- Nombre: el nombre del bucket implicado en el resultado.
- ARN: el ARN del bucket implicado en el resultado.
- Propietario: el ID canónico del usuario propietario del bucket implicado en el resultado. Para más información acerca de los ID de usuario canónico, consulte [AWS account identifiers](#).
- Tipo: el tipo de resultado del bucket, que puede ser de Destino o de Origen.
- Cifrado predeterminado del servidor: los detalles de cifrado del bucket.
- Etiquetas del bucket: una lista de etiquetas asociadas a este recurso, enumeradas en el formato de key-value.
- Permisos efectivos: una evaluación de todos los permisos y políticas efectivos del bucket que indica si el bucket en cuestión está expuesto públicamente. Los valores pueden ser Público o No público.

## S3Object

- Detalles del objeto de S3: incluye la siguiente información sobre el objeto de S3 analizado:

- ARN: nombre de recurso de Amazon (ARN) del objeto de S3 analizado.
- Clave: el nombre asignado al archivo cuando se creó en el bucket de S3.
- ID de versión: si ha habilitado el control de versiones del bucket, este campo indica el identificador de versión asociado a la versión más reciente del objeto de S3 analizado. Para obtener más información, consulte [Uso del control de versiones en buckets de S3](#) en la Guía de usuario de Amazon S3.
- eTag: representa la versión específica del objeto de S3 analizado.
- Hash: hash de la amenaza detectada en este resultado.
- Detalles del bucket de S3: incluye la siguiente información sobre el bucket de Amazon S3 asociado al objeto de S3 analizado:
  - Nombre: indica el nombre del bucket de S3 que contiene el objeto.
  - ARN: el nombre de recurso de Amazon (ARN) del bucket de S3.
- Propietario: ID canónico del propietario del bucket de S3.

## EKSCluster

Detalles del clúster de Kubernetes:

- Nombre: el nombre del clúster de Kubernetes.
- ARN: el ARN que identifica al clúster.
- Hora de creación: fecha y hora en que se ha creado este clúster.

### Note

Las marcas de tiempo de las búsquedas en la GuardDuty consola aparecen en la zona horaria local, mientras que las exportaciones de JSON y las salidas de CLI muestran las marcas de tiempo en UTC.

- ID de VPC: el ID de la VPC asociada al clúster.
- Estado: el estado actual del clúster.
- Etiquetas: los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato `key-value`. Puede definir tanto la clave como el valor.

Las etiquetas del clúster no se propagan a ningún otro recurso asociado al clúster.

### Detalles de la carga de trabajo de Kubernetes:

- Tipo: el tipo de carga de trabajo de Kubernetes, como el pod, la implementación y el trabajo.
- Nombre: el nombre de la carga de trabajo de Kubernetes.
- Uid: el ID único de la carga de trabajo de Kubernetes.
- Hora de creación: fecha y hora en que se ha creado esta carga de trabajo.
- Etiquetas: los pares de clave-valor asociados a la carga de trabajo de Kubernetes.
- Contenedores: los detalles del contenedor que se ejecuta como parte de la carga de trabajo de Kubernetes.
- Espacio de nombres: la carga de trabajo pertenece a este espacio de nombres de Kubernetes.
- Volúmenes: los volúmenes que utiliza la carga de trabajo de Kubernetes.
  - Ruta del host: representa un archivo o directorio preexistente en la máquina host al que se asigna el volumen.
  - Nombre: el nombre del volumen.
- Contexto de seguridad del pod: define la configuración de privilegios y control de acceso para todos los contenedores de un pod.
- Red de host: se establece como `true` si los pods se han incluido en la carga de trabajo de Kubernetes.

### Detalles de usuario de Kubernetes:

- Grupos: grupos de RBAC (control basado en el acceso a roles) de Kubernetes del usuario que ha participado en la actividad que generó el resultado.
- ID: el ID única del usuario de Kubernetes.
- Nombre de usuario: nombre del usuario de Kubernetes que ha participado en la actividad que generó el resultado.
- Nombre de sesión: entidad que ha asumido el rol de IAM con los permisos de RBAC de Kubernetes.

## ECSCluster

### Detalles del clúster de ECS:

- ARN: el ARN que identifica al clúster.

- Nombre: el nombre del clúster.
- Estado: el estado actual del clúster.
- Recuento de servicios activos: la cantidad de servicios que se ejecutan en el clúster en un estado ACTIVE. Puedes ver estos servicios con [ListServices](#)
- Recuento de instancias de contenedor registradas: el número de instancias de contenedor registradas en el clúster. Esto incluye las instancias de contenedor tanto en estado ACTIVE como DRAINING.
- Recuento de tareas en ejecución: el número de tareas del clúster que se encuentran en estado RUNNING.
- Etiquetas: los metadatos que se aplican a los clústeres para ayudarle a categorizarlos y organizarlos. Cada etiqueta consta de una clave y un valor opcional, mostrada en el formato key-value. Puede definir tanto la clave como el valor.
- Contenedores: los detalles sobre el contenedor asociado a la tarea:
  - Nombre del contenedor: el nombre del contenedor.
  - Imagen del contenedor: la imagen del contenedor.
- Detalles de la tarea: los detalles de una tarea en un clúster.
  - ARN: el nombre de recurso de Amazon (ARN) de la tarea.
  - ARN de definición: el nombre de recurso de Amazon (ARN) de la definición de tarea que crea esta.
  - Versión: el contador de versiones de la tarea.
  - Hora de creación de la tarea: la marca de tiempo de Unix en la que se ha creado la tarea.
  - Hora de inicio de la tarea: la marca de tiempo de Unix cuando se ha iniciado la tarea.
  - Tarea iniciada por: la etiqueta especificada cuando se inicia una tarea.

## Container

### Detalles del contenedor:

- Tiempo de ejecución del contenedor: el tiempo de ejecución del contenedor (por ejemplo, docker o containerd) utilizado para ejecutar el contenedor.
- ID: el ID de la instancia de contenedor o las entradas de ARN completas de la instancia de contenedor.
- Nombre: el nombre del contenedor.

- Imagen: la imagen de la instancia de contenedor.
- Monturas de volumen: lista de monturas de volumen de contenedores. Un contenedor puede montar un volumen en su sistema de archivos.
- Contexto de seguridad: el contexto de seguridad de contenedor define la configuración de privilegios y control de acceso de un contenedor.
- Detalles del proceso: describe los detalles del proceso asociado al resultado.

## RDSDBInstance

Detalles de RDSDBInstance:

### Note

Este recurso está disponible en los resultados de RDS Protection relacionados con la instancia de base de datos.

- ID de instancia de base de datos: el identificador asociado a la instancia de base de datos que participó en la GuardDuty búsqueda.
- Motor: el nombre del motor de base de datos de la instancia de base de datos implicada en el resultado. Los valores posibles son Aurora MySQL-Compatible o Aurora PostgreSQL-Compatible.
- Versión del motor: la versión del motor de base de datos que participó en la GuardDuty búsqueda.
- ID del clúster de base de datos: el identificador del clúster de base de datos que contiene el ID de la instancia de base de datos implicada en la GuardDuty búsqueda.
- ARN de instancia de base de datos: el ARN que identifica la instancia de base de datos implicada en el hallazgo. GuardDuty

## RDSLimitlessDB

Detalles de RDSLimitlessDB:

Este recurso está disponible en los resultados de RDS Protection relacionados con la versión de motor compatible de Limitless Database.

- Identificador del grupo de partición de base de datos: el nombre asociado al grupo de partición de base de datos Limitless.
- ID de recurso del grupo de partición de base de datos: el identificador de recursos del grupo de partición de base de datos dentro de la base de datos Limitless.
- ARN del grupo de partición de base de datos: nombre de recurso de Amazon (ARN) que identifica el grupo de partición de base de datos.
- Motor: el identificador de la base de datos Limitless implicada en los resultados.
- Versión de motor: la versión del motor de la base de datos Limitless.
- Identificador del clúster de base de datos: nombre del clúster de base de datos que forma parte de la base de datos Limitless.

Para obtener información sobre los detalles de usuario y de autenticación de la base de datos potencialmente afectada, consulte [Detalles de usuario de la base de datos \(DB\) de RDS](#).

## Lambda

### Detalles de la función de Lambda

- Nombre de la función: el nombre de la función de Lambda implicada en el resultado.
- Versión de la función: la versión de la función de Lambda implicada en el resultado.
- Descripción de la función: una descripción de la función de Lambda implicada en el resultado.
- ARN de la función: el nombre de recurso de Amazon (ARN) de la función de Lambda implicada en el resultado.
- ID de revisión: el ID de revisión de la versión de la función de Lambda.
- Rol: el rol de ejecución de la función de Lambda implicada en el resultado.
- Configuración de VPC: la configuración de Amazon VPC, que incluye el ID de VPC, el grupo de seguridad y los ID de subred asociados a la función de Lambda.
  - ID de VPC: el ID de Amazon VPC asociada a la función de Lambda implicada en el resultado.
  - ID de subred: los ID de las subredes asociadas a la función de Lambda.
  - Grupo de seguridad: el grupo de seguridad asociado a la función de Lambda implicada. Esto incluye el nombre del grupo de seguridad y el ID de grupo.
- Etiquetas: una lista de etiquetas adjuntas a este recurso, con el formato de pares de key-value.

## Detalles de los resultados de la secuencia de ataque

GuardDuty proporciona detalles de cada hallazgo que genere en su cuenta. Estos detalles ayudan a entender los motivos del resultado. Esta sección se centra en los detalles relacionados con [Tipos de resultados de secuencias de ataque](#). Esto incluye información como los recursos potencialmente afectados, el cronograma de los eventos, los indicadores, las señales y los puntos de conexión involucrados en el resultado.

Para ver los detalles asociados a las señales que son GuardDuty hallazgos, consulta las secciones correspondientes de esta página.

En la GuardDuty consola, al seleccionar una secuencia de ataque, el panel lateral de detalles se divide en las siguientes pestañas:

- **Descripción general:** proporciona una vista compacta de los detalles de la secuencia de ataque, incluidas las señales, las tácticas de MITRE y los recursos potencialmente afectados.
- **Señales:** muestra una cronología de los eventos que intervienen en una secuencia de ataque.
- **Recursos:** proporciona información sobre los recursos potencialmente afectados o los recursos que están potencialmente en riesgo.

La siguiente lista proporciona descripciones asociadas a los detalles de resultados de la secuencia de ataque.

### Señales

Una señal puede ser una actividad de la API o un hallazgo que se GuardDuty utiliza para detectar una secuencia de ataque. GuardDuty analiza las señales débiles que no se presentan como una amenaza clara, las agrupa y las correlaciona con los hallazgos generados individualmente. Para obtener más contexto, la pestaña Señales proporciona una cronología de las señales, tal como se observa en. GuardDuty

Cada señal, es decir, un GuardDuty hallazgo, tiene su propio nivel de gravedad y valor asignado. En la GuardDuty consola, puede seleccionar cada señal para ver los detalles asociados.

### Actores

Proporciona detalles sobre los actores de las amenazas en una secuencia de ataque. Para obtener más información, consulte [Actor](#) in Amazon GuardDuty API Reference.

## Puntos de conexión

Proporciona detalles sobre los puntos de conexión de la red que se utilizaron en esta secuencia de ataque. Para obtener más información, consulta [NetworkEndpoint](#) Amazon GuardDuty API Reference. Para obtener información sobre cómo se GuardDuty determina la ubicación, consulte [Detalles de geolocalización](#).

## Indicadores

Incluye datos observados que coinciden con el patrón de un problema de seguridad. Estos datos especifican por qué GuardDuty hay indicios de una actividad potencialmente sospechosa. Por ejemplo, cuando el nombre del indicador es `HIGH_RISK_API`, indica que se trata de una acción que suelen utilizar los actores de amenazas o de una acción delicada que puede tener un impacto potencial en una Cuenta de AWS persona, como acceder a las credenciales o modificar un recurso.

En la siguiente tabla se incluye una lista de indicadores potenciales y sus descripciones:

| Nombre del indicador             | Description (Descripción)                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ATTACK_TACTIC</code>       | Las tácticas MITRE utilizadas por el actor de la amenaza en una secuencia de ataque. Algunos ejemplos son Discovery e Impact.                                                                                                                                                                    |
| <code>ATTACK_TECHNIQUE</code>    | La técnica MITRE utilizada por el actor de la amenaza en una secuencia de ataque. Algunos ejemplos incluyen acceder a los recursos y utilizarlos de forma no deseada, y explotar las vulnerabilidades.                                                                                           |
| <code>CRYPTOMINING_DOMAIN</code> | Indica un nombre de dominio asociado a los grupos o a la infraestructura de minería de criptomonedas. Por ejemplo, las consultas de DNS o las conexiones a estos dominios desde entornos de contenedores o de Kubernetes pueden indicar una actividad de minería de criptomonedas no autorizada. |
| <code>CRYPTOMINING_IP</code>     | Indica una dirección IP asociada a los grupos o a la infraestructura de minería de criptomonedas. Por ejemplo, las conexiones a estas direcciones desde entornos de contenedores o de Kubernetes pueden indicar una actividad de minería de criptomonedas no autorizada.                         |



| Nombre del indicador | Description (Descripción)                                                                                                                                                                                                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CRYPTOMINING_PROCESS | Indica un proceso identificado como software de minería de criptomonedas que se ejecuta en entornos de contenedores o de Kubernetes. Por ejemplo, estos procesos pueden consumir recursos de CPU excesivos.                                                                                                                                        |
| HIGH_RISK_API        | La AWS API que incluye el Servicio de AWS nombre e eventName indica una acción que suelen utilizar los actores de amenazas o es una acción confidencial que puede tener un impacto potencial en una de ellas Cuenta de AWS, como el acceso a una credencial o la modificación de un recurso.                                                       |
| MALICIOUS_DOMAIN     | Indica un nombre de dominio con información sobre posibles inteligencia de amenazas que indica una intención maliciosa. Por ejemplo, esto incluye los servidores de comando y control (C&C), los sitios de distribución de malware o los dominios de suplantación de identidad a los que se accede desde entornos de contenedores o de Kubernetes. |
| MALICIOUS_FILE       | Indica un archivo sospechoso de ser malicioso en función de la información sobre amenazas o un análisis del comportamiento. Por ejemplo, esto incluye los archivos binarios de malware conocidos, los scripts maliciosos o los ejecutables no autorizados.                                                                                         |
| MALICIOUS_IP         | La dirección IP tiene inteligencia de amenazas confirmada que indica una intención maliciosa.                                                                                                                                                                                                                                                      |
| MALICIOUS_PACKAGE    | Indica que un recurso implicado en la secuencia de ataque contiene un paquete de software identificado como malicioso. Los valores del indicador incluyen identificadores de paquetes maliciosos que utilizan la designación OSV (MAL-*) asociada a los paquetes detectados.                                                                       |
| MALICIOUS_PROCESS    | Indica un proceso sospechoso de ser malicioso en función de la inteligencia de amenazas o el análisis del comportamiento. Por ejemplo, esto incluye el malware conocido, las puertas traseras o las herramientas no autorizadas que se ejecutan en una instancia o entorno de contenedores.                                                        |

| Nombre del indicador  | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MISCONFIGURATION      | Indica que un recurso implicado en la secuencia de ataque tiene un error de configuración de seguridad que puede aumentar el impacto potencial. Algunos ejemplos son las políticas de acceso administrativo, la desactivación del control de versiones o la falta de cifrado. Estos errores de configuración se identifican mediante AWS Security Hub CSPM. Para obtener más información, consulte los <a href="#">tipos de características compatibles</a> en la Guía del AWS Security Hub CSPM usuario. |
| REACHABILITY          | Indica que un recurso implicado en la secuencia de ataque es accesible desde Internet o es de acceso público. Los ejemplos incluyen instancias de Amazon EC2 accesibles por Internet, clústeres de Amazon EKS, clústeres de Amazon ECS o buckets de Amazon S3 de acceso público. Para obtener más información, consulte los <a href="#">tipos de características compatibles</a> en la Guía del usuario. AWS Security Hub CSPM                                                                            |
| SENSITIVE_DATA        | Indica que un bucket de Amazon S3 implicado en la secuencia de ataque contiene datos confidenciales, tal y como ha identificado Amazon Macie. AWS Security Hub CSPM                                                                                                                                                                                                                                                                                                                                       |
| SUSPICIOUS_NETWORK    | Se sabe que la red está asociada a puntajes de reputación bajos, como los proveedores de redes privadas virtuales (VPN) y los servicios proxy riesgosos.                                                                                                                                                                                                                                                                                                                                                  |
| SUSPICIOUS_PROCESS    | Indica un proceso sospechoso identificado como anómalo en función de la inteligencia de amenazas o del análisis del comportamiento. Por ejemplo, esto incluye patrones de ejecución de procesos inusuales, relaciones inesperadas entre padres e hijos o procesos con características sospechosas dentro de una instancia o entorno de contenedores.                                                                                                                                                      |
| SUSPICIOUS_USER_AGENT | El agente de usuario está asociado a aplicaciones sospechosas o explotadas potencialmente conocidas, como los clientes de Amazon S3 y las herramientas de ataque.                                                                                                                                                                                                                                                                                                                                         |

| Nombre del indicador          | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TOR_IP                        | La dirección IP está asociada a un nodo de salida de Tor.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| UNUSUAL_API_FOR_ACCOUNT_COUNT | Indica que la AWS API se ha invocado de forma anómala, en función de la línea base histórica de la cuenta. Para obtener más información, consulte <a href="#">Comportamiento anómalo</a> .                                                                                                                                                                                                                                                                                                                             |
| UNUSUAL_ASN_FOR_ACCOUNT_COUNT | Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea de base histórica de la cuenta. Para obtener más información, consulte <a href="#">Comportamiento anómalo</a> .                                                                                                                                                                                                                                                                                                      |
| UNUSUAL_ASN_FOR_USER          | Indica que el número de sistema autónomo (ASN) se identificó como anómalo, en función de la línea base histórica del usuario. Para obtener más información, consulte <a href="#">Comportamiento anómalo</a> .                                                                                                                                                                                                                                                                                                          |
| VULNERABILITY                 | Indica que un recurso implicado en la secuencia de ataque tiene vulnerabilidades conocidas de gravedad crítica, alta, media o baja. Los valores del indicador incluyen los identificadores de CVE y sus niveles de gravedad. Amazon Inspector detecta estas vulnerabilidades y pueden aumentar el impacto potencial de la secuencia de ataque. Para obtener más información sobre los niveles de gravedad, consulte <a href="#">Descripción de los niveles de gravedad</a> en la Guía del usuario de Amazon Inspector. |

## Tácticas de MITRE

En este campo se especifican las tácticas de MITRE ATT&CK que el autor de la amenaza utiliza a través de una secuencia de ataque. GuardDuty utiliza el marco [MITRE ATT&ACK](#), que añade contexto a toda la secuencia de ataque. Los colores que utiliza la GuardDuty consola para especificar los objetivos de amenaza utilizados por el autor de la amenaza se alinean con los colores que indican los valores crítico, alto, medio y bajo. [Niveles de gravedad de los resultados](#)

## Indicadores de red

Los indicadores incluyen una combinación de valores de indicadores de red que explican por qué una red es indicativa de un comportamiento sospechoso. Esta sección es aplicable solo cuando el indicador incluye SUSPICIOUS\_NETWORK o MALICIOUS\_IP. El siguiente ejemplo muestra cómo se pueden asociar los indicadores de red a un indicador, donde:

- *AnyCompany* es un sistema autónomo (AS).
- TUNNEL\_VPN, IS\_ANONYMOUS y ALLOWS\_FREE\_ACCESS son los indicadores de la red.

```
...{
  "key": "SUSPICIOUS_NETWORK",
  "values": [{
    "AnyCompany": [
      "TUNNEL_VPN",
      "IS_ANONYMOUS",
      "ALLOWS_FREE_ACCESS"
    ]
  }]
}
...
```

En la siguiente tabla se incluyen los valores de los indicadores de red y su descripción. Estas etiquetas se añaden en función de la información sobre amenazas GuardDuty recopilada de fuentes como Spur

| Valor de indicador de red | Description (Descripción)                                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TUNNEL_VPN                | La dirección IP o de red está asociada a un tipo de túnel VPN. Se refiere a un protocolo específico que ayuda a establecer una conexión segura y cifrada entre dos puntos a través de una red pública.                                                         |
| TUNNEL_PROXY              | La dirección IP o de red está asociada a un tipo de túnel Proxy. Esto se refiere a un protocolo específico que ayuda a establecer una conexión a través de un servidor proxy.                                                                                  |
| TUNNEL_RDP                | La dirección IP o de red está asociada al uso de un método de encapsulación del tráfico de escritorios remotos (RDP) dentro de otro protocolo para mejorar la seguridad, evitar las restricciones de la red o permitir el acceso remoto a través de firewalls. |
| IS_ANONYMOUS              | La dirección IP o de red está asociada a un servicio anónimo o proxy conocido. Esto puede indicar posibles actividades sospechosas que se esconden detrás de redes anónimas.                                                                                   |

| Valor de indicador de red | Description (Descripción)                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KNOWN_THREAT_OPERATOR     | La dirección IP o de red está asociada a un proveedor de túnel de riesgos conocido. Esto indica que se ha detectado actividad sospechosa en una dirección IP vinculada a una VPN, un proxy u otros servicios de tunelización que se utilizan con frecuencia con fines maliciosos.                                                                                                            |
| ALLOWS_FREE_ACCESS        | La dirección IP o de red está asociada a un operador de túnel que permite el acceso a su servicio sin necesidad de autenticación ni pago. También puede incluir cuentas de prueba o experiencias de uso limitado que ofrecen varios servicios en línea.                                                                                                                                      |
| ALLOWS_CRYPTOCURRENCY     | La dirección IP o de red está asociada a un proveedor de túneles (como una VPN o un servicio proxy) que acepta exclusivamente criptomonedas u otras monedas digitales como método de pago.                                                                                                                                                                                                   |
| ALLOWS_TORRENTS           | La dirección IP o de red está asociada a los servicios o las plataformas que permiten el tráfico de torrents. Estos servicios suelen estar relacionados con el apoyo y el uso de torrents y con actividades de evasión de derechos de autor.                                                                                                                                                 |
| RISK_CALLBACK_PROXY       | La dirección IP o de red está asociada a dispositivos conocidos por enrutar el tráfico a servidores proxy residenciales, servidores proxy de malware u otras redes tipo proxy de devolución de llamadas. Esto no implica que toda la actividad de la red esté relacionada con los servidores proxy, sino que la red tiene la capacidad de enrutar el tráfico en nombre de estas redes proxy. |
| RISK_GEO_MISMATCH         | Este indicador sugiere que el centro de datos o la ubicación del host de una red difieren de la ubicación esperada de los usuarios y dispositivos conectados a ella. Si el valor de este indicador no está presente, no significa que no haya discrepancia. Puede implicar que no hay datos suficientes para confirmar la discrepancia.                                                      |
| IS_SCANNER                | La red o la dirección IP están asociadas a los intentos de inicio de sesión persistentes en los formularios web.                                                                                                                                                                                                                                                                             |

| Valor de indicador de red    | Description (Descripción)                                                                                                                                                                                     |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RISK_WEB_SCRAPING            | La red de direcciones IP está asociada a los clientes web automatizados y a otras actividades web programáticas.                                                                                              |
| CLIENT_BEHAVIOR_FILE_SHARING | La red o la dirección IP están asociadas al comportamiento del cliente, lo que indica actividades de intercambio de archivos, como las redes punto a punto (P2P) o los protocolos de intercambio de archivos. |
| CATEGORY_COMMERCIAL_VPN      | La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un servicio de red privada virtual (VPN) comercial tradicional que opera dentro del espacio del centro de datos.        |
| CATEGORY_FREE_VPN            | La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un servicio de VPN completamente gratuito.                                                                              |
| CATEGORY_RESIDENTIAL_PROXY   | La red o la dirección IP están asociadas a un operador de túnel que se clasifica como un SDK, un malware o un servicio proxy de origen gratuito.                                                              |
| OPERATOR_XXX                 | El nombre del proveedor de servicios que opera este túnel.                                                                                                                                                    |

## Detalles de usuario de la base de datos (DB) de RDS

### Note

Esta sección se aplica a los hallazgos cuando se habilita la función de protección RDS en GuardDuty. Para obtener más información, consulte [GuardDuty Protección RDS](#).

El GuardDuty hallazgo proporciona los siguientes detalles de usuario y autenticación de la base de datos potencialmente comprometida:

- Usuario: el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.
- Aplicación: el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.

- Base de datos: el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.
- SSL: la versión de capa de sockets seguros (SSL) utilizada para la red.
- Método de autenticación: el método de autenticación utilizado por el usuario implicado en el resultado.

Para obtener información acerca del recurso potencialmente afectado, consulte [Recurso](#).

## Detalles del resultado de la supervisión en tiempo de ejecución

### Note

Es posible que estos detalles estén disponibles solo si GuardDuty genera uno de los [GuardDuty Tipos de búsqueda de Runtime Monitoring](#).

Esta sección contiene los detalles del tiempo de ejecución, como los detalles del proceso y cualquier contexto necesario. Los detalles del proceso describen información sobre el proceso observado, y el contexto de ejecución describe cualquier información adicional sobre la actividad potencialmente sospechosa.

### Detalles del proceso

- Nombre: el nombre del proceso.
- Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
- Ejecutable SHA-256: el SHA256 hash del ejecutable del proceso.
- PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
- Directorio de trabajo actual: el directorio de trabajo actual del proceso.
- ID del proceso: el ID asignado al proceso por el sistema operativo.
- startTime: la hora en la que se ha iniciado el proceso. Está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z).
- UUID: el identificador único asignado al proceso por GuardDuty.
- UUID principal: el ID único del proceso principal. Este ID lo asigna al proceso principal. GuardDuty

- Usuario: el usuario que ha ejecutado el proceso.
- ID del usuario: el ID del usuario que ha ejecutado el proceso.
- ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
- Linaje: información sobre los antepasados del proceso.
  - ID del proceso: el ID asignado al proceso por el sistema operativo.
  - UUID: el identificador único asignado al proceso por GuardDuty.
  - Ruta ejecutable: la ruta absoluta del archivo ejecutable del proceso.
  - ID del usuario efectivo: el ID del usuario efectivo del proceso en el momento del evento.
  - UUID principal: el ID único del proceso principal. Este ID lo asigna al proceso principal. GuardDuty
  - Hora de inicio: la hora en la que se ha iniciado el proceso.
  - PID del espacio de nombres: el ID del proceso en un espacio de nombres de PID secundario distinto del espacio de nombres de PID del host. En el caso de los procesos dentro de un contenedor, es el ID de proceso observado dentro del contenedor.
  - ID del usuario: el ID del usuario que ejecutó el proceso.
  - Nombre: el nombre del proceso.

## Contexto del tiempo de ejecución

De los siguientes campos, un resultado generado puede incluir solo los campos que son relevantes para el tipo de resultado.

- Origen de la montura: la ruta en el host que monta el contenedor.
- Destino de la montura: la ruta del contenedor que está asignada al directorio del host.
- Tipo de sistema de archivos: representa el tipo de sistema de archivos montado.
- Marcas: representan las opciones que controlan el comportamiento del evento implicado en este resultado.
- Proceso de modificación: información sobre el proceso que ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución.
- Modificado el: la marca de tiempo en la que el proceso ha creado o modificado un binario, un script o una biblioteca dentro de un contenedor en tiempo de ejecución. Este campo está en formato de cadena de fecha UTC (2023-03-22T19:37:20.168Z).
- Ruta de la biblioteca: la ruta a la nueva biblioteca que se ha cargado.



- Valor de precarga de LD: el valor de la variable de entorno LD\_PRELOAD.
- Ruta del socket: la ruta al socket de Docker al que se accedió.
- Ruta al binario Runc: la ruta al binario runc.
- Ruta del agente de lanzamiento: la ruta al archivo del agente de lanzamiento del cgroup.
- Ejemplo de línea de comandos: ejemplo de la línea de comandos implicada en la actividad potencialmente sospechosa.
- Categoría de herramienta: categoría a la que pertenece la herramienta. Algunos ejemplos son las herramientas de puerta trasera, prueba de penetración, analizador de red y rastreador de red.
- Nombre de la herramienta: el nombre de la herramienta potencialmente sospechosa.
- Ruta del script: la ruta al script ejecutado que generó el resultado.
- Ruta del archivo de amenazas: la ruta sospechosa en la que se encontraron los detalles de la inteligencia de amenazas.
- Nombre del servicio: el nombre del servicio de seguridad que se ha desactivado.
- Nombre del módulo: nombre del módulo que se carga en el kernel.
- Módulo SHA256: el hash SHA256 del módulo.
- Ruta del archivo del módulo: ruta del módulo cargado en el kernel.

## Detalles del análisis de volúmenes de EBS

### Note

Esta sección se aplica a los hallazgos al activar el análisis de GuardDuty-initiated malware [Malware Protection for EC2](#).

El análisis de volúmenes de EBS proporciona detalles sobre el volumen de EBS asociado a la carga de trabajo del contenedor o la instancia de EC2 potencialmente afectada.

- ID de análisis: el identificador del análisis de malware.
- Análisis iniciado el: la fecha y hora en que inició el análisis de malware.
- Análisis completado el: la fecha y la hora en que se completó el análisis de malware.
- Identificador de búsqueda de activación: el identificador de GuardDuty búsqueda del hallazgo que inició este análisis de malware.

- Orígenes: los valores potenciales son Bitdefender y Amazon.

Para obtener más información sobre el motor de análisis utilizado para detectar malware, consulte [GuardDuty motor de escaneo de detección de malware](#).

- Detecciones de análisis: la vista completa de los detalles y los resultados de cada análisis de malware.
  - Recuento de elementos analizados: el número total de archivos analizados. Proporciona detalles como `totalGb`, `files` y `volumes`.
  - Recuento de elementos de amenazas detectadas: el número total de files maliciosos detectados durante el análisis.
  - Detalles de las amenazas de mayor gravedad: los detalles de la amenaza de mayor gravedad detectada durante el análisis y el número de archivos maliciosos. Proporciona detalles como `severity`, `threatName` y `count`.
  - Amenazas detectadas por nombre: el elemento del contenedor que agrupa las amenazas de todos los niveles de gravedad. Proporciona detalles como `itemCount`, `uniqueThreatNameCount`, `shortened` y `threatNames`.

## Detalles de los resultados de Malware Protection for EC2

### Note

Esta sección se aplica a los datos detectados al activar el análisis de GuardDuty-initiated malware [Malware Protection for EC2](#).

Cuando el escáner de Malware Protection for EC2 detecte malware, podrá ver los detalles del análisis seleccionando el resultado correspondiente en la página de resultados de la <https://console.aws.amazon.com/guardduty/console>. La gravedad del hallazgo de Malware Protection for EC2 depende de la gravedad del GuardDuty hallazgo.

La siguiente información está disponible en la sección Amenazas detectadas del panel de detalles.

- Nombre: el nombre de la amenaza, obtenido al agrupar los archivos por detección.
- Gravedad: el nivel de gravedad de la amenaza detectada.
- Hash: el SHA-256 del archivo.
- Ruta de archivo: la ubicación del archivo malicioso en el volumen de EBS.

- Nombre de archivo: el nombre del archivo en el que se detectó la amenaza.
- ARN del volumen: el ARN de los volúmenes de EBS analizados.

La siguiente información está disponible en la sección Detalles del análisis de malware del panel de detalles.

- ID de análisis: el ID del análisis de malware.
- Análisis iniciado el: la fecha y hora en que inició el análisis.
- Análisis completado el: la fecha y la hora en que se completó el análisis.
- Archivos analizados: el número total de archivos y directorios analizados.
- Total de GB analizados: la cantidad de almacenamiento analizada durante el proceso.
- Identificador de búsqueda del disparador: el identificador de GuardDuty búsqueda del hallazgo que inició este análisis de malware.
- La siguiente información está disponible en la sección Detalles del volumen del panel de detalles.
  - ARN del volumen: el nombre de recurso de Amazon (ARN) del volumen.
  - SnapshotARN: el ARN de la instantánea del volumen de EBS.
  - Estado: el estado de análisis del volumen, como Running, Skipped y Completed.
  - Tipo de cifrado: el tipo de cifrado utilizado en el volumen. Por ejemplo, CCMK.
  - Nombre del dispositivo: el nombre del dispositivo. Por ejemplo, /dev/xvda.

## Detalles de los resultados de la protección contra malware para S3

Los siguientes detalles del análisis de software malicioso están disponibles al activar GuardDuty tanto la protección contra malware para S3 en su dispositivo Cuenta de AWS:

- Amenazas: una lista de las amenazas detectadas durante el análisis de malware.

### Múltiples amenazas potenciales en archivos de archivo

Si tiene un archivo de archivo con varias amenazas potenciales, la protección contra malware para S3 solo informa de la primera amenaza detectada. Después de esto, el estado del escaneo se marca como completado. GuardDuty genera el tipo de búsqueda asociado y también envía EventBridge los eventos que genera. Para obtener más información sobre la supervisión de los escaneos de objetos de Amazon S3

mediante los EventBridge eventos, consulte el ejemplo de esquema de notificaciones de THREATS\_FOUND en. [Producto del análisis del objeto S3](#)

- Ruta del elemento: una lista de rutas de elementos anidados y detalles del hash del objeto de S3 analizado.
- Ruta del elemento anidado: ruta del elemento del objeto de S3 analizado en el que se detectó la amenaza.

El valor de este campo solo estará disponible si el objeto de nivel superior es un archivo y si se detecta una amenaza dentro de un archivo.

- Hash: hash de la amenaza detectada en este resultado.
- Orígenes: los valores potenciales son Bitdefender y Amazon.

Para obtener más información sobre el motor de análisis utilizado para detectar malware, consulte [GuardDuty motor de escaneo de detección de malware](#).

## Action

La acción de un resultado proporciona detalles sobre el tipo de actividad que desencadenó el resultado. La información disponible variará en función del tipo de acción.

Tipo de acción: el tipo de actividad del resultado. Este valor puede ser NETWORK\_CONNECTION, PORT\_PROBE, DNS\_REQUEST o RDS\_LOGIN\_ATTEMPT. AWS\_API\_CALL La información disponible variará en función del tipo de acción:

- NETWORK\_CONNECTION: indica que hubo un intercambio de tráfico de la red entre la instancia de EC2 identificada y el host remoto. Este tipo de acción presenta la siguiente información adicional:
  - Dirección de conexión: la dirección de conexión de red observada en la actividad que provocó la generación del hallazgo. GuardDuty Puede ser uno de los siguientes valores:
    - INBOUND: indica que un host remoto inició una conexión con un puerto local en la instancia de EC2 identificada en su cuenta.
    - OUTBOUND: indica que la instancia de EC2 identificada inició una conexión a un host remoto.
    - Desconocido: indica que no se GuardDuty pudo determinar la dirección de la conexión.
  - Protocolo: el protocolo de conexión de red observado en la actividad que provocó GuardDuty la generación del hallazgo.

- **IP local:** la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
- **Bloqueado:** indica si el puerto objetivo está bloqueado.
- **PORT\_PROBE:** indica que un host remoto sondeó la instancia de EC2 identificada en varios puertos abiertos. Este tipo de acción presenta la siguiente información adicional:
  - **IP local:** la dirección IP de origen original del tráfico que activó el resultado. Se puede usar esta información para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico que desencadenó la búsqueda. Por ejemplo, la dirección IP de un pod EKS en lugar de la dirección IP de la instancia en la que se ejecuta el pod EKS.
  - **Bloqueado:** indica si el puerto objetivo está bloqueado.
- **DNS\_REQUEST:** indica que la instancia de EC2 identificada consultó un nombre de dominio. Este tipo de acción presenta la siguiente información adicional:
  - **Protocolo:** el protocolo de conexión de red observado en la actividad que provocó GuardDuty la generación del hallazgo.
  - **Bloqueado:** indica si el puerto objetivo está bloqueado.
- **AWS\_API\_CALL**— Indica que se ha invocado una AWS API. Este tipo de acción presenta la siguiente información adicional:
  - **API:** el nombre de la operación de API que se invocó y, por lo tanto, se GuardDuty le pidió que generara este resultado.

 **Note**

Estas operaciones también pueden incluir eventos que no pertenecen a la API capturados por AWS CloudTrail. Para obtener más información, consulte [Non-API los eventos capturados por CloudTrail](#).

- **Agente de usuario:** el agente de usuario que hizo la solicitud de API. Este valor indica si la llamada se realizó desde Consola de administración de AWS, un AWS servicio, los AWS SDK o el AWS CLI.
- **CÓDIGO DE ERROR:** si una llamada fallida a la API ha desencadenado el resultado, se muestra el código de error de esa llamada.

- Nombre del servicio: el nombre de DNS del servicio que ha intentado hacer la llamada a la API que desencadenó el resultado.
- RDS\_LOGIN\_ATTEMPT: indica que se intentó iniciar sesión en la base de datos potencialmente afectada desde una dirección IP remota.
- Dirección IP: la dirección IP remota que se utilizó para llevar a cabo el intento de inicio de sesión potencialmente sospechoso.

## Actor u objetivo

Un resultado tendrá una sección Actor si el Rol de recurso era TARGET. Esto indica que su recurso fue objeto de actividad sospechosa y la sección Actor contendrá detalles sobre la entidad que tenía el recurso como objetivo.

Un resultado tendrá una sección Objetivo si el Rol de recurso era ACTOR. Esto indica que su recurso estuvo involucrado en actividad sospechosa contra un host remoto y esta sección contendrá información sobre la IP o el dominio que era el objetivo de su recurso.

La información disponible en la sección Actor u Objetivo puede incluir lo siguiente:

- Afiliado: detalla si la AWS cuenta de la persona que llama a la API remota está relacionada con su GuardDuty entorno. Si este valor es `true`, la persona que llama a la API está afiliada a su cuenta de alguna manera; si es `false`, la persona que llama a la API es ajena a su entorno.
- ID de cuenta remota: el ID de cuenta propietaria de la dirección IP saliente que se utilizó para acceder al recurso en la red final.
- Dirección IP: la dirección IP implicada en la actividad que provocó GuardDuty la generación del hallazgo.
- Ubicación: información de ubicación de la dirección IP implicada en la actividad que provocó GuardDuty la generación del hallazgo.
- Organización: información de la organización del ISP sobre la dirección IP implicada en la actividad que motivó GuardDuty la generación del hallazgo.
- Puerto: el número de puerto implicado en la actividad que provocó GuardDuty la generación del hallazgo.
- Dominio: el dominio implicado en la actividad que provocó GuardDuty la generación del hallazgo.
- Dominio con sufijo: el dominio de segundo y superior nivel implicado en una actividad que podría provocar la generación del hallazgo. GuardDuty Para obtener una lista de dominios de primer y segundo nivel, consulte la [lista de sufijos públicos](#).

## Detalles de geolocalización

GuardDuty determina la ubicación y la red de las solicitudes mediante bases de datos de MaxMind GeoIP. MaxMind informa de una precisión muy alta de sus datos a nivel de país, aunque la precisión varía según factores como el país y el tipo de dirección IP.

Para obtener más información MaxMind, consulte [Geolocalización MaxMind IP](#). Si cree que alguno de los datos de GeoIP es incorrecto, envíe una solicitud de corrección MaxMind a [MaxMindCorrect GeoIP2 Data](#).

## Información adicional

Todos los resultados tienen una sección de Información adicional donde se puede encontrar la siguiente información:

- **Nombre de la lista de amenazas:** el nombre de la lista de amenazas que incluye la dirección IP o el nombre de dominio involucrados en la actividad que provocó la GuardDuty búsqueda.
- **Muestra:** un valor verdadero o falso que indica si se trata de un resultado de muestra.
- **Archivado:** un valor verdadero o falso que indica si el resultado se ha archivado.
- **Inusual:** detalles de las actividades que no se han observado históricamente. Pueden incluir cualquier usuario, hora, ubicación, bucket, comportamiento de inicio de sesión u organización de ASN inusuales (no observados previamente).
- **Protocolo inusual:** el protocolo de conexión de red implicado en la actividad GuardDuty que provocó la generación del hallazgo.
- **Detalles del agente:** detalles sobre el agente de seguridad que está implementado actualmente en el clúster de EKS de su Cuenta de AWS. Esto solo se aplica a los tipos de resultados de la Supervisión en tiempo de ejecución de EKS.
  - **Versión del agente:** la versión del agente GuardDuty de seguridad.
  - **ID del agente:** el identificador único del agente GuardDuty de seguridad.

## Evidencia

Los resultados que se obtienen mediante la inteligencia sobre amenazas tienen una sección de Evidencia que incluye la siguiente información:

- **Detalles de inteligencia de amenazas:** el nombre de la lista de amenazas en la que aparece el Threat name reconocido.

- Nombre de la amenaza: el nombre de la familia de malware u otro identificador asociado a la amenaza.
- Archivo de amenaza SHA256: SHA256 del archivo que generó el resultado.

## Comportamiento anómalo

Los tipos de hallazgos que terminan en `AnomalousBehavior` indican que el hallazgo se generó mediante el modelo de aprendizaje automático (ML) de detección de GuardDuty anomalías. El modelo de ML evalúa todas las solicitudes de API a su cuenta e identifica los eventos anómalos relacionados con las tácticas utilizadas por los adversarios. El modelo de ML da seguimiento a varios factores de la solicitud de API, como el usuario que hizo la solicitud, la ubicación desde la que se hizo la solicitud y la API específica que se solicitó.

Los detalles sobre los factores de la solicitud de API que son inusuales para la identidad del CloudTrail usuario que invocó la solicitud se encuentran en los detalles de la búsqueda. Las identidades las define el elemento [CloudTrail UserIdentity](#) y los valores posibles son `Root`, `IAMUser`, `AssumedRole` o `FederatedUser`. `AWSAccount` `AWSService`

Además de los detalles disponibles para todos los GuardDuty hallazgos relacionados con la actividad de la API, `AnomalousBehavior` los hallazgos tienen detalles adicionales que se describen en la siguiente sección. Estos detalles se pueden ver en la consola y también están disponibles en el JSON de los resultados.

- API anómalas: lista de solicitudes de API invocadas por la identidad del usuario cerca de la solicitud de API principal asociada al resultado. En este panel se desglosan en profundidad los detalles del evento de la API de las siguientes maneras.
  - La primera API de la lista es la API principal, que es la solicitud de API asociada a la actividad observada de mayor riesgo. Esta es la API que ha desencadenado el resultado y se correlaciona con la fase de ataque del tipo de resultado. Esta es también la API que se detalla en la sección Acción de la consola y en el JSON del resultado.
  - Todas las demás API de la lista son API anómalas adicionales a la identidad de usuario de la lista observadas cerca de la API principal. Si solo hay una API en la lista, el modelo de ML no ha identificado como anómala ninguna solicitud de API adicional procedente de esa identidad de usuario.
  - La lista de API se divide en función de si una API se llamó correctamente o si se llamó de forma incorrecta, lo que significa que se recibió una respuesta de error. El tipo de respuesta de error recibida aparece encima de cada API llamada incorrectamente. Los posibles tipos de respuesta



de error son: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` y `operation not permitted`.

- Las API se clasifican según su servicio asociado.
- Para obtener más contexto, seleccione API históricas para ver los detalles sobre las API principales, hasta un máximo de 20, que normalmente se muestran tanto para la identidad del usuario como para todos los usuarios de la cuenta. Las API se marcan como Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), en función de la frecuencia con la que se usen en la cuenta.
- Comportamiento inusual (cuenta): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de su cuenta.

#### Comportamiento perfilado

GuardDuty obtiene información continua sobre las actividades de su cuenta en función de los eventos organizados. Estas actividades y su frecuencia observada se conocen como comportamiento perfilado.

La información rastreada en este panel incluye:

- Organización de ASN: la organización de número de sistema autónomo (ASN) desde la que se realizó la llamada anómala a la API.
- Nombre de usuario: el nombre del usuario que hizo la llamada anómala a la API.
- Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
- Tipo de usuario: el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.
- Bucket: el nombre del bucket de S3 al que se ha accedido.
- Comportamiento inusual (identidad de usuario): en esta sección se proporcionan detalles adicionales sobre el comportamiento perfilado de la identidad de usuario implicado en el resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje GuardDuty automático no había visto previamente esta identidad de usuario haciendo esta llamada a la API de esta manera durante el período de entrenamiento. Los siguientes detalles adicionales sobre la identidad de usuario están disponibles:

- Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.
- Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
- Bucket: el nombre del bucket de S3 al que se ha accedido.
- Comportamiento inusual (bucket): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado del bucket de S3 asociado al resultado. Cuando un comportamiento no se identifica como histórico, significa que en el modelo de aprendizaje GuardDuty automático no se habían realizado anteriormente llamadas a la API a este segmento de esta manera durante el período de formación. La información rastreada en esta sección incluye:
  - Organización de ASN: la organización de ASN desde la que se hizo la llamada anómala a la API.
  - Nombre de usuario: el nombre del usuario que hizo la llamada anómala a la API.
  - Agente de usuario: el agente de usuario utilizado para hacer la llamada anómala a la API. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `aws-cli` o `Botocore`.
  - Tipo de usuario: el tipo de usuario que hizo la llamada anómala a la API. Los valores posibles son `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` o `ROLE`.

 Note

Para más información sobre los comportamientos históricos, seleccione Comportamiento histórico en las secciones Comportamiento inusual (cuenta), ID de usuario o Bucket para ver detalles sobre el comportamiento esperado de su cuenta en cada una de las siguientes categorías: Raro (menos de una vez al mes), Poco frecuente (varias veces al mes) o Frecuente (diario o semanal), según la frecuencia con la que se usen en la cuenta.

- Comportamiento inusual (base de datos): en esta sección, se proporcionan detalles adicionales sobre el comportamiento perfilado de la instancia de base de datos asociada al resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje GuardDuty automático no ha visto ningún intento de inicio de sesión en esta instancia de base de datos de esta manera durante el período de entrenamiento. La información recopilada en esta sección del panel de resultados incluye:

- Nombre de usuario: el nombre de usuario utilizado para llevar a cabo el intento de inicio de sesión anómalo.
- Organización de ASN: la organización de ASN desde la que se hizo el intento de inicio de sesión anómalo.
- Nombre de la aplicación: el nombre de la aplicación utilizada para llevar a cabo el intento de inicio de sesión anómalo.
- Nombre de base de datos: el nombre de la instancia de base de datos implicada en el intento de inicio de sesión anómalo.

La sección Comportamiento histórico proporciona más contexto sobre los Nombres de usuario, Organizaciones de ASN, Nombres de las aplicaciones y Nombres de bases de datos observados anteriormente para la base de datos asociada. Cada valor único tiene un recuento asociado que representa el número de veces que se observó este valor en un evento de inicio de sesión exitoso.

- Comportamiento inusual (clúster de Kubernetes de la cuenta, espacio de nombres de Kubernetes y nombre de usuario de Kubernetes): esta sección proporciona detalles adicionales sobre el comportamiento perfilado para el clúster de Kubernetes y el espacio de nombres asociados al resultado. Cuando un comportamiento no se identifica como histórico, significa que el modelo de aprendizaje GuardDuty automático no ha observado previamente esta cuenta, clúster, espacio de nombres o nombre de usuario de esta manera. La información recopilada en esta sección del panel de resultados incluye:
  - Nombre de usuario: el usuario que llamó a la API de Kubernetes asociada al resultado.
  - Nombre de usuario suplantado: el usuario suplantado por `username`.
  - Espacio de nombres: el espacio de nombres de Kubernetes dentro del clúster de Amazon EKS en el que se produjo la acción.
  - Agente de usuario: el agente de usuario asociado a la llamada a la API de Kubernetes. El agente de usuario es el método utilizado para hacer la llamada, por ejemplo, `kubectl`.
  - API: la API de Kubernetes llamada por `username` dentro del clúster de Amazon EKS.
  - Información de ASN: la información de ASN, como la organización y el proveedor de servicios de Internet, asociada a la dirección IP del usuario que realiza esta llamada.
  - Día de la semana: el día de la semana en que se realizó la llamada a la API de Kubernetes.
  - Permiso: el verbo de Kubernetes y el recurso cuyo acceso se comprueba para indicar si el `username` puede o no utilizar la API de Kubernetes.
  - Nombre de la cuenta de servicio: la cuenta de servicio asociada a la carga de trabajo de Kubernetes que proporciona una identidad a la carga de trabajo.

- Registro: el registro del contenedor asociado a la imagen del contenedor que se implementa en la carga de trabajo de Kubernetes.
- Imagen: la imagen de contenedor, sin las etiquetas ni el resumen asociados, que se implementa en la carga de trabajo de Kubernetes.
- Configuración del prefijo de la imagen: el prefijo de la imagen con la configuración de seguridad del contenedor y la carga de trabajo habilitada, por ejemplo `hostNetwork` o `privileged` para el contenedor que usa la imagen.
- Nombre del sujeto: los sujetos, como un `user`, `group`, o `serviceAccountName` que están vinculados a un rol de referencia en un `RoleBinding` o `ClusterRoleBinding`.
- Nombre del rol: el nombre del rol que participa en la creación o modificación de roles o en la API `roleBinding`.

## Anomalías basadas en el volumen de S3

En esta sección, se detalla la información contextual de las anomalías basadas en el volumen de S3. El resultado basado en el volumen ([Exfiltration:S3/AnomalousBehavior](#)) supervisa un número inusual de llamadas a la API de S3 hechas por los usuarios a los buckets de S3, lo que indica una posible exfiltración de datos. Las siguientes llamadas a la API de S3 se supervisan para detectar anomalías basadas en el volumen.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

Las siguientes métricas ayudarían a crear una referencia del comportamiento habitual cuando una entidad de IAM accede a un bucket de S3. Para detectar la exfiltración de datos, el resultado de la detección de anomalías basada en el volumen evalúa todas las actividades con respecto a la referencia de comportamiento habitual. Seleccione Comportamiento histórico en las secciones Comportamiento inusual (identidad de usuario), Volumen observado (identidad de usuario) y Volumen observado (bucket) para ver las siguientes métricas, respectivamente.

- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.

- Número de llamadas a la API `s3-api-name` invocadas por el usuario de IAM o rol de IAM (depende de cuál se haya emitido) asociados a todos los buckets de S3 afectados en las últimas 24 horas.
- Número de llamadas a la API `s3-api-name` en todos los usuarios de IAM o roles de IAM (depende de cuál se haya emitido) asociados al bucket de S3 afectado en las últimas 24 horas.

## Anomalías basadas en la actividad de inicio de sesión en RDS

En esta sección, se detalla el recuento de los intentos de inicio de sesión de un actor inusual y se agrupa por el resultado de los intentos de inicio de sesión. [Tipos de resultados de la protección de RDS](#) identifica el comportamiento anómalo mediante la supervisión de los eventos de inicio de sesión para detectar patrones inusuales de `successfulLoginCount`, `failedLoginCount` y `incompleteConnectionCount`.

- **correcto LoginCount:** este contador representa la suma de las conexiones correctas (combinación correcta de atributos de inicio de sesión) realizadas a la instancia de la base de datos por un actor inusual. Los atributos de inicio de sesión incluyen el nombre de usuario, la contraseña y el nombre de la base de datos.
- **error LoginCount:** este contador representa la suma de los intentos de inicio de sesión fallidos (fallidos) realizados para establecer una conexión con la instancia de base de datos. Esto indica que uno o varios atributos de la combinación de inicio de sesión, como el nombre de usuario, la contraseña o el nombre de la base de datos, eran incorrectos.
- **incompleto ConnectionCount:** este contador representa el número de intentos de conexión que no se pueden clasificar como exitosos o fallidos. Estas conexiones se cierran antes de que la base de datos proporcione una respuesta. Por ejemplo, se analiza un puerto cuando el puerto de la base de datos está conectado, pero no se envía ningún dato a la base de datos o cuando la conexión se interrumpió antes de que se completara el inicio de sesión en un intento exitoso o fallido.

## GuardDuty encontrar agregación

GuardDuty actualiza los hallazgos generados de forma dinámica. Si GuardDuty detecta una nueva actividad relacionada con el mismo problema de seguridad, en lugar de crear un nuevo hallazgo, GuardDuty actualizará el hallazgo original con los detalles más recientes. Este comportamiento le permite identificar problemas en curso sin necesidad de revisar varios informes similares y reduce el volumen general de los resultados de seguridad que ya conoce.

Por ejemplo, para un resultado `UnauthorizedAccess:EC2/SSHBruteForce`, se agregarán varios intentos de acceso contra la instancia al mismo ID de resultado, lo que aumentará el número de recuento en los detalles del resultado. Esto se debe a que ese resultado representa un único problema de seguridad con la instancia que indica que el puerto SSH de la instancia no está protegido adecuadamente contra este tipo de actividad. Sin embargo, si GuardDuty detecta actividad de acceso SSH dirigida a una nueva instancia en su entorno, creará un nuevo resultado con un ID de resultado único para alertarle sobre el hecho de que hay un problema de seguridad asociado con el nuevo recurso.

Cuando se agrega un resultado, se actualiza con la información del último caso de esa actividad. Esto significa que, en el ejemplo anterior, si su instancia es el objetivo de un intento de fuerza bruta de un nuevo actor, los detalles del resultado se actualizarán para reflejar la IP remota del origen más reciente y se sustituirá la información más antigua. La información completa sobre los intentos de actividad individuales seguirá estando disponible en sus CloudTrail registros o en los registros de flujo de VPC.

Los criterios que permiten GuardDuty generar un nuevo hallazgo en lugar de agregar uno existente dependen del tipo de hallazgo. Nuestros ingenieros de seguridad determinan los criterios de agregación para cada tipo de resultado para proporcionarle la mejor información general de los distintos problemas de seguridad dentro de su cuenta.

Cuando GuardDuty genere un tipo de búsqueda de secuencia de ataque en tu cuenta, el resultado solo se agregará cuando GuardDuty identifique señales similares en la misma secuencia en tu cuenta. De lo contrario, GuardDuty generará otra secuencia de ataque.

# Gestión de los GuardDuty hallazgos de Amazon

GuardDuty ofrece varias funciones importantes que le ayudarán a clasificar, almacenar y gestionar sus hallazgos. Estas funciones le ayudarán a adaptar los resultados a su entorno específico, a reducir el ruido que generan los hallazgos de bajo valor y a centrarse en las amenazas que afectan a su AWS entorno específico. Revise los temas que aparecen en esta página para comprender cómo puede utilizar estas características para aumentar el valor de los resultados de seguridad en el entorno.

Temas:

## [Panel de resumen en Amazon GuardDuty](#)

Obtenga información sobre los componentes del panel de resumen disponible en la GuardDuty consola.

## [Filtrar los hallazgos en GuardDuty](#)

Aprenda a filtrar las GuardDuty conclusiones en función de los criterios que especifique.

## [Reglas de supresión en GuardDuty](#)

Aprenda a filtrar automáticamente las GuardDuty alertas de los hallazgos mediante las reglas de supresión. Las reglas de supresión archivan automáticamente los resultados en función de los filtros.

## [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#)

Personalice el alcance GuardDuty de la supervisión mediante listas de IP y listas de amenazas basadas en direcciones IP enrutables públicamente. Las listas de direcciones IP fiables impiden que se generen datos ajenos al DNS a partir de direcciones IP que considera de confianza, mientras que las listas de información sobre amenazas permiten avisarle de la GuardDuty actividad de direcciones IP definidas por el usuario.

## [Exportar los resultados generados a Amazon S3](#)

Exporte los hallazgos generados a un bucket de Amazon S3 para poder mantener registros después del período de retención de hallazgos de 90 días. GuardDuty Utilice estos datos históricos para monitorear posibles actividades sospechosas en la cuenta y evaluar la efectividad de las medidas correctivas implementadas.

## Procesando GuardDuty las conclusiones con Amazon EventBridge

Configura notificaciones automáticas para GuardDuty los hallazgos a través de los EventBridge eventos de Amazon. También puedes automatizar otras tareas EventBridge para ayudarte a responder a los hallazgos.

## Descripción de CloudWatch los registros y los motivos por los que se omiten recursos durante el análisis de EC2 con Malware Protection

Descubra cómo puede auditar los CloudWatch registros de protección contra GuardDuty malware de EC2 y cuáles son los motivos por los que la instancia de Amazon EC2 o los volúmenes de Amazon EBS afectados pueden haberse omitido durante el proceso de escaneo.

## Reportar falsos positivos en la protección contra malware para EC2

Descubra cómo puede denunciar posibles detecciones de amenazas por falsos positivos en Malware Protection for EC2.

## Reportar el producto del análisis de objetos de S3 como falso positivo en la protección contra malware para S3

Obtenga información sobre cómo informar de posibles falsos positivos en detecciones de amenazas en la protección contra malware para S3.

## Notificación de falsos positivos en Malware Protection for Backup

Descubra cómo puede informar sobre posibles detecciones de amenazas de falsos positivos en Malware Protection for Backup.

# Panel de resumen en Amazon GuardDuty

El panel de GuardDuty resumen proporciona una vista agregada de los GuardDuty hallazgos generados en usted Cuenta de AWS en la actualidad Región de AWS.

Si utilizas una cuenta de GuardDuty administrador, el panel proporciona estadísticas y datos agregados de tu cuenta y de las cuentas de los miembros de tu organización.

Visualización del panel Resumen

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

GuardDuty muestra el panel de resumen de forma predeterminada al abrir la consola.



2. En la página de resumen, elija lo que desee en el selector Región de AWS de regiones situado en la esquina superior derecha de la consola.
3. En el menú selector de intervalos de fechas, elija el intervalo de fechas del que desee ver el resumen. De forma predeterminada, el panel muestra los datos del día actual, Hoy.

 Note

Si no se generaron resultados durante el intervalo de fechas seleccionado, el panel no tendrá ningún dato que mostrar. Puede actualizar el panel o ajustar el intervalo de fechas.

## Temas

- [Descripción general de](#)
- [Hallazgos](#)
- [Tipos de resultados más comunes](#)
- [Resultados por gravedad](#)
- [Cuentas con la mayoría de los resultados](#)
- [Recursos con resultados](#)
- [Resultados menos frecuentes](#)
- [Cobertura de los planes de protección](#)

## Descripción general de

En esta sección se proporcionan los siguientes datos:

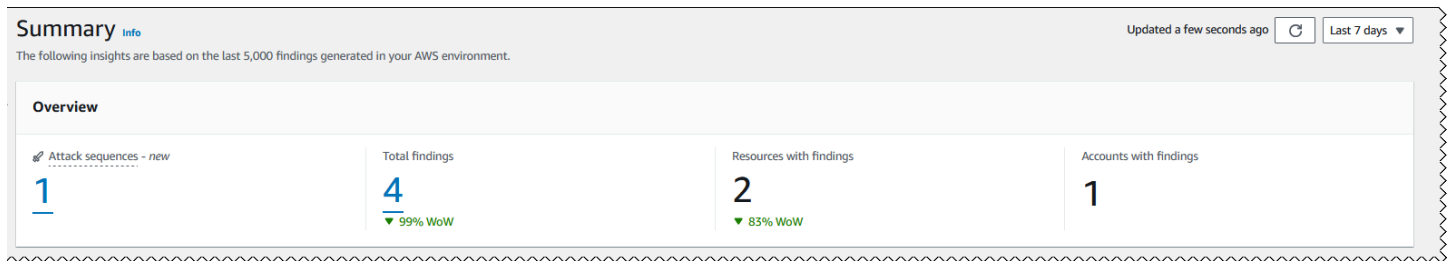
- Secuencias de ataque: indica el número de hallazgos de secuencias de ataque que GuardDuty se generaron en tu cuenta en la región actual.

GuardDuty detecta posibles ataques en varias etapas en tu cuenta. Puede seleccionar el número en Secuencias de ataque para ver sus detalles en la página Resultados.

- Resultados totales: indica el número total de resultados generados en su cuenta en la región actual. Esto incluye tanto los resultados individuales como los resultados de la secuencia de ataque.

- **Recursos con resultados:** indica el número de recursos que están asociados a un resultado y que están potencialmente en peligro.
- **Cuentas con resultados:** indica el número de cuentas en las que se generó al menos un resultado. Si es una cuenta independiente, el valor de este campo es 1.

En el caso de los intervalos de tiempo 7 últimos días y 30 últimos días, en el panel Información general se puede mostrar la diferencia porcentual entre los resultados generados semana tras semana (WoW) o mes tras mes (MoM), respectivamente. Si no se generó ningún resultado la semana o el mes anterior y no hay datos para comparar, es posible que la diferencia porcentual no esté disponible.



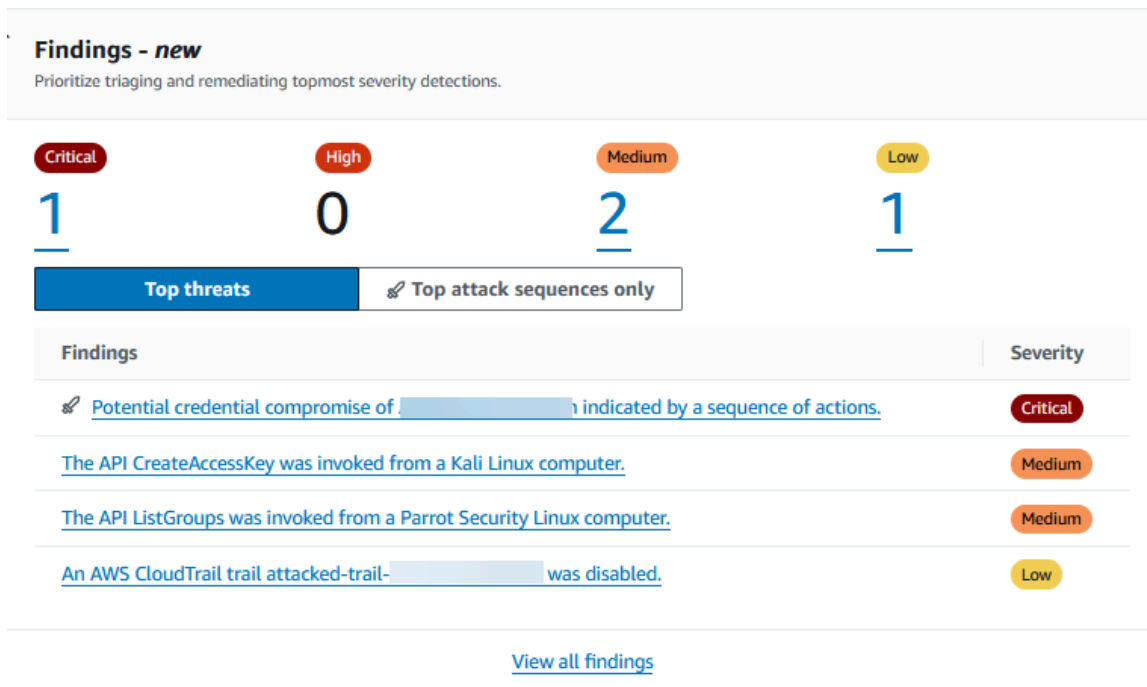
Si eres GuardDuty administrador de una cuenta, todos estos campos proporcionan los datos resumidos de todas las cuentas de los miembros de tu organización.

## Hallazgos

El widget Resultados muestra hasta ocho resultados principales. Estos resultados se enumeran en función de su nivel de gravedad, y los resultados críticos se muestran primero.

De forma predeterminada, puede ver todos los resultados. Para ver solo los datos de los resultados de las secuencias de ataque, active Solo las secuencias de ataque principales.

En esta lista, puede seleccionar cualquier resultado para ver sus detalles.



## Tipos de resultados más comunes

En esta sección se muestra un gráfico circular de los cinco tipos de resultados más comunes generados en la región actual. Al pasar el cursor sobre cada sector del gráfico circular, puede observar lo siguiente:

- Recuento de resultados: indica el número de veces que se ha generado este resultado en el intervalo de tiempo elegido.
- Gravedad: indica el nivel de gravedad del resultado.
- Porcentaje: indica la proporción de este tipo de resultado en relación con el total.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se detectó este tipo de resultado por última vez.

## Resultados por gravedad

En esta sección se muestra un gráfico de barras que muestra el número total de resultados en el intervalo de fechas seleccionado. El gráfico desglosa los resultados por gravedad (crítica, alta, media y baja) y le ayuda a ver el número de resultados en fechas específicas dentro del rango.

Para ver los recuentos de cada nivel de gravedad en una fecha específica, coloque el cursor sobre la barra correspondiente del gráfico.

## Cuentas con la mayoría de los resultados

En esta sección se proporcionan los siguientes datos:

- **Cuenta:** indica el Cuenta de AWS ID en el que se generó el hallazgo.
- **Recuento de resultados:** indica el número de veces que se generó un resultado para este ID de cuenta.
- **Generado más recientemente:** indica cuánto tiempo ha pasado desde que se generó un tipo de resultado por última vez para este ID de cuenta.
- **Filtro de gravedad:** de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Todas las gravedades, Gravedad crítica, Gravedad alta y Gravedad media.

## Recursos con resultados

En esta sección se proporcionan los siguientes datos:

- **Recurso:** muestra el tipo de recurso potencialmente afectado y, si este recurso pertenece a su cuenta, puede acceder al enlace rápido para ver los detalles del recurso. Si es GuardDuty administrador de una cuenta, puede ver los detalles del recurso potencialmente afectado accediendo a la GuardDuty consola con las credenciales de la cuenta del miembro propietario.
- **Cuenta:** indica el Cuenta de AWS ID al que pertenece este recurso.
- **Recuento de resultados:** indica el número de veces que este recurso se asoció a un resultado.
- **Generado más recientemente:** indica cuánto tiempo ha pasado desde que se generó por última vez un tipo de resultado asociado a este recurso.
- **Filtro de tipos de recursos:** de forma predeterminada, los datos se muestran para todos los tipos de recursos. Con este filtro, puede elegir ver los datos de un tipo de recurso específico, como Instance AccessKey, Lambda y otros.
- **Filtro de gravedad:** de forma predeterminada, los datos se muestran para todos los niveles de gravedad. Al usar este filtro, puede elegir ver los datos de otros niveles de gravedad. Las opciones posibles son Gravedad crítica, Gravedad alta, Gravedad media y Todos los niveles de gravedad.

## Resultados menos frecuentes

En esta sección, se destacan los tipos de búsqueda que se producen con poca frecuencia en su AWS entorno. Este widget está diseñado para ayudarle a identificar e investigar posibles patrones de amenazas emergentes.

El widget muestra los siguientes datos:

- Tipo de resultado: muestra el nombre del tipo de resultado.
- Recuento de resultados: indica el número de veces que se generó este tipo de resultado en el intervalo de tiempo elegido.
- Generado más recientemente: indica cuánto tiempo ha pasado desde que se generó este tipo de resultado por última vez.
- Filtro de gravedad: de forma predeterminada, los datos se muestran para los tipos de resultados de gravedad alta. Las opciones posibles para este campo son Gravedad crítica, Gravedad alta, Gravedad media y Todas las gravedades.

## Cobertura de los planes de protección

En esta sección se muestran las estadísticas de las cuentas de miembro de su organización. Muestra el número de cuentas de miembros que están habilitadas GuardDuty (detección de amenazas básica) en la región actual. Solo un GuardDuty administrador delegado puede ver las estadísticas de las cuentas de los miembros de su organización. Al crear una nueva AWS organización, es posible que se tarden hasta 24 horas en generar las estadísticas de toda la organización.

Cómo usar este widget

- Configuración: si un plan de protección no está configurado, elija Configurar en la columna Acciones.
- Visualización de las cuentas habilitadas: coloque el cursor sobre la barra de la columna Cuentas habilitadas para ver cuántas cuentas ha activado cada plan de protección. Para ver más detalles de la cuenta, seleccione la barra verde y elija Ver cuentas.

**Protection plans coverage** Last updated: 3 hours ago

GuardDuty coverage (foundational)  
[4/4 accounts](#)

| Protection plan                                      | Enabled accounts       | Actions                                                                                                                                                                                                              |
|------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S3 Protection                                        | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |
| EKS Protection                                       | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |
| Runtime monitoring                                   | <div><div></div></div> | <div> <div>Runtime monitoring</div> <div> <div><div></div> Enabled accounts 1</div> <div><div></div> Not enabled accounts 3</div> <div> <a href="#">Configure</a> <a href="#">View accounts</a> </div> </div> </div> |
| Automated agent management for EKS                   | <div><div></div></div> |                                                                                                                                                                                                                      |
| Automated agent configuration for Fargate (ECS only) | <div><div></div></div> |                                                                                                                                                                                                                      |
| Automated agent management for EC2                   | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |
| Malware Protection for EC2                           | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |
| Lambda Protection                                    | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |
| RDS Protection                                       | <div><div></div></div> | <a href="#">Configure</a>                                                                                                                                                                                            |

## Filtrar los hallazgos en GuardDuty

Un filtro de resultado le permite ver los resultados que coinciden con los criterios que especifique y filtrar los resultados que no coincidan. Puedes crear fácilmente filtros de búsqueda con la GuardDuty consola de Amazon o puedes crearlos con la [CreateFilter](#) API mediante JSON. Consulte las siguientes secciones para entender cómo crear un filtro en la consola. Para utilizar estos filtros con el objetivo de archivar automáticamente los resultados entrantes, consulte [Reglas de supresión en GuardDuty](#).

Cuando cree filtros, tenga en cuenta la siguiente lista:

- Puede especificar un mínimo de un atributo y un máximo de 50 atributos como criterios para un determinado filtro.
- Cuando se utiliza el operador igual que o no es igual que para filtrar por un valor de atributo, como ID de cuenta, se puede especificar un máximo de 50 valores.
- Cada atributo de los criterios de filtro se evalúa como un operador AND. Se evalúan varios valores para el mismo atributo como AND/OR.
- Para obtener información sobre el número máximo de filtros guardados que puedes crear Cuenta de AWS en cada uno de ellos Región de AWS, consulta [GuardDuty cuotas](#).

- Los campos de abajo `service.additionalInfo` se especifican utilizando su ruta JSON completa, igual que cualquier otro campo. Por ejemplo:  

```
{ "service.additionalInfo.sample": { "Equals": ["true"] } }.
```
- Los campos de fecha y hora aceptan valores en formato Unix Epoch de milisegundos (por ejemplo,). 1486685375000 Para obtener una lista completa de los campos de marca de tiempo, consulte la nota siguiente.

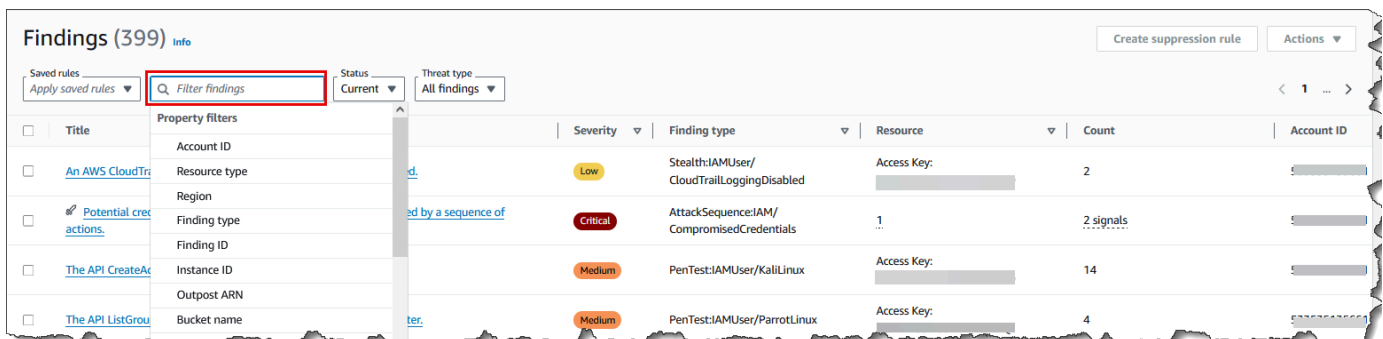
En las siguientes secciones se proporcionan instrucciones sobre cómo crear y guardar filtros mediante la GuardDuty consola y los comandos de API y CLI. Elija su método de acceso preferido para continuar.

## Crear y guardar el conjunto de filtros en la GuardDuty consola

Los filtros de búsqueda se pueden crear y probar a través de la GuardDuty consola. Puede guardar los filtros creados a través de la consola para utilizarlos en reglas de supresión o futuras operaciones de filtro. Un filtro se compone de al menos un criterio de filtro, que consiste en un atributo de filtro emparejado con al menos un valor.

Para crear y guardar criterios de filtro (consola)

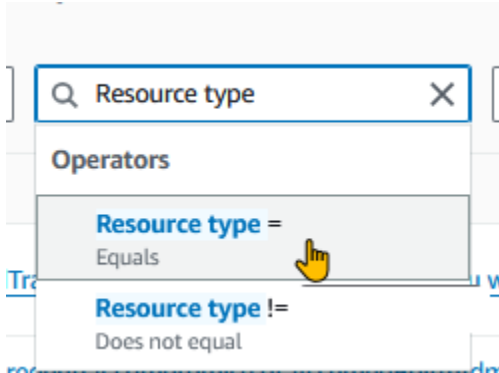
1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación izquierdo, elija Resultados.
3. En la página Resultados, seleccione la barra Filtrar resultados situada junto al menú Reglas guardadas. Aparecerá una lista ampliada de filtros de propiedades.



4. En la lista ampliada de filtros, seleccione un atributo en función del cual desee filtrar la tabla de resultados.

Por ejemplo, para ver los resultados en los que el recurso potencialmente afectado es un S3Bucket, elija el tipo de recurso.

5. En el caso de los operadores, elija uno que ayude a filtrar los resultados para obtener el resultado deseado. Para continuar con el ejemplo del paso anterior, elija Tipo de recurso =. Esto mostrará una lista de tipos de recursos GuardDuty.



Si su caso de uso requiere excluir resultados específicos, puede elegir el operador no es igual que o !=.

6. Especifique el valor del filtro de propiedades seleccionado. Si es necesario, seleccione Aplicar. Para continuar con el ejemplo del paso anterior, puede elegir S3Bucket.

Esto mostrará los resultados que coinciden con los filtros aplicados.

7. Para agregar más de un criterio de filtro, repita los pasos del 3 al 6.

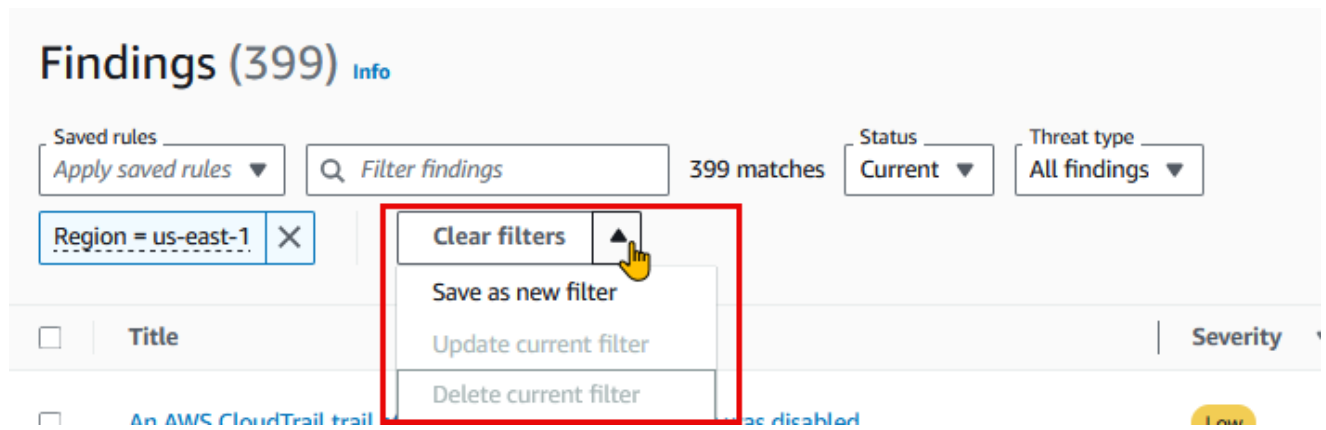
Para obtener una lista completa de los atributos, consulte [La propiedad filtra GuardDuty](#).

8. (Opcional) Guardar los atributos y valores especificados como filtros

Para volver a aplicar esta combinación de filtros en el futuro, puede guardar los atributos especificados y sus valores como un conjunto de filtros.

- a. Tras crear un criterio de filtro con uno o más filtros de propiedades, seleccione la flecha en el menú Borrar filtros.





- b. Introduzca el nombre del conjunto de filtros. El nombre debe tener entre 3 y 64 caracteres. Los caracteres válidos son a-z A-Z, 0-9, punto (.), guión (-) y guión bajo (\_).
- c. La descripción es opcional. Si introduce una descripción, puede tener 512 caracteres como máximo.
- d. Seleccione Crear.

## Crear y guardar un conjunto de filtros mediante GuardDuty API y CLI

Puede crear y probar los filtros de resultados mediante comandos de API o CLI. Un filtro se compone de al menos un criterio de filtro, que consiste en un atributo de filtro emparejado con al menos un valor. Puede guardar los filtros para crear [Reglas de supresión](#) o realizar otras operaciones de filtrado más adelante.

Para crear filtros de búsqueda mediante API/CLI

- Ejecute la [CreateFilter](#) API utilizando el ID del detector regional de la Cuenta de AWS lugar donde desea crear un filtro.

Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

- Como alternativa, puede usar la CLI [create-filter](#) para crear y guardar el filtro. Puede utilizar uno o más criterios de filtrado de [La propiedad filtra GuardDuty](#).

Utilice los siguientes ejemplos al sustituir los valores de los marcadores de posición que se muestran en rojo.

## Ejemplo 1: Cree un filtro nuevo para ver todos los resultados que coincidan con un tipo de resultado específico

En el siguiente ejemplo se crea un filtro que coincide con todos los resultados de PortScan para una instancia creada a partir de una imagen específica. Los valores de los marcadores de posición se muestran en rojo. Sustituya estos valores por valores adecuados para su cuenta. Por ejemplo, `12abc34d567e8fa901bc2d34EXAMPLE` sustitúyalo por el ID de tu detector regional.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"type": {"Equals": ["Recon:EC2/Portscan"]},  
"resource.instanceDetails.imageId": {"Equals": ["ami-0a7a207083example"]}} }'
```

## Ejemplo 2: cree un filtro nuevo para ver todos los resultados que coincidan con los niveles de gravedad

En el siguiente ejemplo, se crea un filtro que coincide con todos los resultados asociados a los niveles de gravedad HIGH. Los valores de los marcadores de posición se muestran en rojo. Sustituya estos valores por valores adecuados para su cuenta. Por ejemplo, `12abc34d567e8fa901bc2d34EXAMPLE` sustitúyalo por el ID de tu detector regional.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34EXAMPLE \  
--name FilterExampleName \  
--finding-criteria '{"Criterion": {"severity": {"Equals": ["7", "8"]}} }'
```

- Por API/CLI ejemplo, [Niveles de gravedad de los resultados](#) se representan como números. Para filtrar los resultados en función de los niveles de gravedad, utilice los siguientes valores:
- Para los niveles de gravedad LOW, utilice { "severity": { "Equals": ["1", "2", "3"] } }
- Para los niveles de gravedad MEDIUM, utilice { "severity": { "Equals": ["4", "5", "6"] } }
- Para los niveles de gravedad HIGH, utilice { "severity": { "Equals": ["7", "8"] } }
- Para los niveles de gravedad CRITICAL, utilice { "severity": { "Equals": ["9", "10"] } }

- Para resultados con varios niveles de gravedad, utilice valores de marcador de posición similares a los del siguiente ejemplo: { "severity": { "Equals": ["7", "8", "9", "10"] } }

En este ejemplo, se mostrarán los resultados que tienen niveles de gravedad HIGH o CRITICAL.

#### Note

Si se especifica un ejemplo con un solo valor numérico en lugar de todos los valores numéricos asociados a un nivel de gravedad, es posible que la API y la CLI muestren los resultados filtrados. Cuando utilice este conjunto de filtros guardado en la GuardDuty consola, no funcionará como se esperaba. Esto se debe a que la GuardDuty consola considera los valores del filtro como CRITICALHIGH, MEDIUM, y LOW. Por ejemplo, se espera que un filtro creado con un comando CLI que incluye { "severity": { "Equals": ["9"] } } muestre una salida adecuada en API/CLI. Sin embargo, este filtro guardado incluye un nivel de gravedad parcial cuando se utiliza en la GuardDuty consola y no mostrará el resultado esperado. Esto hace que sea necesario que la API y la CLI especifiquen todos los valores asociados a cada nivel de gravedad.

## La propiedad filtra GuardDuty

Al crear filtros u ordenar los resultados mediante las operaciones de la API, debe especificar los criterios de filtro en JSON. Estos criterios de filtro se correlacionan con el JSON de los detalles de un resultado. La siguiente tabla contiene una lista de los nombres que se muestran en la consola para los atributos del filtro y sus nombres de campo JSON equivalentes.

| Nombre de campo de la consola | Nombre del campo JSON |
|-------------------------------|-----------------------|
| ID de cuenta                  | accountId             |
| ID del resultado              | id                    |
| Región                        | region                |
| Gravedad                      | severity              |

| Nombre de campo de la consola     | Nombre del campo JSON                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | Puede filtrar los tipos de resultados en función de sus niveles de gravedad. Para obtener más información sobre los valores de gravedad, consulte <a href="#">Niveles de gravedad de GuardDuty los hallazgos</a> . Si lo usa severity con la API AWS CLI, o CloudFormation, se le asigna un valor numérico. Para obtener más información, consulta <a href="#">FindingCriteria</a> en la Amazon GuardDuty API Reference. |
| Tipo de resultado                 | type                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Actualizado a las                 | updatedAt                                                                                                                                                                                                                                                                                                                                                                                                                |
| ID de clave de acceso             | recurso.acceso KeyDetails.accessKeyId                                                                                                                                                                                                                                                                                                                                                                                    |
| ID principal                      | recurso.acceso KeyDetails.principalId                                                                                                                                                                                                                                                                                                                                                                                    |
| Nombre de usuario                 | recurso.acceso KeyDetails.userName                                                                                                                                                                                                                                                                                                                                                                                       |
| Tipo de usuario                   | recurso.acceso KeyDetails.userType                                                                                                                                                                                                                                                                                                                                                                                       |
| ID del perfil de instancia de IAM | recurso.instancia Details.iamInstanceProfile.id                                                                                                                                                                                                                                                                                                                                                                          |
| ID de instancia                   | recurso.instancia Details.instanceId                                                                                                                                                                                                                                                                                                                                                                                     |
| ID de imagen de la instancia      | recurso.instancia Details.imageId                                                                                                                                                                                                                                                                                                                                                                                        |
| Clave de etiqueta de instancia    | recurso.instancia Details.tags.key                                                                                                                                                                                                                                                                                                                                                                                       |
| Valor de etiqueta de instancia    | recurso.instancia Details.tags.value                                                                                                                                                                                                                                                                                                                                                                                     |
| Dirección IPv6                    | recurso.instancia Details.networkInterfaces.ipv6Addresses                                                                                                                                                                                                                                                                                                                                                                |
| Dirección IPv4 privada            | recurso.instancia Details.networkInterfaces.privateIpAddresses.privateIpAddress                                                                                                                                                                                                                                                                                                                                          |

| Nombre de campo de la consola   | Nombre del campo JSON                                                    |
|---------------------------------|--------------------------------------------------------------------------|
| Nombre DNS público              | recurso.instancia Details.networkInterfaces.p<br>ublicDnsName            |
| IP pública                      | recurso.instancia Details.networkInterfaces.p<br>ublicIp                 |
| ID de grupo de seguridad        | recurso.instancia Details.networkInterfaces.s<br>ecurityGroups.groupId   |
| Nombre del grupo de seguridad   | recurso.instancia Details.networkInterfaces.s<br>ecurityGroups.groupName |
| ID de subred                    | recurso.instancia Details.networkInterfaces.s<br>ubnetId                 |
| ID de VPC                       | recurso.instancia Details.networkInterfaces.v<br>pcId                    |
| ARN de Outpost                  | recurso.instancia Details.outpostARN                                     |
| Tipo de recurso                 | resource.resourceType                                                    |
| Permisos de bucket              | recursos.3 BucketDetails.publicAccess.effective<br>Permission            |
| Nombre del bucket               | recursos.3 BucketDetails.name                                            |
| Clave de la etiqueta del bucket | recursos.3 BucketDetails.tags.key                                        |
| valor de la etiqueta del bucket | recursos.3 BucketDetails.tags.value                                      |
| Tipo de bucket                  | recursos.3 BucketDetails.type                                            |
| Tipo de acción                  | service.action.actionType                                                |
| API llamada                     | service.action.aws ApiCallAction.api                                     |
| Tipo de intermediario de la API | service.action.aws ApiCallAction.callerType                              |

| Nombre de campo de la consola                       | Nombre del campo JSON                                                |
|-----------------------------------------------------|----------------------------------------------------------------------|
| Código de error de la API                           | service.action.aws ApiCallAction.errorCode                           |
| Ciudad del intermediario de la API                  | service.action.aws ApiCallAction.remoteIpDetails.city.cityName       |
| País del intermediario de la API                    | service.action.aws ApiCallAction.remoteIpDetails.country.countryName |
| Dirección IPv4 del intermediario de la API          | service.action.aws ApiCallAction.remoteIpDetails.ipAddressV4         |
| Dirección IPv6 de quien realiza la llamada a la API | service.action.aws ApiCallAction.remoteIpDetails.ipAddressV6         |
| ID de ASN del intermediario de la API               | service.action.aws ApiCallAction.remoteIpDetails.organization.asn    |
| Nombre ASN del intermediario de la API              | service.action.aws ApiCallAction.remoteIpDetails.organization.asnOrg |
| Nombre del servicio del intermediario de la API     | service.action.aws ApiCallAction.serviceName                         |
| Dominio de la solicitud DNS                         | service.action.dns RequestAction.domain                              |
| Sufijo de dominio de solicitud de DNS               | service.action.dns RequestAction.domainWithSuffix                    |
| Conexión de red bloqueada                           | service.action.network ConnectionAction.blocked                      |
| Dirección de la conexión de red                     | service.action.network ConnectionAction.connectionDirection          |
| Puerto local de la conexión de red                  | service.action.network ConnectionAction.localPortDetails.port        |
| Protocolo de conexión de red                        | service.action.network ConnectionAction.protocol                     |

| Nombre de campo de la consola                                     | Nombre del campo JSON                                                       |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Ciudad de la conexión de red                                      | service.action.network ConnectionAction.remoteIpDetails.city.cityName       |
| País de la conexión de red                                        | service.action.network ConnectionAction.remoteIpDetails.country.countryName |
| Dirección IPv4 remota de la conexión de red                       | service.action.network ConnectionAction.remoteIpDetails.ipAddressV4         |
| Dirección IPv6 remota de la conexión de red                       | service.action.network ConnectionAction.remoteIpDetails.ipAddressV6         |
| ID de ASN de la IP remota de la conexión de red                   | service.action.network ConnectionAction.remoteIpDetails.organization.asn    |
| Nombre ASN de la IP remota de la conexión de red                  | service.action.network ConnectionAction.remoteIpDetails.organization.asnOrg |
| Puerto remoto de la conexión de red                               | service.action.network ConnectionAction.remotePortDetails.port              |
| Cuenta remota afiliada                                            | service.action.aws ApiCallAction.remoteAccountDetails.affiliated            |
| Dirección IPv4 de la persona que llama a la API de Kubernetes     | service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV4         |
| Dirección IPv6 de quien realiza la llamada a la API de Kubernetes | service.action.kubernetes ApiCallAction.remoteIpDetails.ipAddressV6         |
| Espacio de nombres de Kubernetes                                  | service.action.kubernetes ApiCallAction.name space                          |
| ID de ASN de quien realiza la llamada a la API de Kubernetes      | service.action.kubernetes ApiCallAction.remoteIpDetails.organization.asn    |
| URI de solicitud de llamada a la API de Kubernetes                | service.action.kubernetes ApiCallAction.requestUri                          |

| Nombre de campo de la consola                          | Nombre del campo JSON                                                           |
|--------------------------------------------------------|---------------------------------------------------------------------------------|
| Código de estado de la API de Kubernetes               | service.action.kubernetes ApiCallAction.stat<br>usCode                          |
| Dirección IPv4 local de conexión de red                | service.action.network ConnectionAction.l<br>ocalIpDetails.ipAddressV4          |
| Dirección IPv6 local de la conexión de red             | service.action.network ConnectionAction.l<br>ocalIpDetails.ipAddressV6          |
| Protocolo                                              | service.action.network ConnectionAction.p<br>rotocol                            |
| Nombre del servicio de llamada a la API                | service.action.aws ApiCallAction.serviceName                                    |
| ID de cuenta de la persona que llama a la API          | service.action.aws ApiCallAction.remo<br>teAccountDetails.accountId             |
| Nombre de la lista de amenazas                         | servicio.adicional Info.threatListName                                          |
| Rol de recurso                                         | service.resourceRole                                                            |
| Nombre del clúster de EKS                              | resource.eks ClusterDetails.name                                                |
| Nombre de la carga de trabajo de Kubernetes            | resource.kubernetes Details.kubernetes<br>WorkloadDetails.name                  |
| Nombre de espacio de la carga de trabajo de Kubernetes | recurso.kubernetes Details.kubernetes<br>WorkloadDetails.namespace              |
| Nombre de usuario de Kubernetes                        | recurso.kubernetes Details.kubernetes<br>UserDetails.username                   |
| Imagen del contenedor de Kubernetes                    | recurso.kubernetes Details.kubernetes<br>WorkloadDetails.containers.image       |
| Prefijo de la imagen del contenedor de Kubernetes      | recurso.kubernetes Details.kubernetes<br>WorkloadDetails.containers.imagePrefix |



| Nombre de campo de la consola                        | Nombre del campo JSON                                                                        |
|------------------------------------------------------|----------------------------------------------------------------------------------------------|
| ID de análisis                                       | service.ebs VolumeScanDetails.scanId                                                         |
| Nombre de la amenaza de análisis de volúmenes de EBS | service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.name           |
| Nombre de la amenaza de análisis de objetos de S3    | servicio.malware ScanDetails.threats.name                                                    |
| Gravedad de la amenaza                               | service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.severity       |
| SHA de archivo                                       | service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePaths.hash |
| Nombre del clúster de ECS                            | resource.ecs ClusterDetails.name                                                             |
| Imagen del contenedor de ECS                         | resource.ecs ClusterDetails.taskDetails.containers.image                                     |
| ARN de definición de tarea de ECS                    | resource.ecs ClusterDetails.taskDetails.definitionArn                                        |
| Imagen de contenedor independiente                   | recurso.contenedor Details.image                                                             |
| ID de instancia de base de datos                     | resource.rds DbInstanceDetails.dbInstanceId                                                  |
| ID de clúster de base de datos                       | resource.rds DbInstanceDetails.dbClusterIdentifier                                           |
| Motor de base de datos                               | resource.rds DbInstanceDetails.engine                                                        |
| Usuario de base de datos                             | resource.rds DbUserDetails.user                                                              |

| Nombre de campo de la consola             | Nombre del campo JSON                             |
|-------------------------------------------|---------------------------------------------------|
| Ejecutable SHA-256                        | service.runtime Details.process.executableSHA256  |
| Process name (Nombre del proceso)         | servicio.runtime Details.process.name             |
| Ruta de ejecución                         | servicio.runtime Details.process.executablePath   |
| Nombre de la función Lambda               | recurso.lambda Details.functionName               |
| ARN de la función Lambda                  | recurso.lambda Details.functionArn                |
| Clave de etiqueta de la función de Lambda | recurso.lambda Details.tags.key                   |
| Valor de etiqueta de la función de Lambda | recurso.lambda Details.tags.value                 |
| Dominio de la solicitud DNS               | service.action.dns RequestAction.domainWithSuffix |

Todos los demás campos de búsqueda (que se enumeran a continuación) están disponibles únicamente como criterios de filtrado de reglas de supresión (utilizando y). [CreateFilterUpdateFilter](#) Estos campos no son compatibles con otras operaciones de la API. Las reglas de supresión que utilizan estos campos se deben crear o actualizar a través de la API. Estos campos solo se pueden aplicar a los filtros con una ARCHIVE acción.

#### Note

Los siguientes campos aceptan valores de marca horaria en formato de milisegundos de Unix Epoch (por ejemplo, 1262309025000 representan el viernes 1 de enero de 2010 a las 1:23:45 a.m. GMT):

- createdAt
- updatedAt
- servicio.evento FirstSeen
- servicio.evento LastSeen
- recurso.instancia Details.launchTime
- recurso.lambda Details.lastModifiedAt

- recursos.3 BucketDetails.createdAt
- resource.eks ClusterDetails.createdAt
- resource.ecs ClusterDetails.taskDetails.createdAt
- resource.ecs ClusterDetails.taskDetails.startedAt
- service.ebs VolumeScanDetails.scanStartedAt
- service.ebs VolumeScanDetails.scanCompletedAt
- servicio.tiempo de ejecución Details.context.modifiedAt
- servicio.runtime Details.context.modifyingProcess.startTime
- servicio.runtime Details.context.modifyingProcess.lineage.startTime
- servicio.runtime Details.context.targetProcess.startTime
- servicio.runtime Details.context.targetProcess.lineage.startTime
- servicio.runtime Details.process.startTime
- servicio.runtime Details.process.lineage.startTime
- service.detection.sequence.actors.session.CreatedTime
- Service.Detection.Sequence.Signals.Creado en
- Service.Detection.Sequence.Signals.actualizado en
- service.detection.sequence.signals.first SeenAt
- servicio.detection.secuence.signals.last SeenAt
- service.detection.sequence.resources.data.s3 Bucket.createdAt
- service.detection.sequence.resources.data.ecs Task.createdAt
- service.detection.sequence.resources.data.eks Cluster.createdAt

## Nombre del campo JSON

arn

asociado AttackSequenceArn

createdAt

partición

recurso.acceso KeyDetails.userIdentity.accessKeyId

recurso.acceso KeyDetails.userIdentity.accountId

recurso.acceso KeyDetails.userIdentity.arn

## Nombre del campo JSON

recurso.acceso KeyDetails.userIdentity.principalId

recurso.acceso KeyDetails.userIdentity.sessionContext.attributes.mfaAuthenticated

recurso.acceso KeyDetails.userIdentity.sessionContext.ec2RoleDelivery

recurso.acceso KeyDetails.userIdentity.sessionContext.invokedBy

recurso.acceso KeyDetails.userIdentity.sessionContext.sessionIssuer.accountId

recurso.acceso KeyDetails.userIdentity.sessionContext.sessionIssuer.arn

recurso.acceso KeyDetails.userIdentity.sessionContext.sessionIssuer.principalId

recurso.acceso KeyDetails.userIdentity.sessionContext.sessionIssuer.type

recurso.acceso KeyDetails.userIdentity.sessionContext.sessionIssuer.userName

recurso.acceso KeyDetails.userIdentity.sessionContext.sourceIdentity

recurso.acceso KeyDetails.userIdentity.sessionContext.webIdFederationData.attributes

recurso.acceso KeyDetails.userIdentity.sessionContext.webIdFederationData.federatedProvider

recurso.acceso KeyDetails.userIdentity.type

recurso.acceso KeyDetails.userIdentity.userName

recurso.roca madre GuardrailDetails.guardrailArn

recurso.roca madre GuardrailDetails.guardrailVersion

recurso.contenedor Details.containerRuntime

recurso.contenedor Details.imagePrefix

recurso.contenedor Details.securityContext.allowPrivilegeEscalation

recurso.contenedor Details.securityContext.privileged

## Nombre del campo JSON

recurso.contenedor Details.volumeMounts.mountPath

recurso.contenedor Details.volumeMounts.name

recurso.ebs VolumeDetails.scannedVolumeDetails.deviceName

resource.ebs VolumeDetails.scannedVolumeDetails.encryptionType

resource.ebs VolumeDetails.scannedVolumeDetails.kmsKeyArn

resource.ebs VolumeDetails.scannedVolumeDetails.snapshotArn

resource.ebs VolumeDetails.scannedVolumeDetails.volumeArn

resource.ebs VolumeDetails.scannedVolumeDetails.volumeSizeInGB

resource.ebs VolumeDetails.scannedVolumeDetails.volumeType

resource.ebs VolumeDetails.skippedVolumeDetails.deviceName

resource.ebs VolumeDetails.skippedVolumeDetails.encryptionType

resource.ebs VolumeDetails.skippedVolumeDetails.kmsKeyArn

resource.ebs VolumeDetails.skippedVolumeDetails.snapshotArn

resource.ebs VolumeDetails.skippedVolumeDetails.volumeArn

resource.ebs VolumeDetails.skippedVolumeDetails.volumeSizeInGB

resource.ebs VolumeDetails.skippedVolumeDetails.volumeType

resource.ecs ClusterDetails.activeServicesCount

resource.ecs ClusterDetails.arn

resource.ecs ClusterDetails.registeredContainerInstancesCount

resource.ecs ClusterDetails.runningTasksCount

## Nombre del campo JSON

resource.ecs ClusterDetails.status

resource.ecs ClusterDetails.tags.key

resource.ecs ClusterDetails.tags.value

resource.ecs ClusterDetails.taskDetails.arn

resource.ecs ClusterDetails.taskDetails.containers.containerRuntime

resource.ecs ClusterDetails.taskDetails.containers.id

resource.ecs ClusterDetails.taskDetails.containers.imagePrefix

resource.ecs ClusterDetails.taskDetails.containers.name

resource.ecs ClusterDetails.taskDetails.containers.securityContext.allowPrivilegeEscalation

resource.ecs ClusterDetails.taskDetails.containers.securityContext.privileged

resource.ecs ClusterDetails.taskDetails.containers.volumeMounts.mountPath

resource.ecs ClusterDetails.taskDetails.containers.volumeMounts.name

resource.ecs ClusterDetails.taskDetails.createdAt

resource.ecs ClusterDetails.taskDetails.group

resource.ecs ClusterDetails.taskDetails.launchType

resource.ecs ClusterDetails.taskDetails.startedAt

resource.ecs ClusterDetails.taskDetails.startedBy

resource.ecs ClusterDetails.taskDetails.tags.key

resource.ecs ClusterDetails.taskDetails.tags.value

resource.ecs ClusterDetails.taskDetails.version

## Nombre del campo JSON

resource.ecs ClusterDetails.taskDetails.volumes.hostPath.path

resource.ecs ClusterDetails.taskDetails.volumes.name

resource.eks ClusterDetails.arn

resource.eks ClusterDetails.createdAt

resource.eks ClusterDetails.status

resource.eks ClusterDetails.tags.key

resource.eks ClusterDetails.tags.value

resource.eks ClusterDetails.vpcId

recurso.instancia Details.iamInstanceProfile.arn

recurso.instancia Details.instanceState

recurso.instancia Details.instanceType

recurso.instancia Details.launchTime

recurso.instancia Details.networkInterfaces.networkInterfaceId

recurso.instancia Details.networkInterfaces.privateDnsName

recurso.instancia Details.networkInterfaces.privateIpAddress

recurso.instancia Details.networkInterfaces.privateIpAddresses.privateDnsName

recurso.instancia Details.platform

recurso.instancia Details.productCodes.productCodeId

recurso.instancia Details.productCodes.productCodeType

recurso.kubernetes Details.kubernetesUserDetails.groups

## Nombre del campo JSON

recurso.kubernetes Details.kubernetesUserDetails.impersonatedUser.groups

recurso.kubernetes Details.kubernetesUserDetails.impersonatedUser.username

recurso.kubernetes Details.kubernetesUserDetails.sessionName

recurso.kubernetes Details.kubernetesUserDetails.uid

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.containerRuntime

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.id

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.name

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.allowPrivilegeEscalation

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.securityContext.privileged

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.mountPath

recurso.kubernetes Details.kubernetesWorkloadDetails.containers.volumeMounts.name

recurso.kubernetes Details.kubernetesWorkloadDetails.hostIpc

recurso.kubernetes Details.kubernetesWorkloadDetails.hostNetwork

recurso.kubernetes Details.kubernetesWorkloadDetails.hostPid

recurso.kubernetes Details.kubernetesWorkloadDetails.serviceAccountName

recurso.kubernetes Details.kubernetesWorkloadDetails.type

recurso.kubernetes Details.kubernetesWorkloadDetails.uid

recurso.kubernetes Details.kubernetesWorkloadDetails.volumes.hostPath.path

recurso.kubernetes Details.kubernetesWorkloadDetails.volumes.name

recurso.lambda Details.description



## Nombre del campo JSON

recurso.lambda Details.lastModifiedAt

recurso.lambda Details.revisionId

recurso.lambda Details.vpcConfig.securityGroups.groupId

recurso.lambda Details.vpcConfig.securityGroups.groupName

recurso.lambda Details.vpcConfig.subnetIds

recurso.lambda Details.vpcConfig.vpcId

resource.rds DbInstanceDetails.dbInstanceArn

resource.rds DbInstanceDetails.dbiResourceId

resource.rds DbInstanceDetails.dbSecurityGroups.name

resource.rds DbInstanceDetails.dbSecurityGroups.status

resource.rds DbInstanceDetails.engineVersion

resource.rds DbInstanceDetails.iamDatabaseAuthenticationEnabled

resource.rds DbInstanceDetails.publiclyAccessible

resource.rds DbInstanceDetails.vpcId

resource.rds DbInstanceDetails.vpcSecurityGroups.status

resource.rds DbInstanceDetails.vpcSecurityGroups.vpcSecurityGroupId

resource.rds DbUserDetails.application

resource.rds DbUserDetails.authMethod

resource.rds DbUserDetails.database

resource.rds DbUserDetails.ssl

## Nombre del campo JSON

resource.rds LimitlessDbDetails.dbClusterIdentifier

resource.rds LimitlessDbDetails.dbShardGroupArn

resource.rds LimitlessDbDetails.dbShardGroupIdentifier

resource.rds LimitlessDbDetails.dbShardGroupResourceId

resource.rds LimitlessDbDetails.engine

resource.rds LimitlessDbDetails.engineVersion

resource.rds LimitlessDbDetails.tags.key

resource.rds LimitlessDbDetails.tags.value

recursos.3 BucketDetails.arn

recursos.3 BucketDetails.createdAt

recursos.3 BucketDetails.defaultServerSideEncryption.encryptionType

recursos.3 BucketDetails.defaultServerSideEncryption.kmsMasterKeyArn

recursos.3 BucketDetails.owner.id

recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicAcls

recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.blockPublicPolicy

recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.ignorePublicAcls

recursos.3 BucketDetails.publicAccess.permissionConfiguration.accountLevelPermissions.blockPublicAccess.restrictPublicBuckets

## Nombre del campo JSON

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicReadAccess

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.accessControlList.allowsPublicWriteAccess

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicAcls

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.blockPublicPolicy

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.ignorePublicAcls

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess

recursos.3 BucketDetails.publicAccess.permissionConfiguration.bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess

recursos.3 BucketDetails.s3ObjectDetails.eTag

recursos.3 BucketDetails.s3ObjectDetails.hash

recursos.3 BucketDetails.s3ObjectDetails.key

recursos.3 BucketDetails.s3ObjectDetails.objectArn

recursos.3 BucketDetails.s3ObjectDetails.versionId

schemaVersion

service.action.aws ApiCallAction.domainDetails.domain

service.action.aws ApiCallAction.remoteIpDetails.country.countryCode

## Nombre del campo JSON

service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lat

service.action.aws ApiCallAction.remoteIpDetails.geoLocation.lon

service.action.aws ApiCallAction.remoteIpDetails.organization.isp

service.action.aws ApiCallAction.remoteIpDetails.organization.org

service.action.aws ApiCallAction.userAgent

service.action.dns RequestAction.blocked

service.action.dns RequestAction.protocol

service.action.kubernetes ApiCallAction.parameters

service.action.kubernetes ApiCallAction.remoteIpDetails.country.countryCode

service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lat

service.action.kubernetes ApiCallAction.remoteIpDetails.geoLocation.lon

service.action.kubernetes ApiCallAction.resource

service.action.kubernetes ApiCallAction.resourceName

service.action.kubernetes ApiCallAction.sourceIPs

service.action.kubernetes ApiCallAction.subresource

service.action.kubernetes ApiCallAction.userAgent

service.action.kubernetes ApiCallAction.verb

service.action.kubernetes PermissionCheckedDetails.allowed

service.action.kubernetes PermissionCheckedDetails.namespace

service.action.kubernetes PermissionCheckedDetails.resource

## Nombre del campo JSON

service.action.kubernetes PermissionCheckedDetails.verb

service.action.kubernetes RoleBindingDetails.kind

service.action.kubernetes RoleBindingDetails.name

service.action.kubernetes RoleBindingDetails.roleRefKind

service.action.kubernetes RoleBindingDetails.roleRefName

service.action.kubernetes RoleBindingDetails.uid

service.action.kubernetes RoleDetails.kind

service.action.kubernetes RoleDetails.name

service.action.kubernetes RoleDetails.uid

service.action.network ConnectionAction.localNetworkInterface

service.action.network ConnectionAction.localPortDetails.portName

service.action.network ConnectionAction.remoteIpDetails.country.countryCode

service.action.network ConnectionAction.remoteIpDetails.geoLocation.lat

service.action.network ConnectionAction.remoteIpDetails.geoLocation.lon

service.action.network ConnectionAction.remoteIpDetails.organization.isp

service.action.network ConnectionAction.remoteIpDetails.organization.org

service.action.network ConnectionAction.remotePortDetails.portName

service.action.port ProbeAction.blocked

service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV4

service.action.port ProbeAction.portProbeDetails.localIpDetails.ipAddressV6

## Nombre del campo JSON

service.action.port ProbeAction.portProbeDetails.localPortDetails.port

service.action.port ProbeAction.portProbeDetails.localPortDetails.portName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.city.cityName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryCode

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.country.countryName

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lat

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.geoLocation.lon

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV4

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.ipAddressV6

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asn

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.asnOrg

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.isp

service.action.port ProbeAction.portProbeDetails.remoteIpDetails.organization.org

service.action.rds LoginAttemptAction.loginAttributes.application

service.action.rds LoginAttemptAction.loginAttributes.failedLoginAttempts

service.action.rds LoginAttemptAction.loginAttributes.successfulLoginAttempts

service.action.rds LoginAttemptAction.loginAttributes.user

service.action.rds LoginAttemptAction.remoteIpDetails.city.cityName

service.action.rds LoginAttemptAction.remoteIpDetails.country.countryCode

service.action.rds LoginAttemptAction.remoteIpDetails.country.countryName

## Nombre del campo JSON

service.action.rds LoginAttemptAction.remotepDetails.geoLocation.lat

service.action.rds LoginAttemptAction.remotepDetails.geoLocation.lon

service.action.rds LoginAttemptAction.remotepDetails.ipAddressV4

service.action.rds LoginAttemptAction.remotepDetails.ipAddressV6

service.action.rds LoginAttemptAction.remotepDetails.organization.asn

service.action.rds LoginAttemptAction.remotepDetails.organization.asnOrg

service.action.rds LoginAttemptAction.remotepDetails.organization.isp

service.action.rds LoginAttemptAction.remotepDetails.organization.org

servicio.adicional Info.agentDetails.agentId

servicio.adicional Info.agentDetails.agentVersion

servicio.adicional Info.anomalies.anomalousAPIs

servicio.adicional Info.authenticationMethod

servicio.adicional Info.averagePacketSizeIn

servicio.adicional Info.averagePacketSizeOut

servicio.adicional Info.context

servicio.adicional Info.domain

servicio.adicional Info.inBytes

servicio.adicional Info.localNetworkInterfaceOwner

servicio.adicional Info.localPort

servicio.adicional Info.outBytes

## Nombre del campo JSON

`servicio.adicional Info.packetsIn`

`servicio.adicional Info.packetsOut`

`servicio.adicional Info.policyArn`

`servicio.adicional Info.policyName`

`servicio.adicional Info.remotePort`

`servicio.adicional Info.sample`

`servicio.adicional Info.scannedPort`

`servicio.adicional Info.threatFileSha256`

`servicio.adicional Info.threatName`

`servicio.adicional Info.totalBytesIn`

`servicio.adicional Info.totalBytesOut`

`servicio.adicional Info.type`

`servicio.adicional Info.unusual.asnOrg`

`servicio.adicional Info.unusual.port`

`servicio.adicional Info.unusualProtocol`

`servicio.adicional Info.userAgent.fullUserAgent`

`servicio.adicional Info.userAgent.userAgentCategory`

`servicio.adicional Info.value`

`servicio.adicional Info.vpcOwnerAccountId`

`service.count`



## Nombre del campo JSON

service.detection.sequence.actors.id

service.detection.sequence.actors.process.name

service.detection.sequence.actors.process.path

service.detection.sequence.actors.process.sha256

Service.Detection.Sequence.actors.Session.CreatedTime

service.detection.sequence.actors.session.issuer

Estado de service.detection.Sequence.actors.Session.MFAST

service.detection.sequence.actors.session.uid

service.detection.sequence.actors.user.account.account

service.detection.sequence.actors.user.account.uid

service.detection.sequence.actors.user.CredentialUID

service.detection.sequence.actors.user.name

service.detection.sequence.actors.user.type

service.detection.sequence.actors.user.uid

servicio.detection.sequence.adicional SequenceTypes

servicio.detección.secuencia.descripcion

servicio.detección.secuencia.endpoints.autónomo System.name

servicio.detection.sequence.endpoints.autonomous System.number

servicio.detección.secuencia.endpoints.conexión.dirección

service.detection.sequence.endpoints.domain

## Nombre del campo JSON

service.detection.sequence.endpoints.id

service.detection.sequence.endpoints.ip

service.detection.sequence.endpoints.location.city

servicio.detección.secuencia.endpoints.ubicación.país

service.detection.sequence.endpoints.location.lat

service.detection.sequence.endpoints.location.lon

servicio.detection.sequence.endpoints.port

service.detection.sequence.resources.accountID

Service.Detection.Sequence.Resources.CloudPartition

service.detection.sequence.resources.data.access Key.principalId

service.detection.sequence.resources.data.access Key.userName

service.detection.sequence.resources.data.access Key.userType

service.detection.sequence.resources.data.autoscaling AutoScalingGroup.ec2InstanceUids

service.detection.sequence.resources.data.cloudformation Stack.ec2InstanceUids

service.detection.sequence.resources.data.container.image

service.detection.sequence.resources.data.container.imageUID

service.detection.sequence.resources.data.ec2 Image.ec2InstanceUids

service.detection.sequence.resources.data.ec2 Instance.availabilityZone

service.detection.sequence.resources.data.ec2 Instance.ec2NetworkInterfaceUids

service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.arn

## Nombre del campo JSON

service.detection.sequence.resources.data.ec2 Instance.iamInstanceProfile.id

service.detection.sequence.resources.data.ec2 Instance.imageDescription

service.detection.sequence.resources.data.ec2 Instance.instanceState

service.detection.sequence.resources.data.ec2 Instance.instanceType

service.detection.sequence.resources.data.ec2 Instance.outpostArn

service.detection.sequence.resources.data.ec2 Instance.platform

service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeId

service.detection.sequence.resources.data.ec2 Instance.productCodes.productCodeType

service.detection.sequence.resources.data.ec2 LaunchTemplate.ec2InstanceUids

service.detection.sequence.resources.data.ec2 LaunchTemplate.version

service.detection.sequence.resources.data.ec2 NetworkInterface.ipv6Addresses

service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateDnsName

service.detection.sequence.resources.data.ec2 NetworkInterface.privateIpAddresses.privateIpAddress

service.detection.sequence.resources.data.ec2 NetworkInterface.publicIp

service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupId

service.detection.sequence.resources.data.ec2 NetworkInterface.securityGroups.groupName

service.detection.sequence.resources.data.ec2 NetworkInterface.subnetId

service.detection.sequence.resources.data.ec2 NetworkInterface.vpcId

service.detection.sequence.resources.data.ec2 Vpc.ec2InstanceUids

## Nombre del campo JSON

service.detection.sequence.resources.data.ecs Cluster.ec2InstanceUids

service.detection.sequence.resources.data.ecs Cluster.status

service.detection.sequence.resources.data.ecs Task.containerUids

service.detection.sequence.resources.data.ecs Task.createdAt

service.detection.sequence.resources.data.ecs Task.launchType

service.detection.sequence.resources.data.ecs Task.taskDefinitionArn

service.detection.sequence.resources.data.eks Cluster.arn

service.detection.sequence.resources.data.eks Cluster.createdAt

service.detection.sequence.resources.data.eks Cluster.ec2InstanceUids

service.detection.sequence.resources.data.eks Cluster.status

service.detection.sequence.resources.data.eks Cluster.vpcId

service.detection.sequence.resources.data.iam InstanceProfile.ec2InstanceUids

service.detection.sequence.resources.data.iam InstanceProfile.id

service.detection.sequence.resources.data.kubernetes Workload.containerUids

service.detection.sequence.resources.data.kubernetes Workload.namespace

service.detection.sequence.resources.data.kubernetes Workload.type

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclAccess

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicAclIgnoreBehavior

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicBucketRestrictBehavior

## Nombre del campo JSON

service.detection.sequence.resources.data.s3 Bucket.accountPublicAccess.publicPolicyAccess

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclAccess

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicAclIgnoreBehavior

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicBucketRestrictBehavior

service.detection.sequence.resources.data.s3 Bucket.bucketPublicAccess.publicPolicyAccess

service.detection.sequence.resources.data.s3 Bucket.createdAt

service.detection.sequence.resources.data.s3 Bucket.effectivePermission

service.detection.sequence.resources.data.s3 Bucket.encryptionKeyArn

service.detection.sequence.resources.data.s3 Bucket.encryptionType

service.detection.sequence.resources.data.s3 Bucket.ownerId

service.detection.sequence.resources.data.s3 Bucket.publicReadAccess

service.detection.sequence.resources.data.s3 Bucket.publicWriteAccess

service.detection.sequence.resources.data.s3 Bucket.s3ObjectUids

service.detection.sequence.resources.data.s3 Object.eTag

service.detection.sequence.resources.data.s3 Object.key

service.detection.sequence.resources.data.s3 Object.versionId

servicio.detection.sequence.resources.name

servicio.detección.secuencia.recursos.región

service.detection.sequence.resources.resourceType

## Nombre del campo JSON

`servicio.detection.sequence.resources.service`

`service.detection.sequence.resources.tags.key`

`service.detection.sequence.resources.tags.value`

`service.detection.sequence.resources.uid`

`servicio.detección.secuencia.secuencia Indicators.key`

`servicio.detección.secuencia.secuencia Indicators.title`

`servicio.detección.secuencia.secuencia Indicators.values`

`Service.Detection.Sequence.Signals.ActorIDs`

`service.detection.sequence.signals.count`

`service.detection.Sequence.Signals. Creado en`

`servicio.detection.sequence.signals.descripcion`

`Service.Detection.Sequence.Signals.Endpoint ID`

`service.detection.sequence.signals.first SeenAt`

`servicio.detection.secuence.signals.last SeenAt`

`servicio.detection.sequence.signals.name`

`UIDs de service.detection.sequence.signals.resourceUIDs`

`servicio.detection.secuence.signals.severidad`

`servicio.detección.secuencia.señals.señal Indicators.key`

`servicio.detección.secuencia.señales.señal Indicators.title`

`servicio.detección.secuencia.señales.señal Indicators.values`

## Nombre del campo JSON

`servicio.detección.secuencia.señals.tipo`

`service.detection.sequence.signals.uid`

`service.detection.sequence.signals.actualizado en`

`service.detection.sequence.uid`

## Service.DetectorID

`service.ebs VolumeScanDetails.scanCompletedAt`

`service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.count`

`service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.severity`

`service.ebs VolumeScanDetails.scanDetections.highestSeverityThreatDetails.threatName`

`service.ebs VolumeScanDetails.scanDetections.scannedItemCount.files`

`service.ebs VolumeScanDetails.scanDetections.scannedItemCount.totalGb`

`service.ebs VolumeScanDetails.scanDetections.scannedItemCount.volumes`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.itemCount`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.shortened`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.fileName`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.filePath`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.filePath.volumeArn`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.threatNames.itemCount`

`service.ebs VolumeScanDetails.scanDetections.threatDetectedByName.uniqueThreatNameCount`

## Nombre del campo JSON

service.ebs VolumeScanDetails.scanDetections.threatsDetectedItemCount.files

service.ebs VolumeScanDetails.scanStartedAt

service.ebs VolumeScanDetails.scanType

service.ebs VolumeScanDetails.sources

servicio.evento FirstSeen

servicio.evento LastSeen

servicio.malware ScanDetails.scanCategory

servicio.malware ScanDetails.scanConfiguration.incrementalScanDetails.baselineResourceArn

servicio.malware ScanDetails.scanConfiguration.triggerType

servicio.malware ScanDetails.threats.count

servicio.malware ScanDetails.threats.hash

servicio.malware ScanDetails.threats.itemDetails.additionalInfo.deviceName

servicio.malware ScanDetails.threats.itemDetails.additionalInfo.versionId

servicio.malware ScanDetails.threats.itemDetails.hash

servicio.malware ScanDetails.threats.itemDetails.itemPath

servicio.malware ScanDetails.threats.itemDetails.resourceArn

servicio.malware ScanDetails.threats.itemPaths.hash

servicio.malware ScanDetails.threats.itemPaths.nestedItemPath

servicio.malware ScanDetails.threats.source

servicio.malware ScanDetails.uniqueThreatCount



## Nombre del campo JSON

`servicio.tiempo de ejecución Details.context.addressFamily`

`servicio.runtime Details.context.commandLineExample`

`servicio.runtime Details.context.fileSystemType`

`servicio.runtime Details.context.flags`

`servicio.runtime Details.context.ianaProtocolNumber`

`servicio.runtime Details.context.ldPreloadValue`

`servicio.runtime Details.context.libraryPath`

`servicio.runtime Details.context.memoryRegions`

`servicio.runtime Details.context.modifiedAt`

`servicio.runtime Details.context.modifyingProcess.euid`

`servicio.runtime Details.context.modifyingProcess.executablePath`

`servicio.runtime Details.context.modifyingProcess.executableSha256`

`servicio.runtime Details.context.modifyingProcess.lineage.euid`

`servicio.runtime Details.context.modifyingProcess.lineage.executablePath`

`servicio.runtime Details.context.modifyingProcess.lineage.name`

`servicio.runtime Details.context.modifyingProcess.lineage.namespacePid`

`servicio.runtime Details.context.modifyingProcess.lineage.parentUuid`

`servicio.runtime Details.context.modifyingProcess.lineage.pid`

`servicio.runtime Details.context.modifyingProcess.lineage.startTime`

`servicio.runtime Details.context.modifyingProcess.lineage.userId`

## Nombre del campo JSON

`servicio.runtime Details.context.modifyingProcess.lineage.uuid`

`servicio.runtime Details.context.modifyingProcess.name`

`servicio.runtime Details.context.modifyingProcess.namespacePid`

`servicio.runtime Details.context.modifyingProcess.parentUuid`

`servicio.runtime Details.context.modifyingProcess.pid`

`servicio.runtime Details.context.modifyingProcess.pwd`

`servicio.runtime Details.context.modifyingProcess.startTime`

`servicio.runtime Details.context.modifyingProcess.user`

`servicio.runtime Details.context.modifyingProcess.userId`

`servicio.runtime Details.context.modifyingProcess.uuid`

`servicio.runtime Details.context.mountSource`

`servicio.runtime Details.context.mountTarget`

`servicio.runtime Details.context.relatedFilePaths`

`servicio.runtime Details.context.releaseAgentPath`

`servicio.runtime Details.context.runcBinaryPath`

`servicio.runtime Details.context.scriptPath`

`servicio.runtime Details.context.serviceName`

`servicio.runtime Details.context.shellHistoryFilePath`

`servicio.runtime Details.context.socketPath`

`servicio.runtime Details.context.targetProcess.euid`

## Nombre del campo JSON

`servicio.runtime Details.context.targetProcess.executablePath`

`servicio.runtime Details.context.targetProcess.executableSha256`

`servicio.runtime Details.context.targetProcess.lineage.euid`

`servicio.runtime Details.context.targetProcess.lineage.executablePath`

`servicio.runtime Details.context.targetProcess.lineage.name`

`servicio.runtime Details.context.targetProcess.lineage.namespacePid`

`servicio.runtime Details.context.targetProcess.lineage.parentUid`

`servicio.runtime Details.context.targetProcess.lineage.pid`

`servicio.runtime Details.context.targetProcess.lineage.startTime`

`servicio.runtime Details.context.targetProcess.lineage.userId`

`servicio.runtime Details.context.targetProcess.lineage.uuid`

`servicio.runtime Details.context.targetProcess.name`

`servicio.runtime Details.context.targetProcess.namespacePid`

`servicio.runtime Details.context.targetProcess.parentUid`

`servicio.runtime Details.context.targetProcess.pid`

`servicio.runtime Details.context.targetProcess.pwd`

`servicio.runtime Details.context.targetProcess.startTime`

`servicio.tiempo de ejecución Details.context.targetProcess.user`

`servicio.tiempo de ejecución Details.context.targetProcess.userId`

`servicio.tiempo de ejecución Details.context.targetProcess.uuid`

## Nombre del campo JSON

servicio.tiempo de ejecución Details.context.threatFilePath

servicio.tiempo de ejecución Details.context.toolCategory

servicio.tiempo de ejecución Details.context.toolName

servicio.tiempo de ejecución Details.process.euid

servicio.tiempo de ejecución Details.process.lineage.euid

servicio.tiempo de ejecución Details.process.lineage.executablePath

servicio.tiempo de ejecución Details.process.lineage.name

servicio.tiempo de ejecución Details.process.lineage.namespacePid

servicio.tiempo de ejecución Details.process.lineage.parentUid

servicio.tiempo de ejecución Details.process.lineage.pid

servicio.tiempo de ejecución Details.process.lineage.startTime

servicio.tiempo de ejecución Details.process.lineage.userId

servicio.tiempo de ejecución Details.process.lineage.uid

servicio.tiempo de ejecución Details.process.namespacePid

servicio.tiempo de ejecución Details.process.parentUid

servicio.tiempo de ejecución Details.process.pid

servicio.tiempo de ejecución Details.process.pwd

servicio.tiempo de ejecución Details.process.startTime

servicio.tiempo de ejecución Details.process.user

servicio.tiempo de ejecución Details.process.userId

## Nombre del campo JSON

servicio.tiempo de ejecución Details.process.uuid

Service.Comentarios de los usuarios

## Reglas de supresión en GuardDuty

Una regla de supresión es un conjunto de criterios, que consta de un atributo de filtro emparejado con un valor, utilizado para filtrar resultados mediante el archivado automático de resultados nuevos que coinciden con los criterios especificados. Las reglas de supresión se pueden utilizar para filtrar los resultados de bajo valor, los resultados positivos falsos o las amenazas sobre las que no se pretende actuar, a fin de facilitar el reconocimiento de las amenazas de seguridad que tienen el mayor impacto en su entorno.

Después de crear una regla de supresión, los nuevos resultados que coincidan con los criterios definidos en la regla se archivan automáticamente siempre que la regla de supresión esté en su lugar. Puede utilizar un filtro existente para crear una regla de supresión o crear una regla de supresión a partir de un nuevo filtro que defina. Puede configurar reglas de supresión para suprimir tipos de hallazgos completos o definir criterios de filtro más detallados para suprimir sólo instancias específicas de un tipo de hallazgo determinado. Puede editar las reglas de supresión en cualquier momento.

Los hallazgos suprimidos no se envían a AWS Security Hub CSPM Amazon Simple Storage Service, Amazon Detective ni Amazon EventBridge, lo que reduce el ruido de las búsquedas si se consumen GuardDuty los hallazgos a través de Security Hub CSPM, un SIEM de terceros u otras aplicaciones de alerta y emisión de tickets. Si la has activado [Malware Protection for EC2](#), los GuardDuty resultados suprimidos no iniciarán un análisis de software malicioso.

GuardDuty sigue generando hallazgos incluso cuando se ajustan a tus reglas de supresión; sin embargo, esos hallazgos se marcan automáticamente como archivados. El hallazgo archivado se almacena GuardDuty durante 90 días y se puede ver en cualquier momento durante ese período. Para ver los hallazgos suprimidos en la GuardDuty consola, selecciona Archivado en la tabla de hallazgos o a través de la GuardDuty API utilizando la [ListFindings](#) API con un `findingCriteria` criterio de `service.archived` igual a verdadero.

 Note

En un entorno con varias cuentas, solo el GuardDuty administrador puede crear reglas de supresión.

## Uso de reglas de supresión con Detección Extendida de Amenazas

GuardDuty La detección extendida de amenazas detecta automáticamente los ataques en varias etapas que abarcan fuentes de datos, varios tipos de AWS recursos y tiempo, en un mismo momento. Cuenta de AWS Correlaciona los eventos en diferentes orígenes de datos para identificar los escenarios que se presentan como una amenaza potencial para su entorno AWS y, a continuación, genera un resultado de la secuencia de ataque. Para obtener más información, consulte [Cómo funciona la Detección Extendida de Amenazas](#).

Al crear reglas de supresión que archivan los resultados, la Detección Extendida de Amenazas no puede usar estos resultados archivados para correlacionar los eventos para las secuencias de ataque. Las normas de supresión amplias pueden afectar a la capacidad de detectar comportamientos GuardDuty relacionados con la detección de ataques en varias etapas. Los resultados que se archivan debido a las reglas de supresión no se consideran señales para las secuencias de ataque. Por ejemplo, si crea una regla de supresión que archive todos los hallazgos relacionados con los clústeres de EKS en lugar de centrarse en actividades específicas conocidas, GuardDuty no podrá utilizar esos hallazgos para detectar una secuencia de ataque en la que un actor de amenazas explote un contenedor, obtenga fichas privilegiadas y acceda a recursos confidenciales.

Ten en cuenta las siguientes recomendaciones de: GuardDuty

- Siga utilizando las reglas de supresión para reducir las alertas procedentes de actividades de confianza conocidas.
- Mantenga las reglas de supresión centradas en comportamientos específicos sobre los que no GuardDuty desee generar una conclusión.

## Casos de uso comunes para reglas de supresión y ejemplos

Los siguientes tipos de resultados tienen casos de uso comunes para la aplicación de reglas de supresión. Seleccione el nombre del resultado para obtener más información sobre el mismo. Revise

la descripción del caso de uso para decidir si desea crear una regla de supresión para ese tipo de resultado.

 Important

GuardDuty recomienda que cree reglas de supresión de forma reactiva y solo para los hallazgos en los que haya identificado repetidamente falsos positivos en su entorno.

- [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#): utilice una regla de supresión para archivar automáticamente resultados generados cuando se configuran las redes de la VPC para dirigir el tráfico de Internet a fin de que salga desde una puerta de enlace en las instalaciones en lugar de una puerta de enlace de Internet de VPC.

Este resultado se genera cuando la red está configurada para dirigir el tráfico de Internet de tal forma que salga por una puerta de enlace en las instalaciones y no por una puerta de enlace de Internet (IGW) de la VPC. Las configuraciones comunes, como el uso de [AWS Outposts](#) o de conexiones de VPN de la VPC, pueden generar tráfico dirigido de esta manera. Si el comportamiento es el previsto, se recomienda utilizar reglas de supresión y crear una regla que conste de dos criterios de filtrado. El primer criterio es Tipo de resultado, que debería ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. El segundo criterio de filtro es la Dirección IPv4 de la persona que llama a la API con el rango de direcciones IP o CIDR de su puerta de enlace de Internet en las instalaciones. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de la dirección IP de la persona que llama a la API.

Finding type: `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`  
API caller IPv4 address: `198.51.100.6`

 Note

Para incluir varias IP de personas que llaman a la API, puede agregar un nuevo filtro de direcciones IPv4 de las personas que llaman a la API para cada una de ellas.

- [Recon:EC2/Portscan](#): utilice una regla de supresión para archivar automáticamente los resultados cuando utilice una aplicación de evaluación de vulnerabilidades.

La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/Portscan`. El segundo criterio de filtro debe coincidir con la instancia o instancias que alojan estas herramientas de evaluación de vulnerabilidades. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada AML.

Finding type: *Recon:EC2/Portscan* Instance image ID: *ami-999999999*

- [UnauthorizedAccess:EC2/SSHBruteForce](#): utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias de bastión.

Si el objetivo del intento de fuerza bruta es un bastión anfitrión, esto puede representar el comportamiento esperado para su entorno. AWS Si este es el caso, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `UnauthorizedAccess:EC2/SSHBruteForce`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de la instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con un determinado valor de etiqueta de instancia.

Finding type: *UnauthorizedAccess:EC2/SSHBruteForce* Instance tag value: *devops*

- [Recon:EC2/PortProbeUnprotectedPort](#): utilice una regla de supresión para archivar automáticamente los resultados cuando tengan como objetivo las instancias que se hayan visto expuestas de manera intencional.

Puede haber casos en los que las instancias se expongan de forma intencionada, por ejemplo, si están alojando servidores web. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este hallazgo. La regla de supresión debe constar de dos criterios de filtro. Los primeros criterios deben utilizar el atributo Tipo de resultado con un valor de `Recon:EC2/PortProbeUnprotectedPort`. El segundo criterio de filtro debe coincidir con la instancia o instancias que sirven como host bastión. Puede utilizar el atributo ID de imagen de instancia o el atributo de valor Etiqueta en función de los criterios que se identifiquen con las



instancias que alojan estas herramientas. En el siguiente ejemplo, se representa el filtro que utilizaría para suprimir este tipo de resultado en función de las instancias con una determinada clave de etiqueta de instancia en la consola.

Finding type: *Recon:EC2/PortProbeUnprotectedPort* Instance tag key: *prod*

## Reglas de supresión recomendadas para los resultados de la Supervisión en tiempo de ejecución

- [PrivilegeEscalation:Runtime/DockerSocketAccessed](#) se genera cuando un proceso dentro de un contenedor se comunica con el socket de Docker. Es posible que haya contenedores de su entorno que necesiten acceso al socket de Docker por motivos legítimos. El acceso desde dichos contenedores generará resultados PrivilegeEscalation:Runtime/DockerSocketAccessed. Si este es el caso de su AWS entorno, le recomendamos que configure una regla de supresión para este tipo de hallazgo. Los primeros criterios deben utilizar el campo Tipo de resultado con un valor equivalente a PrivilegeEscalation:Runtime/DockerSocketAccessed. El segundo criterio de filtro es el campo Ruta ejecutable con un valor igual al executablePath del proceso en el resultado generado. Como alternativa, el segundo criterio de filtro puede usar un SHA-256 campo ejecutable con un valor igual al del proceso executableSha256 en la búsqueda generada.
- Los clústeres de Kubernetes ejecutan sus propios servidores DNS como pods; por ejemplo, coredns. Por lo tanto, para cada búsqueda de DNS desde un pod, GuardDuty captura dos eventos de DNS: uno del pod y otro del pod del servidor. Esto puede generar duplicados para los siguientes resultados de DNS:
  - [Backdoor:Runtime/C&CActivity.B!DNS](#)
  - [CryptoCurrency:Runtime/BitcoinTool.B!DNS](#)
  - [Impact:Runtime/AbusedDomainRequest.Reputation](#)
  - [Impact:Runtime/BitcoinDomainRequest.Reputation](#)
  - [Impact:Runtime/MaliciousDomainRequest.Reputation](#)
  - [Impact:Runtime/SuspiciousDomainRequest.Reputation](#)
  - [Trojan:Runtime/BlackholeTraffic!DNS](#)
  - [Trojan:Runtime/DGADomainRequest.C!DNS](#)
  - [Trojan:Runtime/DriveBySourceTraffic!DNS](#)
  - [Trojan:Runtime/DropPoint!DNS](#)

- [Trojan:Runtime/PhishingDomainRequest!DNS](#)

Los resultados duplicados incluirán los detalles del pod, el contenedor y el proceso que corresponden al pod de su servidor DNS. Puede configurar una regla de supresión para suprimir estos resultados duplicados utilizando estos campos. El primer criterio de filtro debe utilizar el campo Tipo de resultado con un valor igual a un tipo de resultado de DNS de la lista de resultados proporcionada anteriormente en esta sección. El segundo criterio de filtro puede ser una ruta ejecutable con un valor igual al del servidor DNS `executablePath` o un ejecutable SHA-256 con un valor igual al del servidor DNS `executableSHA256` en el resultado generado. Como tercer criterio de filtro opcional, puede utilizar el campo Imagen del contenedor de Kubernetes con un valor igual al de la imagen del contenedor del pod del servidor DNS en el resultado generado.

## Crear reglas de supresión en GuardDuty

Una regla de supresión es un conjunto de criterios que incluye el uso de atributos de filtro y el suministro de valores para los que no se GuardDuty desea generar un tipo de búsqueda. Los tipos de resultados que cumplen estos criterios se archivan automáticamente. Para reducir el ruido, los resultados suprimidos no se envían a ninguno de los dispositivos Servicios de AWS con los que se pueda realizar la integración. Para obtener más información sobre los casos de uso comunes para la creación de reglas de supresión, consulte [Reglas de supresión](#).

Puede visualizar, crear y gestionar las reglas de supresión mediante la página de reglas de supresión de la GuardDuty consola. Las reglas de supresión también se pueden generar a partir de los filtros guardados existentes. Para obtener más información acerca de la creación de filtros, consulte [Filtrar los hallazgos en GuardDuty](#).

Los criterios de filtrado pueden incluir una coincidencia exacta mediante `iguales` y `NotEquals` operadores, una coincidencia comodín con las coincidencias y `NotMatches` los operadores o una coincidencia comparativa con `GreaterThanLessThanEquals` los operadores `LessThan`. `GreaterThanEquals` Puede encontrar más información sobre los operadores disponibles en la [Conditions](#) página.

Elija el método de acceso que prefiera para crear una regla de supresión para GuardDuty buscar tipos.

## Console

Para crear una regla de supresión mediante la consola:

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En la página de reglas de supresión, haga clic en Crear regla de supresión para abrir el formulario Crear regla de supresión.
3. Introduzca un nombre para la regla de supresión. El nombre debe tener entre 3 y 64 caracteres. Los caracteres válidos son a-z A-Z, 0-9, punto (.), guión (-) y guión bajo (\_).
4. La descripción es opcional. Si introduce una descripción, puede tener 512 caracteres como máximo. Los caracteres válidos son a-z, 0-9 A-Z, punto (.), guión (-), dos puntos (:), corchetes ({ } ( ) [ ]), barra diagonal (/) y espacio.
5. El rango es opcional. Puede ser un valor numérico desde 1 hasta el recuento total de filtros y reglas de supresión, más 1.
6. En la sección Atributos, seleccione una clave y un operador en el menú desplegable.
7. Introduzca el valor «cadena» o «fecha» en el selector de fechas en función de la clave seleccionada. Si se trata de un valor de cadena, escriba el texto y pulse enter. Se pueden añadir varios valores en el caso de valores de cadena.
8. Para añadir criterios adicionales, seleccione Añadir criterio para añadir otro conjunto de claves, operadores y valores.
9. Seleccione Crear regla de supresión para crear y guardar la regla de supresión.

También puede crear una regla de supresión a partir de un filtro guardado existente. Para obtener más información acerca de la creación de filtros, consulte [Filtrar los hallazgos en GuardDuty](#).

Para crear una regla de supresión a partir de un filtro guardado:

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En la página Resultados, en el menú Reglas guardadas, seleccione una regla de conjunto de filtros guardada. Esto mostrará automáticamente el conjunto de filtros y los resultados que coincidan con los criterios.
3. También puede agregar más criterios de filtro a esta regla guardada. Puede omitir este paso si no necesita criterios de filtro adicionales. Para añadir uno o más criterios de filtrado, siga

los pasos 3 a 7 en [Adding filters on Findings page](#), a continuación, continúe con los pasos siguientes.

4. Una vez que haya agregado los criterios de filtro y haya confirmado que los resultados filtrados cumplen sus requisitos, elija Crear regla de supresión.
5. Introduzca un nombre para la regla de supresión. El nombre debe tener entre 3 y 64 caracteres. Los caracteres válidos son a-z A-Z, 0-9, punto (.), guión (-) y guión bajo (\_).
6. La descripción es opcional. Si introduce una descripción, puede tener 512 caracteres como máximo.
7. Seleccione Crear.
8. Si no necesita añadir criterios de filtro adicionales a la regla guardada, siga los pasos 4 a 7 para crear el filtro.

## API/CLI

Para crear una regla de supresión mediante una API:

1. También puede crear reglas de supresión a través de la API [CreateFilter](#). Para ello, especifique los criterios de filtro en un archivo JSON según el formato del ejemplo que se detalla a continuación. El siguiente ejemplo suprimirá cualquier resultado de baja gravedad no archivado que contenga una solicitud de DNS al dominio `test.example.com`. Para los resultados de gravedad media, la lista de entrada será `["4", "5", "7"]`. Para los resultados de gravedad alta, la lista de entrada será `["6", "7", "8"]`. Para los resultados de gravedad crítica, la lista de entrada será `["9", "10"]`. También puede filtrar en función de cualquier valor de la lista.

En el siguiente ejemplo, se agrega un filtro para los hallazgos de baja gravedad para las funciones lambda con el prefijo «MyFunc» y la etiqueta de la función con el prefijo no como «» TestTag

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
        "test.example.com"
      ]
    },
    "severity": {
```

```

        "Equals": [
            "1",
            "2",
            "3"
        ]
    }
}

```

Puede crear reglas de supresión utilizando los caracteres comodín \* y ? . Los caracteres comodín en los filtros solo se admiten si se utilizan coincidencias y NotMatches operadores. Para hacer coincidir cualquier número de caracteres, puede usar \* en el valor del atributo y, para hacer coincidir un solo carácter, ¿puede usar? en el valor del atributo. Los filtros admiten un máximo de 5 atributos en una sola condición de comodín y un máximo de 5 caracteres comodín dentro de un solo atributo. En el siguiente ejemplo, se agrega un filtro para el nombre de Lambda que coincide con el prefijo «MyFunc», pero no para las funciones Lambda con etiquetas con «TestTag» como prefijo seguido de 0 a 2 caracteres.

```

{
  "Criterion": {
    "resource.lambdaDetails.functionName": {
      "Matches": [
        "MyFunc*"
      ]
    },
    "resource.lambdaDetails.tags.key": {
      "NotMatches": [
        "TestTag??"
      ]
    }
  }
}

```

Para obtener una lista de los nombres de campo JSON y su equivalente de consola, consulte [La propiedad filtra GuardDuty](#).

Para probar sus criterios de filtro, utilice el mismo criterio de JSON en la API [ListFindings](#) y confirme que se hayan seleccionado los resultados correctos. Para probar tus criterios de filtro, AWS CLI sigue el ejemplo con tu propio DetectorID y un archivo.json.

Para encontrar los detectorId de tu cuenta y región actuales, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la API [ListDetectors](#)

```
aws guardduty list-detector
```

```
aws guardduty list-findings \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--finding-criteria file://criteria.json
```

 Note

Los comodines que coincidan no están disponibles para ListFindings y GetFindingsStatistics. Los criterios que contienen caracteres comodín no se pueden validar mediante ListFindings y. GetFindingsStatistics

2. Cargue el filtro para utilizarlo como regla de supresión con la API [CreateFilter](#) o mediante la CLI de AWS según el ejemplo siguiente con su propio ID de detector, un nombre para la regla de supresión y un archivo .json.

Para encontrar los detectorId de su cuenta y región actuales, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecute la [ListDetectors](#) API.

```
aws guardduty create-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--action ARCHIVE \  
--name yourfiltername \  
--finding-criteria file://criteria.json
```

Puede ver una lista de sus filtros mediante programación con la API [ListFilter](#). Para ver los detalles de un filtro individual, proporcione el nombre del filtro a la API [GetFilter](#). Actualice los filtros mediante la API [UpdateFilter](#) o elimínelos con ayuda de la API [DeleteFilter](#).

## Actualización de las reglas de supresión en GuardDuty

En esta sección se proporcionan los pasos para actualizar una regla de supresión Cuenta de AWS en una específica Región de AWS.

Puede actualizar las reglas de supresión existentes desde la página de reglas de supresión de la GuardDuty consola. GuardDuty permite actualizar la descripción, el rango y los criterios de filtrado del filtro de supresión desde la GuardDuty consola o mediante el GuardDuty CLI/API. La regla de supresión de actualizaciones sigue las mismas restricciones en cuanto a los valores de campo de descripción, clasificación y criterios que [Crear reglas de supresión](#).

Si se trata de una cuenta de miembro, la cuenta de administrador puede realizar esta acción en su nombre. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para eliminar una regla de supresión para GuardDuty buscar tipos.

### Console

1. Abre la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
2. En la página de reglas de supresión, seleccione la regla de supresión que desee actualizar.
3. En el menú desplegable Acciones, selecciona Actualizar la regla de supresión.
4. Esto abre el formulario de regla de supresión existente.
5. Realice los cambios necesarios en la sección de descripción, rango y atributos.
6. Seleccione Actualizar regla de supresión para actualizar la regla de supresión.

## API/CLI

Para actualizar una regla de supresión mediante la API:

1. Puedes actualizar las reglas de supresión a través de la UpdateFilter API. Solo la descripción, el rango y los criterios se pueden actualizar mediante la UpdateFilter API. Todos estos tres campos son opcionales.
2. Para actualizar un filtro existente, necesitará el nombre del filtro que planea actualizar.
3. Si desea actualizar los criterios existentes, cree un archivo JSON con los criterios actualizados de forma similar a como creó el filtro por primera vez. Un ejemplo de criterio para suprimir cualquier hallazgo de baja gravedad no archivado que contenga una solicitud de DNS al dominio test.example.com. Para los resultados de gravedad media, la lista de entrada será ["4", «5", «7"]. Para los hallazgos de gravedad alta, la lista de entrada será ["6", «7", «8"]. En el caso de los hallazgos de gravedad crítica, la lista de entrada será ["9", «10"]. También puede filtrar en función de cualquier valor de la lista. En el siguiente ejemplo, se añade un filtro para los resultados de gravedad baja.

```
{
  "Criterion": {
    "service.action.dnsRequestAction.domain": {
      "Equals": [
        "test.example.com"
      ]
    },
    "severity": {
      "Equals": [
        "1",
        "2",
        "3"
      ]
    }
  }
}
```

Para obtener una lista de los nombres de campo JSON y su equivalente de consola, consulte [La propiedad filtra GuardDuty](#).



Para probar sus criterios de filtro, utilice el mismo criterio de JSON en la API [ListFindings](#) y confirme que se hayan seleccionado los resultados correctos. Para probar tus criterios de filtro, AWS CLI sigue el ejemplo con tu propio DetectorID y un archivo.json.

Para encontrar los detectorId de tu cuenta y región actuales, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/> consola o ejecuta la API [ListDetectors](#)

```
aws guardduty list-detectors --region us-east-1
```

4. Si desea actualizar la descripción, puede incluir el parámetro de descripción en la llamada CLI.
5. Si desea actualizar la clasificación, puede incluir el parámetro de clasificación en la llamada CLI.
6. Si desea pasar de un filtro de supresión a un filtro normal, utilice el parámetro de acción y el valor ARCHIVE en la llamada CLI.
7. Actualice su API de filtro existente o utilice el AWS CLI siguiente ejemplo con su propio ID de detector, un nombre para la regla de supresión y un archivo.json.
8. El siguiente es un ejemplo de CLI que actualiza todos los parámetros descritos anteriormente. Puede seleccionar los parámetros específicos que desea actualizar para su caso de uso con el comando -

```
aws guardduty update-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--region us-east-1 \  
--action ARCHIVE \  
--rank 1 \  
--description "Updated description" \  
--finding-criteria file://criteria.json
```

## Eliminar las reglas de supresión en GuardDuty

En esta sección se proporcionan los pasos para eliminar una regla de supresión Cuenta de AWS en una específica Región de AWS.

Es posible que desee eliminar una regla de supresión que ya no represente un comportamiento esperado en el entorno. Ya no desea suprimir el tipo de búsqueda asociado para GuardDuty poder generar un tipo de búsqueda.

Si se trata de una cuenta de miembro, la cuenta de administrador puede realizar esta acción en su nombre. Para obtener más información, consulte [Relaciones entre la cuenta de administrador y la cuenta de miembro](#).

Elija el método de acceso que prefiera para eliminar una regla de supresión de tipos de GuardDuty búsqueda.

### Console

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En la página de reglas de supresión, seleccione la regla de supresión que desee eliminar.
3. En el menú desplegable Acciones, selecciona Eliminar regla de supresión.
4. Aparece una ventana emergente de confirmación. Seleccione Eliminar para continuar con la eliminación. O bien, seleccione Cancelar para cancelar la operación.

### API/CLI

Ejecute la API [DeleteFilter](#). Especifique el nombre del filtro y el ID del detector asociado para la región en cuestión.

Como alternativa, puede utilizar el siguiente AWS CLI ejemplo sustituyendo los valores formateados en *red*:

```
aws guardduty delete-filter \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--filter-name filterName \  
--region us-east-1
```

Para encontrar los `detectorId` valores de tu cuenta y región actuales, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

## Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP

Amazon GuardDuty supervisa la seguridad de su AWS entorno mediante el análisis y el procesamiento de los registros de flujo de VPC, los registros de AWS CloudTrail eventos y los registros de DNS. Al habilitar uno o más [planes Use-case de GuardDuty protección específicos](#) (excepto [Supervisión en tiempo de ejecución](#)), puede ampliar las capacidades de monitoreo internas GuardDuty.

Con las listas, le GuardDuty ayuda a personalizar el alcance de la detección de amenazas en su entorno. Puede configurarlo GuardDuty para que deje de generar hallazgos a partir de sus fuentes confiables y genere hallazgos de fuentes maliciosas conocidas a partir de sus listas de amenazas. GuardDuty sigue siendo compatible con las listas de direcciones IP antiguas y amplía el soporte a las listas de entidades (recomendado) que pueden contener direcciones IP, dominios o ambos.

### Temas

- [Comprender las listas de entidades y listas de direcciones IP](#)
- [Consideraciones importantes para GuardDuty las listas](#)
- [Formatos de las listas](#)
- [Explicación de los estados de las listas](#)
- [Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP](#)
- [Añadir y activar una lista de entidades o una lista de IP](#)
- [Actualización de una lista de entidades o una lista de direcciones IP](#)
- [De-activating lista de entidades o lista de direcciones IP](#)
- [Eliminar la lista de entidades o la lista de direcciones IP](#)

## Comprender las listas de entidades y listas de direcciones IP

GuardDuty ofrece dos enfoques de implementación: listas de entidades (recomendadas) y listas de IP. Ambos enfoques le ayudan a especificar fuentes confiables, que dejan GuardDuty de generar hallazgos y las amenazas conocidas, que GuardDuty utilizan para generar hallazgos.

Las listas de entidades admiten direcciones IP, nombres de dominio y códigos hash de SHA-256 archivos. Utilizan el acceso directo a Amazon Simple Storage Service (Amazon S3) con un único permiso de IAM que no afecta a los límites de tamaño de las políticas de IAM en múltiples regiones.

Las listas de IP solo admiten direcciones IP y utilizan [GuardDuty rol vinculado a un servicio \(SLR\)](#) (SLR), por lo que es necesario actualizar las políticas de IAM por región, lo que puede afectar a los límites de tamaño de las políticas de IAM.

Las listas de confianza (tanto listas de entidades como listas de direcciones IP) incluyen entradas en las que puede confiar para una comunicación segura con su AWS infraestructura. GuardDuty no genera resultados para las entradas incluidas en fuentes confiables. En un momento dado, solo puede añadir una lista de entidades de confianza y una lista de direcciones IP de confianza Cuenta de AWS por región.

Las listas de amenazas (tanto listas de entidades como listas de direcciones IP) incluyen entradas que haya identificado como fuentes maliciosas conocidas. Cuando GuardDuty detecta una actividad relacionada con estas fuentes, genera resultados que le avisan de posibles problemas de seguridad. Puede crear sus propias listas de amenazas o incorporar fuentes de inteligencia de amenazas de terceros. La inteligencia sobre amenazas de terceros puede ofrecer esta lista, que también se puede crear específicamente para su organización. Además de generar hallazgos debido a una actividad potencialmente sospechosa, GuardDuty también genera hallazgos basados en una actividad que implica entradas de sus listas de amenazas. En cualquier momento, puede cargar hasta seis listas de entidades de amenazas y listas de direcciones IP de amenazas Cuenta de AWS por región.

### Note

Para migrar de las listas de direcciones IP a las listas de entidades, siga [Requisitos previos para las listas de entidades](#) y, a continuación, añada y active la lista de entidades requerida. Después de esto, puede optar por desactivar o eliminar la lista de direcciones IP correspondiente.

## Consideraciones importantes para GuardDuty las listas

Antes de comenzar a trabajar con listas, lea las siguientes consideraciones:

- Las listas de IP y de entidades se aplican únicamente al tráfico destinado a dominios y direcciones IP enrutables públicamente.
- En una lista de entidades, las entradas se aplican a CloudTrail los registros de flujo de VPC en Amazon VPC y a los resultados de los registros de consultas DNS de Route53 Resolver.

En una lista de direcciones IP, las entradas se aplican a CloudTrail los hallazgos de los registros de flujo de VPC en Amazon VPC, pero no a los hallazgos de los registros de consultas de DNS de Route53 Resolver.

- Si incluye la misma dirección IP o dominio en las listas de confianza y de amenazas, prevalecerá esta entrada de la lista de confianza. GuardDuty no generará ningún resultado si hay una actividad asociada a esta entrada.
- En un entorno con varias cuentas, solo la cuenta de GuardDuty administrador puede administrar las listas. Esta configuración se aplica automáticamente a las cuentas de los miembros. GuardDuty genera hallazgos basados en una actividad que involucra direcciones IP (y dominios) maliciosos conocidos de las fuentes de amenazas de la cuenta de administrador, y no genera hallazgos basados en actividades que involucren direcciones IP (y dominios) de las fuentes de confianza de la cuenta de administrador. Para obtener más información, consulte [Varias cuentas en Amazon GuardDuty](#).
- Solo se aceptan direcciones IPv4. No se admiten direcciones IPv6.
- SHA-256 Los hashes de archivos solo se admiten en las listas de entidades amenazantes. No puede incluir los hashes de archivos en las listas de entidades de confianza ni en las listas de direcciones IP.
- Tras activar, desactivar o eliminar una lista de entidades o una lista de direcciones IP, se estima que el proceso se completará en 15 minutos. En algunos casos, este proceso puede tardar hasta 40 minutos en completarse.
- GuardDuty utiliza una lista para detectar amenazas solo cuando el estado de la lista pasa a ser Activo.
- Siempre que añada o actualice una entrada en la ubicación del bucket S3 de la lista, debe volver a activar la lista. Para obtener más información, consulte [Actualización de una lista de entidades o una lista de direcciones IP](#).

- Las listas de entidades y las direcciones IP tienen cuotas diferentes. Para obtener más información, consulte [GuardDuty cuotas](#).

## Formatos de las listas

GuardDuty acepta varios formatos de archivo para sus listas y listas de entidades, con un máximo de 35 MB por archivo. Cada formato tiene requisitos y capacidades específicos.

### Texto sin formato (TXT)

Este formato admite direcciones IP, rangos de CIDR, nombres de dominio y hashes de SHA-256 archivos. Los hashes de archivos solo se admiten en las listas de entidades de amenazas. Cada entrada debe aparecer en una línea independiente.

### Example Ejemplo de lista de entidades

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
```

### Example Ejemplo de lista de entidades de amenazas con hashes de archivos

```
192.0.2.1
192.0.2.0/24
example.com
example.org
*.example.org
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3
```

### Example Ejemplo de lista de direcciones IP

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

### Structured Threat Information Expression (STIX)

Este formato admite direcciones IP, bloques CIDR, nombres de dominio y hashes de SHA-256 archivos. STIX le permite incluir contexto adicional en su inteligencia sobre amenazas. GuardDuty

procesa las direcciones IP, los rangos de CIDR, los nombres de dominio y los hashes de SHA-256 archivos a partir de los indicadores STIX. SHA-256 Los hashes de archivos solo se admiten en las listas de entidades de amenazas.

### Example Ejemplo de una lista de entidades

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:indicator="http://stix.mitre.org/Indicator-2"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
  id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
  version="1.2">
  <stix:Indicators>
    <stix:Indicator
      id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeefffff"
      timestamp="2025-08-12T00:00:00Z"
      xsi:type="indicator:IndicatorType"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <indicator:Title>Malicious domain observed Example</indicator:Title>
      <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
Watchlist</indicator:Type>
      <indicator:Observable id="example:Observable-0000-1111-2222-3333">
        <cybox:Object id="example:Object-0000-1111-2222-3333">
          <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
            <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```

### Example Ejemplo de lista de entidades de amenazas con hashes de archivos

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
```

```

xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:cybox="http://cybox.mitre.org/cybox-2"
xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:indicator="http://stix.mitre.org/Indicator-2"
xmlns:stixCommon="http://stix.mitre.org/common-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
xmlns:DomainNameObj="http://cybox.mitre.org/objects#DomainNameObject-1"
xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
id="example:Package-a1b2c3d4-1111-2222-3333-444455556666"
version="1.2">
<stix:Indicators>
  <stix:Indicator
    id="example:indicator-a1b2c3d4-aaaa-bbbb-cccc-ddddeeeefffff"
    timestamp="2025-08-12T00:00:00Z"
    xsi:type="indicator:IndicatorType"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <indicator:Title>Malicious domain observed Example</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">Domain
Watchlist</indicator:Type>
    <indicator:Observable id="example:Observable-0000-1111-2222-3333">
      <cybox:Object id="example:Object-0000-1111-2222-3333">
        <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
          <DomainNameObj:Value condition="Equals">bad.example.com</
DomainNameObj:Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
  </stix:Indicator>
  <stix:Indicator
    id="example:indicator-a1b2c3d4-eeee-ffff-0000-111122223333"
    timestamp="2025-08-12T00:00:00Z"
    xsi:type="indicator:IndicatorType"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <indicator:Title>File hash for malware variant</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">File Hash
Watchlist</indicator:Type>
    <indicator:Observable id="example:Observable-4444-5555-6666-7777">
      <cybox:Object id="example:File-4444-5555-6666-7777">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
          <FileObj:Hashes>
            <cyboxCommon:Hash>
              <cyboxCommon:Type
xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>

```



```

        <cyboxCommon:Simple_Hash_Value
condition="Equals">a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3</
cyboxCommon:Simple_Hash_Value>
        </cyboxCommon:Hash>
    </FileObj:Hashes>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>

```

## Example Ejemplo de una lista de direcciones IP

```

<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixCommon="http://stix.mitre.org/common-1"
  xmlns:ttp="http://stix.mitre.org/TTP-1"
  xmlns:cybox="http://cybox.mitre.org/cybox-2"
  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
  xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
  xmlns:example="http://example.com/"
  xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
  id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
  version="1.2">
  <stix:Observables cybox_major_version="1" cybox_minor_version="1">
    <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
      <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">

```

```

        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">

    <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
        </cybox:Properties>
    </cybox:Object>
</cybox:Observable>
<cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
    <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
            <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    <cybox:Observable
id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
        <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
            <cybox:Properties xsi:type="AddressObject:AddressObjectType"
category="ipv4-addr">
                <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
                    </cybox:Properties>
                </cybox:Object>
            </cybox:Observable>
        </stix:Observables>
    </stix:STIX_Package>

```

## CSV de Open Threat Exchange (OTX)<sup>TM</sup>

Este formato admite el bloqueo CIDR, las direcciones IP individuales, los dominios y el tipo de SHA256 indicador de los hashes de los archivos. SHA-256 Los hashes de archivos solo se admiten en las listas de entidades de amenazas. Este formato de archivo tiene valores separados por comas.

### Example Ejemplo de lista de entidades

```

Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example

```

Domain name, example.net, example

### Example Ejemplo de lista de entidades de amenazas con hashes de archivos

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
Domain name, example.net, example
SHA256, a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3, example
```

### Example Ejemplo de lista de direcciones IP

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

## FireEye™ iSight Threat Intelligence CSV

Este formato admite el bloqueo CIDR, las direcciones IP individuales, los dominios y los hashes de SHA-256 archivos de la columna. sha256 SHA-256 Los hashes de archivos solo se admiten en las listas de entidades de amenazas. En las siguiente listas de ejemplo se utiliza un formato de CSV de FireEye™.

### Example Ejemplo de lista de entidades

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,  
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,  
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,  
sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,  
filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,  
protocol, registrantEmail, registrantName, networkType, url, malwareFamily,  
malwareFamilyId, actor, actorId, observationTime  
  
01-000000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-000000001, https://www.example.com/  
report/01-000000001, , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000002, https://www.example.com/  
report/01-00000002, , , , , , , , , , , , , , , , , , , Related,  
198.51.100.1, , , , network, , Ursnif,  
12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400  
  
01-00000003, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000003, https://www.example.com/  
report/01-00000003, , , , , , , , , , , , , , , , , , , Related,  
203.0.113.1, , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,  
1494944400  
  
01-00000002, Malicious domain observed in test, Test, Operational, threat,  
1494944400, https://www.example.com/report/01-00000002,https://www.example.com/  
report/01-00000002,,,,,,,,,,,,, 203.0.113.0/24, example.com,, Related,  
203.0.113.0, 8080, UDP,,, network,, Ursnif, fc13984c-c767-40c9-8329-f4c59557f73b,,,  
1494944400
```

### Example Ejemplo de lista de entidades de amenazas con hashes de archivos

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp, subject,
recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier, md5, sha1,
sha256, description, fileType, packer, userAgent, registry, fileCompilationDateTime,
filePath, asn, cidr, domain, domainTimeOfLookup, networkIdentifier, ip, port,
protocol, registrantEmail, registrantName, networkType, url, malwareFamily,
malwareFamilyId, actor, actorId, observationTime
```

```
01-00000001, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000001, https://www.example.com/  
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,  
Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,  
1494944400
```

```
01-00000002, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000002, https://www.example.com/  
report/01-00000002, , , , , , , , , , , , , , , , , , , Related,  
198.51.100.1, , , , network, , Ursnif,  
12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , , 1494944400
```

```
01-00000003, Example, Test, Operational, threat, 1494944400,  
https://www.example.com/report/01-00000003, https://www.example.com/  
report/01-00000003, / / / / / / / / / / / / / / / / , Related,
```

[illegible]

### Example Ejemplo de lista de direcciones IP

[illegible]

## CSV de Proofpoint™ ET Intelligence Feed

En formato ProofPoint CSV, puede añadir direcciones IP o nombres de dominio en una lista. En la siguiente lista de ejemplo se utiliza el formato de CSV de Proofpoint. Proporcionar un valor para el parámetro `ports` es opcional. Si no lo proporciona, deje una coma (,) al final.

### Example Ejemplo de lista de entidades

```
domain, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

### Example Ejemplo de lista de direcciones IP

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

## AlienVaultFuente de reputación de™

En la siguiente lista de ejemplo se utiliza el formato AlienVault. Este formato también admite los hash de los SHA-256 archivos en la columna del indicador. SHA-256 Los hashes de archivos solo se admiten en las listas de entidades de amenazas.

### Example Ejemplo de lista de entidades

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
```

### Example Ejemplo de lista de entidades de amenazas con hashes de archivos

```
192.0.2.1#4#2#Malicious Host#KR##37.5111999512,126.974098206#3
192.0.2.2#4#2#Scanning Host#IN#Gurgaon#28.4666996002,77.0333023071#3
192.0.2.3#4#2##CN#Guangzhou#23.1166992188,113.25#3
www.test.org#4#2#Malicious Host#CA#Brossard#45.4673995972,-73.4832000732#3
www.example.com#4#2#Malicious Host#PL##52.2393989563,21.0361995697#3
a665a45920422f9d417e4867efdc4fb8a04a1f3fff1fa07e998e86f7f7a27ae3#4#2#Malicious
Hash###0.0,0.0#3
```

## Example Ejemplo de lista de direcciones IP

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

## Explicación de los estados de las listas

Al añadir una lista de entidades o una lista de direcciones IP, GuardDuty muestra el estado de esa lista. La columna Estado indica si la lista está en vigor y si es necesario realizar acciones. En la lista siguiente se describen los valores de estado válidos:

- **Activa:** indica que la lista se está utilizando actualmente para la detección personalizada de amenazas.
- **Inactiva:** indica que la lista no está en uso actualmente. GuardDuty Para utilizar esta lista para detectar amenazas en su entorno, consulte el paso 3: Activar una lista de entidades o una lista de direcciones IP en [Añadir y activar una lista de entidades o una lista de IP](#).
- **Error:** indica que hay un problema con la lista. Pase el cursor sobre el estado para ver los detalles del error.
- **Activación:** indica que GuardDuty se ha iniciado el proceso de activación de la lista. Puede seguir supervisando el estado de esta lista. Si no hay ningún error, el estado debería actualizarse a Activa. Mientras el estado siga siendo Activación, no podrá realizar ninguna acción de esta lista. El estado de la lista puede tardar unos minutos en pasar a Activo.
- **Desactivar:** indica que se GuardDuty ha iniciado el proceso de desactivación de la lista. Puede seguir supervisando el estado de esta lista. Si no hay ningún error, el estado debería actualizarse a Inactivo. Mientras el estado siga siendo Desactivación, no podrá realizar ninguna acción de esta lista.
- **Eliminación pendiente:** indica que la lista está en proceso de eliminarse. Mientras el estado siga siendo Eliminar pendientes, no podrá realizar ninguna acción de esta lista.

## Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP

GuardDuty utiliza listas de entidades y listas de direcciones IP para personalizar la detección de amenazas en su AWS entorno. Las listas de entidades (recomendado) admiten direcciones IP y

nombres de dominio, mientras que las listas de direcciones IP solo admiten direcciones IP. Antes de comenzar a crear estas listas, debe agregar los permisos necesarios para el tipo de lista que desea usar.

## Requisitos previos para las listas de entidades

Al añadir listas de entidades, GuardDuty lee las listas de confianza y de inteligencia sobre amenazas de los buckets de S3. El rol que utilice para crear las listas de entidades debe tener el permiso `s3:GetObject` para los buckets de S3 que contienen estas listas.

### Note

En un entorno con varias cuentas, solo la cuenta de GuardDuty administrador puede administrar las listas, que se aplican automáticamente a las cuentas de los miembros.

Si aún no tiene el `s3:GetObject` permiso para la ubicación del bucket de S3, utilice la siguiente política de ejemplo y *amzn-s3-demo-bucket* sustitúyalo por su ubicación de bucket de S3.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[object-key]"
    }
  ]
}
```

## Requisitos previos para las listas de direcciones IP

Varias identidades de IAM requieren permisos especiales para funcionar con listas de IP confiables y listas de amenazas. GuardDuty Una identidad con la política administrada [AmazonGuardDutyFullAccess\\_v2 \(recomendado\)](#) adjunta solo puede cambiar de nombre y desactivar las listas de IP de confianza y las listas de amenazas cargadas.



Para conceder a diferentes identidades acceso completo para trabajar con listas de IP de confianza y listas de amenazas (además de cambiar de nombre y desactivar estas listas, esto incluye la adición, activación, eliminación y actualización de la ubicación o el nombre de las listas), asegúrese de que las siguientes acciones estén presentes en la política de permisos adjunta a un usuario, grupo o rol:

```
{
  "Effect": "Allow",
  "Action": [
    "iam:PutRolePolicy",
    "iam>DeleteRolePolicy"
  ],
  "Resource": "arn:aws:iam::555555555555:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

 Important

Estas acciones no se incluyen en la política administrada AmazonGuardDutyFullAccess.

## Uso del SSE-KMS cifrado con listas de entidades y listas de IP

GuardDuty soporta SSE-AES256 y SSE-KMS cifrado para sus listas. SSE-C no es compatible. Para obtener más información sobre los tipos de cifrado para S3, consulte [Protección de los datos con el cifrado del servidor](#).

Independientemente de si utiliza listas de entidades o listas de IP, si las utiliza SSE-KMS, añada la siguiente declaración a su AWS KMS key política. **123456789012** Sustitúyala por tu propia ID de cuenta.

```
{
  "Sid": "AllowGuardDutyServiceRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
  },
  "Action": "kms:Decrypt*",
  "Resource": "*"
}
```

## Añadir y activar una lista de entidades o una lista de IP

Las listas de entidades y las listas de direcciones IP le ayudan a personalizar las capacidades de detección de amenazas en GuardDuty. Para obtener más información sobre estas listas, consulte [Comprender las listas de entidades y listas de direcciones IP](#). Para gestionar los datos fiables y de inteligencia sobre amenazas de su AWS entorno, GuardDuty recomienda utilizar listas de entidades. Antes de comenzar, consulte [Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP](#).

Elija uno de los siguientes métodos de acceso para agregar y activar una lista de entidades, una lista de entidades de amenazas, una lista de IP de confianza o una lista de IP de amenazas.

### Console

(Opcional) Paso 1: obtención de la URL de ubicación de la lista

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. En el panel de navegación, elija Buckets.
3. Elija el nombre del bucket de Amazon S3 que contiene la lista específica que desea agregar.
4. Elija el nombre del objeto (lista) para consultar sus detalles.
5. En la pestaña Propiedades, copie el URI de S3 de este objeto.

Paso 2: Añadir datos de inteligencia de amenazas o de confianza

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña Listas de entidades o Listas de direcciones IP.
4. En función de la pestaña seleccionada, elija agregar una lista de confianza o una lista de amenazas.
5. En el cuadro de diálogo para agregar una lista de confianza o una lista de amenazas, haga lo siguiente.
  - a. En Nombre de la lista, ingrese un nombre para la lista.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una región Cuenta de AWS y.

- b. En Ubicación, indique la ubicación en la que ha cargado la lista. Si aún no la tiene, consulte [Step 1: Fetching location URL of your list](#).

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Formato de la URL de ubicación:

- <https://s3.amazonaws.com/bucket.name/file.txt>
  - <https://s3-aws-region.amazonaws.com/bucket.name/file.txt>
  - <http://bucket.s3.amazonaws.com/file.txt>
  - <http://bucket.s3-aws-region.amazonaws.com/file.txt>
  - <s3://bucket.name/file.txt>
- c. (Opcional) Para el propietario esperado del bucket, puede introducir el Cuenta de AWS ID propietario del bucket de Amazon S3 especificado en el campo Ubicación.

Si no especificas un Cuenta de AWS ID de propietario, se GuardDuty comporta de forma diferente para las listas de entidades y las listas de direcciones IP. En el caso de las listas de entidades, GuardDuty validará que la cuenta del miembro actual sea propietaria del bucket de S3 especificado en el campo Ubicación. En el caso de las listas de direcciones IP, si no especificas un propietario de Cuenta de AWS ID, GuardDuty no realizará ninguna validación.

Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar la lista.

- d. Active la casilla I agree.
- e. Elija Add list. De forma predeterminada, el estado de la lista agregada es Inactivo. Para que la lista sea efectiva, debe activarla.

### Paso 3: Activar una lista de entidades o una lista de direcciones IP

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.

2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña en la que desee activar la lista: Listas de entidades o Listas de direcciones IP.
4. Seleccione una lista que desea activar. Esto habilitará el menú Acción y Edición.
5. Elija Acción y, a continuación, elija Activar.

## API/CLI

Para añadir y activar una lista de entidades de confianza

1. Ejecute [CreateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de confianza. Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty create-trusted-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que va a crear la lista de entidades de confianza y por otros valores de marcador de posición que lo sean *shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el Cuenta de AWS ID asociado a este `--detector-id` valor sea propietario del bucket de S3 especificado en el

--location parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para añadir y activar listas de entidades de amenazas

1. Ejecute [CreateThreatEntitySet](#). Asegúrese de proporcionar el detectorId de la cuenta de miembro para la que desea crear esta lista de entidades de amenazas. Para encontrar el detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty create-threat-entity-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

detector-idSustitúyelo por el identificador de la cuenta de miembro para la que va a crear la lista de entidades de confianza y por otros valores de marcador de posición que lo sean*shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro --activate por. --no-activate

El parámetro expected-bucket-owner es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el Cuenta de AWS ID asociado a este --detector-id valor sea propietario del bucket de S3 especificado en el --location parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

### Creación y activación de una lista de direcciones IP de confianza

1. Ejecute [CreateIPSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS región.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
aws guardduty create-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--format TXT \  
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-  
FILE.format" \  
--activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que va a crear la lista de IP de confianza y por otros valores de marcador de posición que lo sean *shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no especificas el ID de cuenta propietario del bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de

cuenta para el `expected-bucket-owner` parámetro, GuardDuty valida que este Cuenta de AWS ID sea propietario del bucket de S3 especificado en el `--location` parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Para añadir y activar listas de IP de amenazas

1. Ejecute [CreateThreatIntelSet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS región.

2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de IP de amenazas.

```
aws guardduty create-threat-intel-set \
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \
--name "AnyOrganization ListEXAMPLE" \
--format TXT \
--location "https://s3.amazonaws.com/amzn-s3-demo-bucket/DOC-EXAMPLE-SOURCE-FILE.format" \
--activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que va a crear la lista de direcciones IP peligrosas y otros valores de marcador de posición que lo sean *shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no especificas el ID de cuenta propietario del bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de

cuenta para el `expected-bucket-owner` parámetro, GuardDuty valida que este Cuenta de AWS ID sea propietario del bucket de S3 especificado en el `--location` parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Después de activar una lista de entidades o de direcciones IP, es posible que la lista tarde unos minutos en surtir efecto. Para obtener más información, consulte [Consideraciones importantes para GuardDuty las listas](#).

## Actualización de una lista de entidades o una lista de direcciones IP

Las listas de entidades y las listas de direcciones IP le ayudan a personalizar las capacidades de detección de amenazas en GuardDuty. Para obtener más información sobre estas listas, consulte [Comprender las listas de entidades y listas de direcciones IP](#).

Puede actualizar el nombre de una lista, la ubicación del bucket en S3, el identificador de cuenta del propietario previsto del bucket y las entradas de una lista existente. Si actualiza las entradas de una lista, debe seguir los pasos para GuardDuty volver a activar la lista y utilizar la última versión de la lista. Es posible que, después de actualizar o activar una lista de entidades o de direcciones IP, se necesiten unos minutos para que se encuentre efectiva. Para obtener más información, consulte [Consideraciones importantes para GuardDuty las listas](#).

### Note

Si el estado de una lista es Activación, Desactivación o Eliminación de datos pendientes, debe esperar unos minutos antes de realizar cualquier acción. Para obtener información sobre estos estados, consulte [Explicación de los estados de las listas](#).

Elija uno de los métodos de acceso de la para actualizar una lista de entidades o de direcciones IP.

### Console

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Listas, seleccione la pestaña correspondiente: Listas de entidades o Listas de direcciones IP.



4. Seleccione una lista (de confianza o de amenazas) que desee actualizar. Esto habilitará el menú Acción y Edición.
5. Elija Edit (Edición de).
6. En el cuadro de diálogo para actualizar la lista, especifique los detalles que desee actualizar.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una región Cuenta de AWS y.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

7. (Opcional) Para el propietario esperado del bucket, puede introducir el Cuenta de AWS ID propietario del bucket de Amazon S3 especificado en el campo Ubicación.

Si no especificas un Cuenta de AWS ID de propietario, se GuardDuty comporta de forma diferente para las listas de entidades y las listas de direcciones IP. En el caso de las listas de entidades, GuardDuty validará que la cuenta del miembro actual sea propietaria del bucket de S3 especificado en el campo Ubicación. En el caso de las listas de direcciones IP, si no especificas un propietario de Cuenta de AWS ID, GuardDuty no realizará ninguna validación.

Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar la lista.

8. Seleccione la casilla Estoy de acuerdo y, a continuación, elija Actualizar lista.

## API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, como `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de lista que desee actualizar.

Para actualizar y activar una lista de entidades de confianza

1. Ejecute [UpdateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidad de confianza. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página

de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

2. Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface que actualizará el name de la lista de la y también la activará:

```
aws guardduty update-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que va a crear la lista de entidades de confianza y por otros valores de marcador de posición que lo seans*shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por. `--no-activate`

El parámetro `expected-bucket-owner` es opcional. Independientemente de que especifique o no el valor de este parámetro, GuardDuty valida que el Cuenta de AWS ID asociado a este `--detector-id` valor sea propietario del bucket de S3 especificado en el `--location` parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para actualizar y activar una lista de entidades de amenazas

1. Ejecute [UpdateThreatEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectorsAPI](#).

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

2. Como alternativa, puede ejecutar el siguiente comando AWS Command Line Interface que actualizará el name de la lista de la y también la activará:

```
aws guardduty update-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

detector-idSustitúyalo por el ID de detector de la cuenta de miembro para la que crearás la lista de entidades amenazantes y otros valores de marcador de posición que lo sean*shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro --activate por. --no-activate

El parámetro expected-bucket-owner es opcional. Si especifica o no el valor de este parámetro, GuardDuty valida que el Cuenta de AWS ID asociado a este --detector-id valor sea propietario del bucket de S3 especificado en el --location parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Solo se aplica a conjuntos personalizados de amenazas y entidades de confianza personalizadas. Si proporciona una URL de ubicación que no coincide con los siguientes formatos admitidos, recibirá un mensaje de error durante la adición y activación de la lista.

Para actualizar y activar una lista de direcciones IP de confianza

1. Ejecute [CreateIPSet](#). Asegúrese de proporcionar el valor de detectorId de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#)API.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS región.

2. También puede ejecutar el siguiente comando AWS Command Line Interface que también activa la lista.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que vaya a actualizar la lista de IP de confianza y por otros valores de marcador de posición que lo sean *shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no especificas el ID de cuenta propietario del bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de cuenta para el `expected-bucket-owner` parámetro, GuardDuty valida que este Cuenta de AWS ID sea propietario del bucket de S3 especificado en el `--location` parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

Para añadir y activar listas de IP de amenazas

1. Ejecute [CreateThreatIntelSet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

Restricciones de nombre de la lista: el nombre de la lista puede incluir letras minúsculas, mayúsculas, números, guión (-) y guión bajo (\_).

En el caso de una lista de direcciones IP, el nombre de la lista debe ser único dentro de una Cuenta de AWS región.

2. También puede ejecutar el siguiente comando AWS Command Line Interface que también activa la lista.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--name "AnyOrganization ListEXAMPLE" \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--activate
```

detector-idSustitúyelo por el identificador de la cuenta de miembro para la que vaya a actualizar la lista de direcciones IP peligrosas y por otros valores de marcador de posición que lo sean*shown in red*.

Si no desea activar esta lista recién creada, sustituya el parámetro `--activate` por `--no-activate`.

El parámetro `expected-bucket-owner` es opcional. Si no especificas el ID de cuenta propietario del bucket de S3, GuardDuty no realiza ninguna validación. Al especificar el ID de cuenta para el `expected-bucket-owner` parámetro, GuardDuty valida que este Cuenta de AWS ID sea propietario del bucket de S3 especificado en el `--location` parámetro. Si GuardDuty descubre que este bucket de S3 no pertenece al ID de cuenta especificado, aparecerá un mensaje de error al activar esta lista.

## De-activating lista de entidades o lista de direcciones IP

Cuando ya no desee GuardDuty utilizar una lista, puede desactivarla. El proceso puede tardar unos minutos en completarse. Para obtener más información, consulte [Consideraciones importantes para GuardDuty las listas](#). Una vez desactivada la lista, las entradas de la lista de entidades o de la lista de direcciones IP no afectarán a la detección de amenazas en ella. GuardDuty

Elija uno de los métodos de acceso para desactivar la lista.

### Console

Para desactivar la lista de entidades o la lista de direcciones IP

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, elija Listas.

3. En la página Lista, seleccione la pestaña en la que desee desactivar la lista: Listas de entidades o Lista de direcciones IP.
4. En la pestaña seleccionada, elija la lista que desee desactivar.
5. Elija Acciones y, a continuación, elija Desactivar.
6. Confirme la acción y elija Desactivar.

## API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, por ejemplo, `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de la lista que desee desactivar.

Para desactivar una lista de entidades de confianza

1. Ejecute [UpdateTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de entidades de confianza. Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty update-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

`detector-id` Sustitúyelo por el identificador de la cuenta de miembro para la que va a desactivar la lista de entidades de confianza y otros valores de marcador de posición que lo sean. *shown in red*

Para desactivar las listas de entidades de amenazas

1. Ejecute [UpdateThreatEntitySet](#). Asegúrese de proporcionar el valor de `detectorId` de la cuenta de miembro para la que desea desactivar esta lista de entidades de amenazas. Para encontrar el correspondiente `detectorId` a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty update-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

detector-idSustitúyalo por el ID de detector de la cuenta de miembro para la que crearás la lista de entidades amenazantes y otros valores de marcador de posición que lo sean*shown in red*.

Para desactivar una lista de direcciones IP de confianza

1. Ejecute [UpdateIPSet](#). Asegúrese de proporcionar el detectorId de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el detectorId correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#)API.
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir detector-id por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
aws guardduty update-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

Para desactivar la lista de IP de amenazas

1. Ejecute [UpdateThreatIntelSet](#). Asegúrese de proporcionar el detectorId de la cuenta de miembro para la que desea desactivar esta lista de direcciones IP de amenazas. Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#)API.
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir detector-id por el ID de detector de la cuenta de miembro para la que desactivará la lista de IP de amenazas.

```
aws guardduty update-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example \  
--no-activate
```

## Eliminar la lista de entidades o la lista de direcciones IP

Cuando ya no desee mantener una entrada de la lista en su conjunto de entidades o de direcciones IP, puede eliminarla. El proceso puede tardar unos minutos en completarse. Para obtener más información, consulte [Consideraciones importantes para GuardDuty las listas](#).

Si el estado de la lista es Activación o Desactivación, debe esperar unos minutos antes de realizar cualquier acción. Para obtener más información, consulte [Explicación de los estados de las listas](#).

Elija uno de los métodos de acceso para eliminar la lista.

### Console

Para eliminar la lista de entidades o la lista de direcciones IP

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, elija Listas.
3. En la página Lista, seleccione la pestaña en la que desee eliminar la lista: Listas de entidades o Lista de direcciones IP.
4. En la pestaña seleccionada, elija la lista que desee eliminar.
5. Elija Acciones y, a continuación, elija Eliminar.

El estado de la lista cambiará a Eliminar pendiente. Es posible que se tarde unos minutos en eliminar la lista.

### API/CLI

Para empezar con los siguientes procedimientos, necesitará el identificador, por ejemplo, `trustedEntitySetId`, `threatEntitySetId`, `trustedIpSet` o `threatIpSet`, que esté asociado al recurso de la lista que desee eliminar.



## Para eliminar una lista de entidades de confianza

1. Ejecute [DeleteTrustedEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea eliminar esta lista de entidades de confianza. Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty delete-trusted-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--trusted-entity-set-id d4b94fc952d6912b8f3060768example
```

`detector-id` Sustitúyalo por el identificador de la cuenta de miembro de la que vas a eliminar la lista de entidades de confianza y otros valores de marcador de posición que lo sean *shown in red*.

## Para desactivar las listas de entidades de amenazas

1. Ejecute [DeleteThreatEntitySet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea eliminar esta lista de entidades de amenazas. Para encontrar el `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.
2. También puede ejecutar el siguiente comando AWS Command Line Interface para hacerlo.

```
aws guardduty delete-threat-entity-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-entity-set-id d4b94fc952d6912b8f3060768example
```

`detector-id` Sustitúyalo por el ID de detección de la cuenta del miembro cuya lista de entidades amenazantes vaya a eliminar, junto con otros marcadores de posición. *shown in red*

Para eliminar una lista de direcciones IP de confianza

1. Ejecute [DeleteIPSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de confianza. Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir el `detector-id` por el ID de detector de la cuenta de miembro para la que actualizará la lista de direcciones IP de confianza.

```
aws guardduty delete-ip-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--ip-set-id d4b94fc952d6912b8f3060768example
```

`detector-id` Sustitúyalo por el ID de detección de la cuenta del miembro cuya lista de entidades amenazantes vaya a eliminar, junto con otros marcadores de posición. *shown in red*

Para eliminar la lista de IP de amenazas

1. Ejecute [DeleteThreatIntelSet](#). Asegúrese de proporcionar el `detectorId` de la cuenta de miembro para la que desea crear esta lista de direcciones IP de amenazas. Para encontrar el `detectorId` correspondiente a su cuenta y región actual, consulte la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecute la [ListDetectors](#) API.
2. Como alternativa, puede ejecutar el siguiente comando de la AWS Command Line Interface y asegurarse de sustituir `detector-id` por el ID de detector de la cuenta de miembro para la que eliminará la lista de IP de amenazas.

```
aws guardduty delete-threat-intel-set \  
--detector-id 12abc34d567e8fa901bc2d34e56789f0 \  
--threat-intel-set-id d4b94fc952d6912b8f3060768example
```

`detector-id` Sustitúyalo por el ID de detección de la cuenta del miembro cuya lista de entidades amenazantes vaya a eliminar, junto con otros marcadores de posición. *shown in red*

# Exportación de GuardDuty los hallazgos generados a buckets de Amazon S3

GuardDuty conserva los hallazgos generados durante un período de 90 días. GuardDuty exporta los resultados activos a Amazon EventBridge (EventBridge). Opcionalmente, puede exportar los resultados generados a un bucket de Amazon Simple Storage Service (Amazon S3). Esto ayudará a realizar un seguimiento de los datos históricos de actividades potencialmente sospechosas en la cuenta y a evaluar si las medidas de corrección recomendadas han tenido éxito.

Todos los nuevos hallazgos activos que se GuardDuty generen se exportan automáticamente unos 5 minutos después de generarse el hallazgo. Puede establecer la frecuencia con la que se exportan las actualizaciones de los hallazgos activos EventBridge. La frecuencia que seleccione se aplica a la exportación de nuevas apariciones de hallazgos existentes a EventBridge su bucket de S3 (cuando está configurado) y a Detective (cuando está integrado). Para obtener información sobre cómo GuardDuty se agregan varias apariciones de hallazgos existentes, consulte [GuardDuty encontrar agregación](#).

Cuando configura los ajustes para exportar los hallazgos a un bucket de Amazon S3, GuardDuty utiliza AWS Key Management Service (AWS KMS) para cifrar los datos de los hallazgos en su bucket de S3. Esto requiere que añada permisos a su bucket de S3 y a la AWS KMS clave para GuardDuty poder utilizarlos para exportar los resultados a su cuenta.

## Contenido

- [Consideraciones](#)
- [Paso 1: Permisos necesarios para la exportación de resultados](#)
- [Paso 2: Asociar la política a la clave de KMS](#)
- [Paso 3: Asociar la política al bucket de Amazon S3](#)
- [Paso 4: Exportar resultados a un bucket de S3 \(consola\)](#)
- [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#)

## Consideraciones

Antes de seguir con los requisitos previos y los pasos para exportar los resultados, considere los siguientes conceptos clave:

- Los ajustes de exportación son regionales: debe configurar las opciones de exportación en cada región que utilice GuardDuty.
- Exportación de los resultados a buckets de Amazon S3 en diferentes regiones Regiones de AWS (entre regiones): GuardDuty admite la siguiente configuración de exportación:
  - El bucket u objeto de Amazon S3 y la AWS KMS clave deben pertenecer al mismo sitio Región de AWS.
  - En el caso de los resultados generados en una región comercial, puede optar por exportar esos resultados a un bucket de S3 en cualquier región comercial. Sin embargo, no puede exportar estos resultados a un bucket de S3 en una región de inscripción.
  - En el caso de los resultados generados en una región de inscripción, puede optar por exportarlos a la misma región de inscripción en la que se generaron o a cualquier región comercial. Sin embargo, no puede exportar los resultados de una región de inscripción a otra región de inscripción.
- Permisos para exportar los hallazgos: para configurar los ajustes de exportación de los hallazgos activos, su bucket de S3 debe tener permisos que le GuardDuty permitan cargar objetos. También debe tener una AWS KMS clave que GuardDuty pueda utilizar para cifrar los hallazgos.
- Los resultados archivados no se exportan: el comportamiento predeterminado es que no se exportan los resultados archivados, incluidas las nuevas instancias de resultados suprimidos.

Cuando un GuardDuty hallazgo se genere como archivado, tendrás que desarchivarlo. Esto cambia el estado de búsqueda del filtro a Activo. GuardDuty exporta las actualizaciones de los hallazgos no archivados existentes en función de la configuración. [Paso 5: Frecuencia de exportación de los resultados](#)

- GuardDuty la cuenta de administrador puede exportar las conclusiones generadas en las cuentas de los miembros asociadas: al configurar la exportación en una cuenta de administrador, todas las conclusiones de las cuentas de los miembros asociadas que se generan en la misma región también se exportan a la misma ubicación que configuró para la cuenta de administrador. Para obtener más información, consulte [Comprender la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros](#).

## Paso 1: Permisos necesarios para la exportación de resultados

Al configurar los ajustes para la exportación de los resultados, selecciona un depósito de Amazon S3 donde puede almacenar los hallazgos y una AWS KMS clave para usarla para el cifrado de

datos. Además de los permisos para GuardDuty las acciones, también debe tener permisos para las siguientes acciones a fin de configurar correctamente los ajustes de exportación de los hallazgos:

- `s3:GetBucketLocation`
- `s3:PutObject`

Si necesita exportar los resultados a un prefijo específico de su bucket de Amazon S3, también debe añadir los siguientes permisos al rol de IAM:

- `s3:GetObject`
- `s3:ListBucket`

## Paso 2: Asociar la política a la clave de KMS

GuardDuty cifra los datos de los hallazgos de su depósito mediante AWS Key Management Service. Para configurar correctamente los ajustes, primero debe dar GuardDuty permiso para usar una clave KMS. Para conceder los permisos, [adjunte la política](#) a su clave de KMS.

Cuando usas una clave KMS de otra cuenta, debes aplicar la política de claves iniciando sesión en el Cuenta de AWS propietario de la clave. Al configurar los ajustes para exportar los resultados, también necesitará el ARN de la clave de la cuenta a la que pertenece la clave.

Para modificar la política de claves de KMS GuardDuty para cifrar los hallazgos exportados

1. Abra la AWS KMS consola en. <https://console.aws.amazon.com/kms>
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. Seleccione una clave de KMS existente o siga los pasos para [Crear una nueva clave](#) en la Guía para desarrolladores de AWS Key Management Service , que utilizará para cifrar los resultados exportados.

### Note

La clave Región de AWS de KMS y el bucket de Amazon S3 deben ser iguales.

Puede utilizar el mismo bucket de S3 y el mismo par de claves de KMS para exportar los resultados de cualquier región aplicable. Para obtener más información, consulte [Consideraciones](#) para exportar los resultados entre regiones.

4. En la sección Key policy (Política de claves), elija Edit (Editar).

Si aparece Cambiar a vista de política, elíjala para mostrar la Política de claves y, a continuación, elija Editar.

5. Copia el siguiente bloque de políticas a tu política de claves de KMS para conceder GuardDuty permiso para usar tu clave.

```
{
  "Sid": "AllowGuardDutyKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "guardduty.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "KMS key ARN",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "aws:SourceArn":
        "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
    }
  }
}
```

6. Edite la política sustituyendo los siguientes valores formateados *red* en el ejemplo de política:
  1. *KMS key ARN* Sustitúyala por el nombre de recurso de Amazon (ARN) de la clave KMS. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .
  2. *123456789012* Sustitúyalo por el Cuenta de AWS ID propietario de la GuardDuty cuenta que exporta los resultados.
  3. *Region2* Sustitúyalo por el Región de AWS lugar donde se generan los GuardDuty hallazgos.
  4. *SourceDetectorID* Sustitúyalo por el detectorID de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

Para encontrar la `detectorId` correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

 Note

Si la utilizas GuardDuty en una región con suscripción voluntaria, sustituye el valor del «Servicio» por el punto final regional de esa región. Por ejemplo, si utilizas GuardDuty la región de Oriente Medio (Baréin) (me-south-1), sustitúyala por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` [Para obtener información sobre los puntos de conexión de cada región que se haya suscrito, consulta GuardDuty los puntos de conexión y las cuotas.](#)

7. Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Seleccione Save.

8. (Opcional) copie la clave de ARN en un bloc de notas para utilizarla en los pasos posteriores.

## Paso 3: Asociar la política al bucket de Amazon S3

Añada permisos al depósito de Amazon S3 al que exportará los resultados para GuardDuty poder cargar objetos en este depósito de S3. Independientemente de si utiliza un bucket de Amazon S3 que pertenezca a su cuenta o a otra Cuenta de AWS, debe añadir estos permisos.

Si en algún momento decide exportar los resultados a un bucket de S3 diferente, para continuar con la exportación de resultados deberá agregar permisos a ese bucket de S3 y volver a configurar los ajustes de exportación de resultados.

Si aún no dispone de un bucket de Amazon S3 al que desee exportar estos resultados, consulte [Crear un bucket](#) en la Guía del usuario de Amazon S3.

## Para asociar permisos a la política del bucket de S3

1. Siga los pasos descritos en [Para crear o editar una política de bucket](#) en la Guía del usuario de Amazon S3, hasta que aparezca la página Editar política de bucket.
2. La política de ejemplo muestra cómo conceder GuardDuty permisos para exportar los resultados a su bucket de Amazon S3. Si cambia la ruta después de configurar la exportación de resultados, deberá modificar la política para conceder permiso a la nueva ubicación.

Copie la siguiente política de ejemplo y péguela en el Editor de políticas de bucket.

Si ha agregado la instrucción de política antes de la instrucción final, agregue una coma antes de agregar esta instrucción. Asegúrese de que la sintaxis JSON de la política de la clave de KMS es válida.

Política de ejemplo de bucket de S3

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow GetBucketLocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "guardduty.amazonaws.com"
      },
      "Action": "s3:GetBucketLocation",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "aws:SourceArn": "arn:aws:guardduty:us-east-2:123456789012:detector/SourceDetectorID"
        }
      }
    },
    {
      "Sid": "Allow PutObject",
      "Effect": "Allow",
```



```

    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012",
        "aws:SourceArn": "arn:aws:guardduty:us-east-2:123456789012:detector/SourceDetectorID"
      }
    }
  },
  {
    "Sid": "Deny unencrypted object uploads",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "aws:kms"
      }
    }
  },
  {
    "Sid": "Deny incorrect encryption header",
    "Effect": "Deny",
    "Principal": {
      "Service": "guardduty.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption-aws-kms-key-id":
        "arn:aws:kms:us-east-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      }
    }
  }
}

```

```

    }
  },
  {
    "Sid": "Deny non-HTTPS access",
    "Effect": "Deny",
    "Principal": "*",
    "Action": "s3:*",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket[optional prefix]/
    *,
    "Condition": {
      "Bool": {
        "aws:SecureTransport": "false"
      }
    }
  }
]
}

```

3. Edite la política sustituyendo los siguientes valores que están formateados *red* en el ejemplo de política:
  1. *Amazon S3 bucket ARN* Sustitúyalo por el nombre de recurso de Amazon (ARN) del bucket de Amazon S3. Puedes encontrar el ARN del bucket en la página Editar política del bucket de la <https://console.aws.amazon.com/s3/console>.
  2. *123456789012* Sustitúyalo por el Cuenta de AWS ID propietario de la GuardDuty cuenta que exporta los resultados.
  3. *us-east-2* Sustitúyalo por el Región de AWS lugar donde se generan los GuardDuty hallazgos.
  4. *SourceDetectorID* Sustitúyalo por el detectorID de la GuardDuty cuenta de la región específica en la que se generaron los hallazgos.

Para encontrar la detectorId correspondiente a tu cuenta y región actual, consulta la página de configuración de la <https://console.aws.amazon.com/guardduty/console> o ejecuta la [ListDetectors](#) API.

5. Sustituya *[optional prefix]* parte del valor del *S3 bucket ARN/[optional prefix]* marcador de posición por una ubicación de carpeta opcional a la que desee exportar los resultados. Para obtener más información sobre el uso de prefijos, consulte [Organizar objetos mediante prefijos](#) en la Guía del usuario de Amazon S3.

Si proporciona una ubicación de carpeta opcional que aún no existe, solo la GuardDuty creará si la cuenta asociada al depósito de S3 es la misma que la cuenta que exporta los resultados. Al exportar resultados a un bucket de S3 que pertenece a otra cuenta, la ubicación de la carpeta ya debe existir.

6. **KMS key ARN** Sustitúyala por el nombre de recurso de Amazon (ARN) de la clave de KMS asociada al cifrado de los hallazgos exportados al bucket de S3. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .

 Note

Si la utiliza GuardDuty en una región con suscripción voluntaria, sustituya el valor del «Servicio» por el punto final regional de esa región. Por ejemplo, si utiliza GuardDuty la región de Oriente Medio (Baréin) (me-south-1), sustitúyala por. "Service": "guarddduty.amazonaws.com" "Service": "guarddduty.me-south-1.amazonaws.com" [Para obtener información sobre los puntos de conexión de cada región que se haya suscrito, consulta GuardDuty los puntos de conexión y las cuotas.](#)

4. Seleccione Save.

## Paso 4: Exportar resultados a un bucket de S3 (consola)

GuardDuty permite exportar los resultados a un depósito existente en otro. Cuenta de AWS

Al elegir un bucket nuevo o existente en su cuenta, puede agregar un prefijo. Al configurar las conclusiones de exportación, GuardDuty crea una nueva carpeta en el depósito de S3 para guardar las conclusiones. El prefijo se añadirá a la estructura de carpetas predeterminada que se GuardDuty creó. Por ejemplo, el formato del prefijo opcional /AWSLogs/**123456789012**/GuardDuty/**Region**.

La ruta completa del objeto de S3 será **amzn-s3-demo-bucket/prefix-name/UUID.jsonl.gz**. El UUID se genera aleatoriamente y no representa el ID del detector ni el ID del resultado.

 Important

La clave de KMS y el bucket de S3 deben estar en la misma región.

Antes de completar estos pasos, asegúrese de que ha asociado las políticas respectivas a la clave de KMS y al bucket de S3 existente.

### Configuración de la opción de exportación de resultados

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, seleccione Configuración.
3. En la página Configuración, bajo Opciones de exportación de resultados, en Bucket de S3, elija Configurar ahora (o Editar, según sea necesario).
4. En ARN del bucket de S3, ingrese el **bucket ARN**. Para encontrar el ARN del bucket, consulte [Ver las propiedades de un bucket de S3](#) en la Guía del usuario de Amazon S3.
5. En ARN de la clave de KMS, ingrese el **key ARN**. Para localizar el ARN de la clave, consulte [Encontrar el ID y el ARN de la clave](#) en la Guía para desarrolladores de AWS Key Management Service .
6. Asociar políticas
  - Siga los pasos para asociar la política del bucket de S3. Para obtener más información, consulte [Paso 3: Asociar la política al bucket de Amazon S3](#).
  - Siga los pasos para asociar la política de clave de KMS. Para obtener más información, consulte [Paso 2: Asociar la política a la clave de KMS](#).
7. Seleccione Save.

## Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados

Configure la frecuencia para exportar los resultados activos actualizados según convenga al entorno. De forma predeterminada, los resultados actualizados se exportan cada 6 horas. Esto significa que cualquier dato que se actualice después de la exportación más reciente se incluirá en la siguiente exportación. Si los hallazgos actualizados se exportan cada 6 horas y la exportación se produce a las 12:00, cualquier hallazgo que actualice después de las 12:00 se exportará a las 18:00.

### Establecimiento de la frecuencia

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Seleccione Configuración.

3. En la sección Opciones de exportación de resultados, seleccione Frecuencia de los resultados actualizados. Esto establece la frecuencia de exportación de los hallazgos activos actualizados tanto EventBridge a Amazon S3 como a Amazon S3. Puede elegir entre las siguientes opciones:
  - Actualice EventBridge y S3 cada 15 minutos
  - Actualice EventBridge y S3 cada 1 hora
  - Actualice EventBridge y S3 cada 6 horas (predeterminado)
4. Seleccione Save changes (Guardar cambios).

## Procesando GuardDuty las conclusiones con Amazon EventBridge

GuardDuty publica (envía) automáticamente los resultados como eventos a Amazon EventBridge (anteriormente Amazon CloudWatch Events), un servicio de bus de eventos sin servidor. EventBridge ofrece un flujo de datos prácticamente en tiempo real desde aplicaciones y servicios a destinos como temas AWS Lambda, funciones y transmisiones de Amazon Kinesis del Amazon Simple Notification Service (Amazon SNS). Para obtener más información, consulta la [Guía EventBridge del usuario de Amazon](#).

EventBridge permite la supervisión y el procesamiento automatizados de GuardDuty los hallazgos mediante la recepción de [eventos](#). EventBridge recibe eventos tanto para los hallazgos recién generados como para los hallazgos agregados, donde las apariciones posteriores de un hallazgo existente se combinan con el original. A cada GuardDuty hallazgo se le asigna un identificador de hallazgo y GuardDuty crea un EventBridge evento para cada hallazgo con un identificador de hallazgo único. Para obtener información sobre cómo funciona la agregación GuardDuty, consulte [GuardDuty encontrar agregación](#).

Además de la supervisión y el procesamiento automatizados, el uso de EventBridge permite conservar los datos de sus hallazgos a más largo plazo. GuardDuty almacena los resultados durante 90 días. Con EventBridge él, puede enviar los datos de los hallazgos a su plataforma de almacenamiento preferida y almacenar los datos durante el tiempo que desee. Para conservar los hallazgos durante más tiempo, GuardDuty apoya [Exportar los resultados generados a Amazon S3](#).

### Temas

- [Comprender la frecuencia EventBridge de las notificaciones en GuardDuty](#)
- [Configuración de un tema y un punto de conexión de Amazon SNS \(correo electrónico, Slack y Amazon Chime\)](#)

- [Uso de Amazon EventBridge para encontrar GuardDuty información](#)
- [Crear una EventBridge regla para los GuardDuty hallazgos](#)
- [EventBridge regla para entornos con GuardDuty varias cuentas](#)

## Comprender la frecuencia EventBridge de las notificaciones en GuardDuty

En esta sección se explica con qué frecuencia recibes notificaciones de búsqueda EventBridge y cómo actualizar la frecuencia para que se produzcan búsquedas posteriores.

Notificaciones de resultados recién generados con un identificador de resultado único

GuardDuty envía estas notificaciones prácticamente en tiempo real cuando genera un hallazgo con un identificador de hallazgo único. La notificación incluye todas las apariciones posteriores de este identificador de búsqueda durante el proceso de generación de la notificación.

La frecuencia de notificación de los resultados recién generados es casi en tiempo real. De forma predeterminada, no se puede modificar esta frecuencia.

Notificaciones de casos de resultados subsiguientes

GuardDuty agrupa todas las incidencias subsiguientes de un tipo de hallazgo concreto que se produzcan en intervalos de 6 horas en un único suceso. Solo una cuenta de administrador puede actualizar la frecuencia de EventBridge notificaciones para que se produzcan búsquedas posteriores. Una cuenta de miembro no puede actualizar esta frecuencia para su propia cuenta. Por ejemplo, si la cuenta de GuardDuty administrador delegado actualiza la frecuencia a una hora, todas las cuentas de los miembros también tendrán una frecuencia de notificación de una hora sobre las siguientes búsquedas que EventBridge se envíen. Para obtener más información, consulte [Varias cuentas en Amazon GuardDuty](#).

Como cuenta de administrador, puede personalizar la frecuencia predeterminada de las notificaciones sobre las incidencias de resultados posteriores. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. Para obtener información acerca de la configuración de la frecuencia de estas notificaciones, consulte [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#).

Para obtener más información sobre cómo las cuentas de administrador reciben EventBridge notificaciones para las cuentas de los miembros, consulte [EventBridge regla para entornos con varias cuentas](#).

## Configuración de un tema y un punto de conexión de Amazon SNS (correo electrónico, Slack y Amazon Chime)

Amazon Simple Notification Service (Amazon SNS) es un servicio totalmente administrado que proporciona la entrega de mensajes de los publicadores a los suscriptores. Los publicadores se comunican de forma asíncrona con los suscriptores mediante el envío de mensajes a un tema. Un tema es un punto de acceso lógico y un canal de comunicación que le permite agrupar varios puntos de enlace AWS Lambda, como Amazon Simple Queue Service (Amazon HTTP/S SQS) y una dirección de correo electrónico.

### Note

Puedes añadir un tema de Amazon SNS a la regla de EventBridge eventos que prefieras durante o después de la creación de la regla.

### Crear un tema de Amazon SNS

Para empezar, antes se debe configurar un tema en Amazon SNS y agregar un punto de conexión. Para crear un tema, siga los pasos indicados en [Paso 1: Crear un tema](#) en la Guía para desarrolladores de Amazon Simple Notification Service. Después de crear el tema, copie el ARN del tema en el portapeles. Utilizará este ARN del tema para continuar con una de las configuraciones preferidas.

Elija un método preferido para establecer a dónde quiere enviar los datos de GuardDuty búsqueda.

### Email setup

Para configurar un punto de conexión de correo electrónico

Después de [Create an Amazon SNS topic](#), el siguiente paso es crear una suscripción a este tema. Siga los pasos indicados en [Paso2: Creación de una suscripción a un tema de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Notification Service.

1. Para el ARN del tema, utilice el ARN del tema creado en el paso [Create an Amazon SNS topic](#). El ARN de tema tiene un aspecto similar al siguiente:

```
arn:aws:sns:us-east-2:123456789012:your_topic
```

2. En Protocol, seleccione Email.
3. En Punto de conexión, escriba la dirección de correo electrónico donde desee que se reciban las notificaciones de Amazon SNS.

Después de creada la suscripción, tendrá que confirmarla a través del cliente de correo electrónico.

## Slack setup

Configuración de un Amazon Q Developer en el cliente de aplicaciones de chat - Slack

Después de [Create an Amazon SNS topic](#), el siguiente paso es configurar el cliente para Slack.

Siga los pasos en [Tutorial: Primeros pasos con Slack](#) en la Guía del administrador de aplicaciones de chat de Amazon Q Developer.

## Chime setup

Configuración de un Amazon Q Developer en el cliente de aplicaciones de chat - Chime

Después de [Create an Amazon SNS topic](#), el siguiente paso es configurar Amazon Q Developer para Chime.

Siga los pasos en [Tutorial: Primeros pasos con Amazon Chime](#) en la Guía del administrador de aplicaciones de chat de Amazon Q Developer.

## Uso de Amazon EventBridge para encontrar GuardDuty información

Con EventBridge, crea reglas para especificar los eventos que desea monitorear. Estas reglas también especifican los servicios y aplicaciones de destino que pueden realizar acciones automatizadas si se producen estos eventos. Un [objetivo](#) es un destino (un recurso o un punto final) EventBridge al que se envía un evento cuando el evento coincide con el patrón de eventos definido en la regla. Cada evento es un objeto JSON que se ajusta al EventBridge esquema de AWS eventos y contiene una representación en JSON de un hallazgo. Puede personalizar la regla para que envíe solo los eventos que cumplan determinados criterios. Para obtener más información, consulte [tema sobre el esquema de JSON]. Como los datos de los hallazgos están estructurados como un [EventBridgeevento](#), puedes monitorizarlos, procesarlos y actuar en consecuencia mediante el uso de otras aplicaciones, servicios y herramientas.



Para recibir notificaciones sobre GuardDuty los hallazgos basados en eventos, debe crear una EventBridge regla y un objetivo para GuardDuty. Esta regla permite EventBridge enviar notificaciones de los hallazgos que se GuardDuty generen al objetivo especificado en la regla.

#### Note

EventBridge y CloudWatch Events son el mismo servicio y API subyacentes. Sin embargo, EventBridge incluye funciones adicionales que le ayudan a recibir eventos de aplicaciones de software como servicio (SaaS) y de sus propias aplicaciones. Como el servicio y la API subyacentes son los mismos, el esquema de eventos para GuardDuty los hallazgos también es el mismo.

### Cómo funcionan los hallazgos archivados y no archivados con GuardDuty EventBridge

En el caso de las conclusiones que se archivan manualmente, las apariciones iniciales y todas las posteriores (generadas una vez finalizado el archivado) se envían en EventBridge función de una frecuencia de notificación específica. Para obtener más información, consulte [Comprender la frecuencia EventBridge de las notificaciones en GuardDuty](#).

En el caso de las conclusiones que se archivan automáticamente [Reglas de supresión](#), no se envían a la carpeta ni a todas las incidencias posteriores (generadas una vez finalizado el archivado). EventBridge Puede ver estas conclusiones archivadas automáticamente en la consola. GuardDuty

### Esquema de evento

Un [patrón de eventos](#) define los datos que se EventBridge utilizan para determinar si se debe enviar el evento al objetivo. El EventBridge evento para GuardDuty tiene el siguiente formato:

```
{
  "version": "0",
  "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
  "detail-type": "GuardDuty Finding",
  "source": "aws.guardduty",
  "account": "111122223333",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
}
```

El valor de `detail` devuelve los detalles en formato JSON de un solo resultado como objeto, en lugar de devolver toda la sintaxis de la respuesta resultados, que puede respaldar varios resultados dentro de una matriz.

Para obtener una lista completa de todos los parámetros incluidos en `GUARDDUTY_FINDING_JSON_OBJECT`, consulte [GetFindings](#). El parámetro `id` que aparece en la `GUARDDUTY_FINDING_JSON_OBJECT` es el ID de resultado descrito anteriormente.

## Crear una EventBridge regla para los GuardDuty hallazgos

En los siguientes procedimientos se explica cómo utilizar la EventBridge consola de Amazon y el [AWS Command Line Interface \(AWS CLI\)](#) para crear una EventBridge regla para GuardDuty los hallazgos. La regla detecta EventBridge los eventos que utilizan el esquema y el patrón de eventos para los GuardDuty hallazgos y los envía a una AWS Lambda función para su procesamiento.

AWS Lambda es un servicio informático que puede utilizar para ejecutar código sin aprovisionar ni administrar servidores. Empaqueta el código y lo carga AWS Lambda como una función Lambda. AWS Lambda luego ejecuta la función cuando se invoca la función. Una función se puede invocar manualmente, automáticamente en respuesta a eventos o en respuesta a solicitudes de aplicaciones o servicios. Para obtener más información acerca de cómo crear e invocar funciones de Lambda, consulte la [Guía para desarrolladores de AWS Lambda](#).

Elige el método que prefieras para crear una EventBridge regla que envíe tu GuardDuty hallazgo a un objetivo.

### Console

Siga estos pasos para usar la EventBridge consola de Amazon y crear una regla que envíe automáticamente todos los eventos de GuardDuty búsqueda a una función de Lambda para su procesamiento. La regla usa la configuración predeterminada para las reglas que se ejecutan cuando se reciben eventos específicos. Para obtener más información sobre la configuración de las reglas o para aprender a crear una regla que utilice una configuración personalizada, consulta [Crear reglas que reaccionen a los eventos](#) en la Guía del EventBridge usuario de Amazon.

Antes de crear la regla, cree la función de Lambda que quiere que la regla utilice como destino. Cuando cree la regla, tendrá que especificar esta función como destino. Su destino también puede ser el tema de SNS que creó anteriormente. Para obtener más información, consulte [Configuración de un tema y un punto de conexión de Amazon SNS \(correo electrónico, Slack y Amazon Chime\)](#).

## Crear una regla para un evento con la consola

1. Inicia sesión en la EventBridge consola de Amazon Consola de administración de AWS y ábrela en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, en Buses, elija Reglas.
3. En la sección Reglas, elija Crear regla.
4. En la página Definir detalle de la regla, haga lo siguiente:
  - a. En Nombre, ingrese el nombre de la regla.
  - b. (Opcional) En Descripción, ingrese una breve descripción de la regla de autorización.
  - c. En el caso del Bus de eventos, asegúrese de que esté seleccionada la opción predeterminada y que esté activada la opción Habilitar la regla en el bus de eventos seleccionado.
  - d. En Tipo de regla, elija Regla con un patrón de evento.
  - e. Cuando haya terminado, elija Siguiente.
5. En la página Crear patrón de evento, realice una de las siguientes acciones:
  - a. En Origen del evento, selecciona AWS eventos o eventos EventBridge asociados.
  - b. (Opcional) En el caso de un evento de muestra, consulta un ejemplo de evento de búsqueda GuardDuty para saber qué puede contener un evento. Para ello, seleccione AWS eventos. A continuación, en Ejemplos de eventos, selecciona GuardDutyBuscar.
  - c. Opción 1: usar el formulario de patrón, una plantilla que EventBridge proporciona

En la sección Patrón de eventos, realice una de las siguientes acciones:

1. En Método de creación, seleccione Usar forma de patrón.
2. En Origen del evento, elija Servicios de AWS.
3. En Servicio de AWS, elija GuardDuty.
4. En Tipo de evento, elija GuardDuty Buscar.

Cuando haya terminado, elija Siguiente.

- d. Opción 2: Uso de un patrón de eventos personalizado en JSON

En la sección Patrón de eventos, realice una de las siguientes acciones:

1. En Método de creación, elija Patrón personalizado (editor JSON).

2. En el patrón de eventos, pegue el siguiente JSON personalizado para crear una alerta con los resultados medios, altos y críticos. Para obtener más información, consulte [Niveles de gravedad de los resultados](#).

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
```

```
        6.7,  
        6.8,  
        6.9,  
        7,  
        7.0,  
        7.1,  
        7.2,  
        7.3,  
        7.4,  
        7.5,  
        7.6,  
        7.7,  
        7.8,  
        7.9,  
        8,  
        8.0,  
        8.1,  
        8.2,  
        8.3,  
        8.4,  
        8.5,  
        8.6,  
        8.7,  
        8.8,  
        8.9,  
        9,  
        9.0,  
        9.1,  
        9.2,  
        9.3,  
        9.4,  
        9.5,  
        9.6,  
        9.7,  
        9.8,  
        9.9,  
        10,  
        10.0  
    ]  
}  
}
```

Cuando haya terminado, elija Siguiente.

## 6. Opción A: Seleccionar Servicio de AWS - AWS Lambda como objetivo

En la página Seleccionar destino(s), haga lo siguiente:

- Para los tipos de destino, seleccione Servicio de AWS.
- En Seleccione destino, elija Función de Lambda. Luego, en Función, elija la función de Lambda a la que quiera enviar los eventos de resultados.
- version/alias En Configure, introduzca los ajustes de versión o alias de la función Lambda de destino.
- (Opcional) En Configuración adicional, introduzca una configuración personalizada para especificar qué datos de eventos desea enviar a la función de Lambda. También puede especificar cómo gestionar los eventos que no se envíen correctamente a la función.
- Cuando haya terminado, elija Siguiente.

## 7. Opción B: Selección del tema de SNS como destino

En la página Seleccionar destino(s), haga lo siguiente:

- Para los tipos de destino, seleccione Servicio de AWS.
- Para Seleccione un destino, elija Tema de SNS. A continuación, en Ubicación de destino, seleccione la opción adecuada en función de la ubicación de destino. En la lista Tema, seleccione el nombre del tema de SNS que creó.
- Amplíe Configuración adicional. En Configurar entrada de destino, seleccione Transformador de entrada).
- Elija Configurar transformador de entrada.
- Copie el siguiente código en el campo Ruta de entrada de la sección Transformador de entrada de destino.

```
{
  "severity": "$.detail.severity",
  "Account_ID": "$.detail.accountId",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_Description": "$.detail.description"
}
```

- Copie el código siguiente y péguelo en el campo Plantilla para dar formato al correo

electrónico

```
"You have a severity <severity> GuardDuty finding type <Finding_Type> in the
<region> Region."
"Finding Description:"
"<Finding_Description>. "
"For more details open the GuardDuty console at https://
console.aws.amazon.com/guardduty/home?region=<region>#/findings?search=id
%3D<Finding_ID>"
```

8. En la página Configurar etiquetas, si lo desea, introduzca una o más etiquetas para asignarlas a la regla. A continuación, elija Siguiente.
9. En la página Revisar y crear, revise cada configuración y compruebe que es correcta.

Para cambiar una configuración, elija Editar en la sección que contiene la configuración y, a continuación, escriba la configuración adecuada. También puede usar las pestañas de navegación para ir a la página que contiene una configuración.

10. Cuando termine de verificar la configuración, elija Crear regla.

## API

El siguiente procedimiento muestra cómo utilizar los AWS CLI comandos para crear una EventBridge regla y un destino para GuardDuty. En concreto, el procedimiento muestra cómo crear una regla que permita EventBridge enviar eventos para todos los hallazgos que se GuardDuty generen a una AWS Lambda función como destino de la regla.

### Note

En este ejemplo, utilizamos una función Lambda como objetivo de la regla que se activa. EventBridge También puedes configurar otros AWS recursos como objetivos para EventBridge activarlos. GuardDuty y EventBridge admiten los siguientes tipos de objetivos: instancias de Amazon EC2, transmisiones de Amazon Kinesis, tareas de Amazon ECS AWS Step Functions , máquinas de estado, comandos y run destinos integrados. Para obtener más información, consulta [PutTargets](#) la referencia de la EventBridge API de Amazon.

## Creación de una regla y un destino

1. Para crear una regla que permita EventBridge enviar eventos para todos los hallazgos que se GuardDuty generen, ejecute el siguiente comando EventBridge CLI.

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guarddduty\"]}"
```

Puede personalizar aún más la regla para que indique que solo se EventBridge envíen eventos para un subconjunto de los GuardDuty-generated hallazgos. Este subconjunto se basa en los atributos de resultado o atributos especificados en la regla. Por ejemplo, utilice el siguiente comando CLI para crear una regla que EventBridge permita enviar solo eventos para los GuardDuty hallazgos con una gravedad de 5 u 8:

```
aws events put-rule --name your-rule-name --event-pattern "{\"source\":  
[\"aws.guarddduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":  
{\"severity\":[5,8]}}"
```

Para ello, puede utilizar cualquiera de los valores de propiedad que estén disponibles en el JSON para GuardDuty los hallazgos.

2. Para adjuntar una función Lambda como destino para la regla que creó en el paso 1, ejecute el siguiente comando CloudWatch CLI.

```
aws events put-targets --rule your-target-name --targets  
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:your_function
```

Asegúrese de reemplazar *your-target-name* el comando anterior por su función Lambda real para los GuardDuty eventos.

3. Para agregar los permisos necesarios para invocar el destino, ejecute el siguiente comando de la CLI de Lambda.

```
aws lambda add-permission --function-name your-target-name --statement-id 1 --  
action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

Asegúrese de reemplazar *your\_function* el comando anterior por su función Lambda real para los GuardDuty eventos.



## EventBridge regla para entornos con GuardDuty varias cuentas

Al utilizar una cuenta de GuardDuty administrador delegado, puede ver los eventos generados en las cuentas de los miembros y tomar medidas mediante otras aplicaciones y servicios. EventBridge las reglas de su cuenta de administrador se activarán en función de las conclusiones aplicables de sus cuentas de miembros. Si configuras la búsqueda de notificaciones a través EventBridge de tu cuenta de administrador, recibirás notificaciones de los hallazgos tanto de tu cuenta como de las cuentas de los miembros. Por ejemplo, puede utilizar EventBridge para enviar tipos específicos de resultados a una función Lambda que procesa y envía los datos a su sistema de gestión de incidentes y eventos de seguridad (SIEM).

Puede identificar la cuenta del miembro en la que se originó el GuardDuty hallazgo mediante el `accountId` campo de los detalles JSON del hallazgo. Para crear una regla de eventos personalizada para cuentas de miembros específicas, cree una nueva regla y use la siguiente plantilla en Patrón de eventos. `123456789012` Sustitúyala por la `accountId` de la cuenta de miembro para la que quieres activar el evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

### Note

En este ejemplo, se crea una regla que coincide con todos los resultados del identificador de cuenta especificado. Se pueden incluir varios ID de cuenta separándolos con comas, siguiendo la sintaxis JSON.

# Descripción de CloudWatch los registros y los motivos por los que se omiten recursos durante el análisis de EC2 con Malware Protection

GuardDuty Malware Protection for EC2 publica los eventos en el grupo de CloudWatch registro de Amazon `aws/guardduty/malware-scan-events`. Para cada uno de los eventos relacionados con el análisis de malware, puede supervisar el estado y el resultado del análisis de los recursos afectados. Es posible que se hayan omitido determinados recursos de Amazon EC2 y volúmenes de Amazon EBS durante el análisis de Malware Protection for EC2.

## Los registros de auditoría en Malware Protection for EC2 CloudWatch GuardDuty

El grupo de registros `aws/guardduty` CloudWatch `/malware-scan-events` admite tres tipos de eventos de análisis.

| Nombre del evento de análisis de Malware Protection for EC2 | Explicación                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2_SCAN_STARTED                                            | Se crea cuando una protección contra GuardDuty malware para EC2 inicia el proceso de análisis de malware, por ejemplo, cuando se prepara para tomar una instantánea de un volumen de EBS.                                                                                                                                                                        |
| EC2_SCAN_COMPLETED                                          | Se crea cuando GuardDuty Malware Protection for EC2 escanea al menos uno de los volúmenes de EBS del recurso afectado. Este evento también incluye el valor de <code>snapshotId</code> que pertenece al volumen de EBS analizado. Una vez finalizado el análisis, el resultado será <code>CLEAN</code> , <code>THREATS_FOUND</code> o <code>NOT_SCANNED</code> . |
| EC2_SCAN_SKIPPED                                            | Se crea cuando el escaneo de GuardDuty Malware Protection for EC2 omite todos los                                                                                                                                                                                                                                                                                |

| Nombre del evento de análisis de Malware Protection for EC2 | Explicación                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             | volúmenes de EBS del recurso afectado. Para identificar el motivo de la omisión, seleccione el evento correspondiente y consulte los detalles. Para obtener más información sobre los motivos de la omisión, consulte <a href="#">Motivos para omitir un recurso durante el análisis de malware</a> a continuación. |

### Note

Si utilizas una AWS Organizations, los eventos de CloudWatch registro de las cuentas de los miembros de Organizations se publican tanto en la cuenta del administrador como en el grupo de registro de la cuenta de miembro.

Elige el método de acceso que prefieras para ver y consultar CloudWatch los eventos.

### Console

1. Inicie sesión en Consola de administración de AWS y abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, en Registros, seleccione Grupos de registros. Seleccione el grupo de registros/aws/guardduty/malware-scan-events para ver los eventos de análisis de Malware Protection for EC2. GuardDuty

Para ejecutar una consulta, elija Información de registros.

Para obtener información sobre cómo ejecutar una consulta, consulte [Análisis de datos de registro con CloudWatch Logs Insights](#) en la Guía del CloudWatch usuario de Amazon.

3. Elija ID de análisis para supervisar los detalles del recurso afectado y los resultados de malware. Por ejemplo, puede ejecutar la siguiente consulta para filtrar los eventos del CloudWatch registro mediante scanId. Asegúrese de usar su propia versión válida *scan-id*.

```
fields @timestamp, @message, scanRequestDetails.scanId as scanId
```

```
| filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
| sort @timestamp asc
```

## API/CLI

- Para trabajar con grupos de registros, consulte [Buscar entradas de registro mediante AWS CLI](#) la Guía del CloudWatch usuario de Amazon.

Elija el grupo de registros/aws/guardduty/malware-scan-events para ver los eventos de escaneo de Malware Protection for EC2. GuardDuty

- Para ver y filtrar los eventos de registro, consulte [GetLogEvents](#) y [FilterLogEvents](#), respectivamente, en la referencia de la CloudWatch API de Amazon.

## GuardDuty Protección contra malware para la retención de registros de EC2

El período de retención de registros predeterminado para el grupo de registros aws/guardduty/malware-scan-events es de 90 días, tras lo cual los eventos de registro se eliminan automáticamente. Para cambiar la política de retención de registros de tu grupo de CloudWatch registros, consulta [Cambiar la retención de datos de registro en CloudWatch los registros](#) en la Guía del CloudWatch usuario de Amazon o [PutRetentionPolicy](#) en la Referencia de la CloudWatch API de Amazon.

## Motivos para omitir un recurso durante el análisis de malware

En los eventos relacionados con el análisis de malware, es posible que se hayan omitido algunos recursos de EC2 y volúmenes de EBS durante el proceso de análisis. En la siguiente tabla se enumeran los motivos por los que GuardDuty Malware Protection for EC2 puede no analizar los recursos. Si procede, siga los pasos propuestos para resolver estos problemas y analice estos recursos la próxima vez que GuardDuty Malware Protection for EC2 inicie un análisis de malware. Los demás problemas se utilizan para informarle sobre el curso de los eventos y no son procesables.

| Razones de omisión  | Explicación                                              | Pasos propuestos                                            |
|---------------------|----------------------------------------------------------|-------------------------------------------------------------|
| RESOURCE_ NOT_FOUND | La resourceArn información proporcionada para iniciar el | Valide el valor de resourceArn de la carga de trabajo de su |

| Razones de omisión | Explicación                                                                                                                         | Pasos propuestos                                                                                                                                                         |  |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                    | análisis de malware bajo demanda no se encontró en su AWS entorno.                                                                  | instancia o contenedor de Amazon EC2 e inténtelo de nuevo.                                                                                                               |  |
| ACCOUNT_INELIGIBLE | El identificador de AWS cuenta desde el que intentó iniciar un análisis de On-demand software malicioso no está activado GuardDuty. | Comprueba que GuardDuty esté activado para esta AWS cuenta.<br><br>Cuando GuardDuty habilitas una nueva Región de AWS , la sincronización puede tardar hasta 20 minutos. |  |

| Razones de omisión         | Explicación                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Pasos propuestos                                                                                                                                                                                                                                        |  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| UNSUPPORTED_KEY_ENCRYPTION | <p>GuardDuty Malware Protection for EC2 admite volúmenes cifrados y no cifrados con una clave gestionada por el cliente. No admite el análisis de volúmenes de EBS cifrados con el <a href="#">cifrado de Amazon EBS</a>.</p> <p>Actualmente, existe una diferencia regional por la que no se aplica este motivo de omisión. Para obtener más información al respecto Regiones de AWS, consulte. <a href="#">Region-specific disponibilidad de funciones</a></p> | <p>Sustituya la clave de cifrado por una clave administrada por el cliente. Para obtener más información sobre los tipos de cifrado GuardDuty compatibles, consulte <a href="#">Volúmenes de Amazon EBS compatibles con el análisis de malware</a>.</p> |  |

| Razones de omisión        | Explicación                                                                                                                                                                                                                                                                                                                                                                      | Pasos propuestos                                                                                                                                                                                              |  |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| EXCLUDED_BY_SCAN_SETTINGS | La instancia de EC2 o el volumen de EBS se excluyó durante el análisis de malware. Hay dos posibilidades: la etiqueta se agregó a la lista de inclusión, pero el recurso no está asociado a esta etiqueta, la etiqueta se agregó a la lista de exclusión y el recurso está asociado a esta etiqueta o la etiqueta GuardDuty Excluded está establecida en true para este recurso. | Actualice las opciones de análisis o las etiquetas asociadas a su recurso de Amazon EC2. Para obtener más información, consulte <a href="#">Opciones de análisis con etiquetas definidas por el usuario</a> . |  |
| UNSUPPORTED_VOLUME_SIZE   | El volumen es mayor que 2048 GB.                                                                                                                                                                                                                                                                                                                                                 | No se puede procesar.                                                                                                                                                                                         |  |
| NO_VOLUMES_ATTACHED       | GuardDuty Malware Protection for EC2 encontró la instancia en su cuenta, pero no se adjuntó ningún volumen de EBS a esta instancia para continuar con el escaneo.                                                                                                                                                                                                                | No se puede procesar.                                                                                                                                                                                         |  |
| UNABLE_TO_SCAN            | Se trata de un error de servicio interno.                                                                                                                                                                                                                                                                                                                                        | No se puede procesar.                                                                                                                                                                                         |  |

| Razones de omisión     | Explicación                                                                                                                                                                                   | Pasos propuestos                                                                                                                                                                                                                                                               |  |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| SNAPSHOT_NOT_FOUND     | No se encontraron las instantáneas creadas a partir de los volúmenes de EBS y compartidas con la cuenta de servicio, y GuardDuty Malware Protection for EC2 no pudo continuar con el escaneo. | Asegúrese de que CloudTrail las instantáneas no se hayan eliminado de forma intencionada.                                                                                                                                                                                      |  |
| SNAPSHOT_QUOTA_REACHED | Ha alcanzado el volumen máximo permitido de instantáneas para cada región. Esto impide no solo retener, sino también crear nuevas instantáneas.                                               | Puede eliminar las instantáneas antiguas o solicitar un aumento de cuota. Puede ver el límite predeterminado de instantáneas por región y consultar cómo solicitar un aumento de cuota en el apartado <a href="#">Service quotas</a> en la Guía de referencia general de AWS . |  |



| Razones de omisión                     | Explicación                                                                                                                                                                                                     | Pasos propuestos      |  |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--|
| MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED | Se adjuntaron más de 11 volúmenes de EBS a una instancia EC2. GuardDuty Malware Protection for EC2 escaneó los primeros 11 volúmenes de EBS y los obtuvo ordenando los alfabéticamente. <code>deviceName</code> | No se puede procesar. |  |

| Razones de omisión                    | Explicación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Pasos propuestos      |  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|--|
| UNSUPPORT<br>ED_PRODUC<br>T_CODE_TYPE | <p>GuardDuty puede escanear la mayoría de las instancias con as. productCode de marketplace. Es posible que algunas instancias del mercado no sean aptas para el escaneo. GuardDuty omitirá esas instancias y registrará el motivo como UNSUPPORT ED_PRODUC T_CODE_TYPE .</p> <p>Esta compatibilidad varía en AWS GovCloud (US) y en las regiones de China. Para obtener más información, consulte <a href="#">Region-specific disponibilidad de funciones</a>.</p> <p>Para obtener más información, consulte <a href="#">AMI pagadas</a> en la Guía del usuario de Amazon EC2.</p> <p>Para obtener más información sobre productCode , consulte <a href="#">ProductCode</a></p> | No se puede procesar. |  |

| Razones de omisión | Explicación                               | Pasos propuestos |  |
|--------------------|-------------------------------------------|------------------|--|
|                    | en la Referencia de la API de Amazon EC2. |                  |  |

## Reportar falsos positivos en la protección contra malware para EC2

GuardDuty Los escaneos de Malware Protection for EC2 pueden identificar un archivo inofensivo en la carga de trabajo de su instancia o contenedor de Amazon EC2 como malicioso o dañino. Para mejorar su experiencia con Malware Protection for EC2 y el GuardDuty servicio, puede informar de resultados falsos positivos si cree que un archivo identificado como malicioso o dañino durante un análisis no contiene realmente malware.

Para reportar un producto de análisis de malware de Amazon EC2 como falso positivo

Para iniciar el proceso, póngase en contacto con Soporte. Siga los siguientes pasos para proporcionar detalles sobre el recurso escaneado:

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Elija Análisis de malware de EC2.
3. Elija un análisis para ver su ID de resultado.
4. Proporcione el ID de resultado. También debes proporcionar el SHA-256 hash del archivo. Esto es necesario para garantizar que GuardDuty Malware Protection for EC2 haya recibido el archivo correcto.
5. El Soporte equipo le proporcionará una URL prefirmada de Amazon Simple Storage Service (Amazon S3) que podrá utilizar para cargar el archivo y el hash potencialmente maliciosos. SHA-256 Para obtener información sobre los pasos que se deben seguir para cargar el objeto analizado, consulte [Cargar objetos con URL previamente firmadas](#) en la Guía del usuario de Amazon S3.
6. Una vez que hayas subido el archivo, informa al Soporte equipo.

Soporte Proporcionarán un acuse de recibo después de recibir el archivo. Los miembros del equipo de GuardDuty servicio analizarán su envío y tomarán las medidas adecuadas para mejorar su experiencia con Malware Protection for EC2 y el GuardDuty servicio. El Soporte equipo seguirá proporcionando información actualizada sobre el estado de su caso. GuardDuty conserva su objeto S3 durante un máximo de 30 días.

# Reportar el producto del análisis de objetos de S3 como falso positivo en la protección contra malware para S3

Un análisis de protección contra malware para S3 puede identificar un objeto como potencialmente malicioso o dañino. Si cree que el objeto de S3 indicado no contiene malware, reporte este resultado de análisis de malware como falso positivo.

Puede enviar un informe de falso positivo, aunque utilice la protección contra malware para S3 de forma independiente. En este caso, no GuardDuty está diseñado para generar un hallazgo. Para obtener información sobre cómo verificar el estado del análisis y el estado del producto, consulte [Supervisión de los análisis de objetos de S3](#).

Para reportar un producto de análisis de objetos de S3 como falso positivo

Para iniciar el proceso, póngase en contacto con Soporte. Utilice los siguientes pasos para proporcionar detalles sobre el objeto de S3 analizado:

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Según el caso de uso, elija los pasos apropiados:

## Using Malware Protection for S3 with GuardDuty

1. En el panel de navegación, seleccione Resultados.
2. En la página Resultados, seleccione el resultado falso positivo para ver sus detalles.
3. Revise los detalles del resultado y proporcione el ID del resultado, la región, el nombre del bucket de S3 protegido y la clave del objeto analizado.

En los detalles Ruta del elemento, proporcione el Hash del objeto. Esto es necesario para garantizar que se GuardDuty ha recibido el archivo correcto.

## Using Malware Protection for S3 independently

Proporcione el nombre del bucket de S3 protegido, el nombre del objeto analizado y la Región de AWS.

3. El Soporte equipo le proporcionará una URL prefirmada de Amazon Simple Storage Service (Amazon S3) que podrá utilizar para cargar el archivo y el hash potencialmente maliciosos.

Para obtener información sobre los pasos que se deben seguir para cargar el objeto analizado, consulte [Cargar objetos con URL previamente firmadas](#) en la Guía del usuario de Amazon S3.

4. Tras cargar el objeto S3, informa al Soporte equipo.

Soporte Proporcionarán un acuse de recibo de la recepción del objeto. Los miembros del equipo de GuardDuty servicio analizarán su envío y tomarán las medidas adecuadas para mejorar su experiencia con Malware Protection for S3 y el GuardDuty servicio. El Soporte equipo seguirá proporcionando información actualizada sobre el estado de su caso. GuardDuty conserva su objeto S3 durante un máximo de 30 días.

## Notificación de falsos positivos en Malware Protection for Backup

Para mejorar su experiencia con GuardDuty Malware Protection for Backup, puede denunciar posibles falsos positivos y falsos negativos.

Para denunciar un posible falso positivo o falso negativo identificado en Malware Protection for Backup

Para iniciar el proceso, póngase en contacto con Soporte. Siga los siguientes pasos para proporcionar detalles sobre el recurso escaneado:

1. Inicie sesión en Consola de administración de AWS y abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. Elija Análisis de malware.
3. Elija un análisis para ver su ID de resultado.
4. Proporcione el ID de resultado. También debes proporcionar el SHA-256 hash del archivo. Esto es necesario para garantizar que se GuardDuty ha recibido el archivo correcto. Indique también la región desde la que proporcionará la muestra.
5. El Soporte equipo le proporcionará una URL prefirmada de Amazon Simple Storage Service (Amazon S3) que utilizará para cargar el archivo y el hash potencialmente maliciosos. SHA-256 Para obtener información sobre los pasos para cargar el recurso escaneado, consulte [Carga de objetos con URL prefirmadas](#) en la Guía del usuario de Amazon S3.
6. Una vez que haya cargado el archivo, informe al equipo. Soporte

Soporte Proporcionarán un acuse de recibo después de recibir el archivo. Los miembros del equipo de GuardDuty servicio analizarán su envío y tomarán las medidas adecuadas

para mejorar su experiencia con Malware Protection for EC2. El Soporte equipo seguirá proporcionando información actualizada sobre el estado de su caso. GuardDuty conserva su objeto S3 durante un máximo de 30 días.

# Corregir los hallazgos de GuardDuty seguridad detectados

Amazon GuardDuty genera [hallazgos](#) que indican posibles hallazgos de seguridad asociados con la detección GuardDuty de amenazas básica y los planes de protección dedicados. En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Si existen escenarios de corrección alternativos, se describirán en las descripciones de cada tipo de resultado. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [Tabla de tipos de resultados activos](#).

## Contenido

- [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#)
- [Corregir un bucket de S3 potencialmente comprometido](#)
- [Corregir un objeto de S3 potencialmente malicioso](#)
- [Corregir una instantánea de EBS potencialmente comprometida](#)
- [Corregir una AMI de EC2 potencialmente comprometida](#)
- [Corregir un punto de recuperación de EC2 potencialmente comprometido](#)
- [Corregir un punto de recuperación de S3 potencialmente comprometido](#)
- [Corregir un clúster de ECS potencialmente comprometido](#)
- [Corregir las credenciales potencialmente comprometidas AWS](#)
- [Corregir un contenedor independiente potencialmente comprometido](#)
- [Corregir los resultados de EKS Protection](#)
- [Corregir los resultados de la Supervisión en tiempo de ejecución](#)
- [Corregir una base de datos potencialmente comprometida](#)
- [Corregir una función de Lambda potencialmente comprometida](#)

## Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida

Cuando GuardDuty genere [tipos de búsqueda que indiquen recursos de Amazon EC2 potencialmente comprometidos](#), su recurso será Instance. Los posibles tipos de resultados podrían ser [Tipos de resultados de EC2](#), [GuardDuty Tipos de búsqueda de Runtime Monitoring](#) o [Tipos de](#)

[resultados de la protección contra malware para EC2](#). Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de utilizar [Reglas de supresión](#).

Siga los siguientes pasos para corregir la instancia de Amazon EC2 potencialmente comprometida:

### 1. Identifique la instancia de Amazon EC2 potencialmente comprometida

Examine la instancia posiblemente comprometida en busca de malware y elimínelo. Puede utilizar [On-demand escanea el malware GuardDuty](#) para identificar el malware en la instancia de EC2 potencialmente afectada o comprobar [AWS Marketplace](#) para ver si hay productos asociados útiles para identificar y eliminar el malware.

### 2. Aísle la instancia de Amazon EC2 potencialmente comprometida

Si es posible, siga los siguientes pasos para aislar la instancia potencialmente comprometida:

1. Cree un grupo de seguridad de aislamiento dedicado. Un grupo de seguridad de aislamiento solo debe tener acceso entrante y saliente desde direcciones IP específicas. Asegúrese de que no hay ninguna regla de entrada o salida que permita el tráfico para 0.0.0.0/0 (0-65535).
2. Asocie el grupo de seguridad de aislamiento a esta instancia.
3. Elimine todas las asociaciones de grupos de seguridad distintas del grupo de seguridad de aislamiento recién creado de la instancia potencialmente comprometida.

#### Note

Las conexiones rastreadas existentes no se terminarán como resultado del cambio de grupo de seguridad. Únicamente el tráfico futuro será bloqueado de forma efectiva por el nuevo grupo de seguridad.

Para obtener información sobre cómo bloquear más tráfico procedente de conexiones existentes sospechosas, consulte [Aplicar las NACL en función de la red loCs para evitar más tráfico](#) en el manual de respuesta a incidentes.

### 3. Identifique el origen de la actividad sospechosa

Si se detecta malware, con base en el tipo de resultado de su cuenta, identifique y detenga la actividad potencialmente no autorizada en su instancia de EC2. Esto puede requerir acciones como cerrar cualquier puerto abierto, cambiar las políticas de acceso y actualizar las aplicaciones para corregir las vulnerabilidades.



Si no puede identificar y detener la actividad no autorizada en la instancia de EC2 potencialmente comprometida, recomendamos que termine la instancia de EC2 comprometida y la sustituya por una nueva instancia según sea necesario. A continuación se enumeran recursos adicionales para proteger instancias EC2:

- Secciones “Seguridad” y “Redes” en [Prácticas recomendadas de Amazon EC2](#)
- [Grupos de seguridad de Amazon EC2 para instancias de Linux](#)
- [Seguridad en Amazon EC2](#)
- [Sugerencias para proteger la instancia EC2 \(Linux\)](#).
- [AWS prácticas recomendadas de seguridad](#)
- [AWS Guía técnica de respuesta a incidentes de seguridad](#).

#### 4. Examinar AWS re:Post

Vaya a [AWS re:Post](#) para obtener más ayuda.

#### 5. Envíe una solicitud de asistencia técnica

Si es suscriptor de un paquete Premium Support, puede enviar una solicitud de [asistencia técnica](#).

## Corregir un bucket de S3 potencialmente comprometido

Cuando se GuardDuty genera [GuardDuty Tipos de búsqueda de protección S3](#), indica que sus buckets de Amazon S3 se han visto comprometidos. Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de crear [Reglas de supresión](#). Si no se esperaba este comportamiento, siga estos pasos recomendados para corregir un bucket de Amazon S3 de su AWS entorno que pueda estar en peligro:

#### 1. Identifique el recurso de S3 potencialmente comprometido.

Si se GuardDuty busca S3, se mostrará el bucket de S3 asociado, su nombre de recurso de Amazon (ARN) y su propietario en los detalles de búsqueda.

#### 2. Identifique el origen de la actividad sospechosa y la llamada a la API que se utilizó.

La llamada a la API utilizada se mostrará como API en los detalles de resultado. El origen será una entidad principal de IAM (ya sea un rol de IAM, un usuario o una cuenta) y los detalles de identificación figurarán en el resultado. Según el tipo de origen, estará disponible la dirección IP remota o la información del dominio de origen, lo que puede ayudarle a evaluar si el origen fue

autorizado. Si el resultado implica credenciales de una instancia de Amazon EC2, también se incluirán los detalles de ese recurso.

3. Determine si el origen de la llamada tenía autorización para acceder al recurso identificado.

Por ejemplo, considere lo siguiente:

- Si un usuario de IAM estuvo involucrado, ¿es posible que sus credenciales hayan sido potencialmente comprometidas? Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).
- Si se ha invocado una API desde una entidad principal que no tiene antecedentes de haber invocado este tipo de API, ¿este origen necesita permisos de acceso para esta operación? ¿Se pueden restringir aún más los permisos del bucket?
- Si el acceso se vio desde nombre de usuario ANONYMOUS\_PRINCIPAL con el tipo de usuario de la AWSAccount, esto indica que el bucket es público y se ha accedido a él. ¿Este bucket debería ser público? Si no es así, consulte las siguientes recomendaciones de seguridad para encontrar soluciones alternativas al uso compartido de los recursos de S3.
- Si el acceso se hizo mediante una llamada a PreflightRequest correcta desde el nombre de usuario ANONYMOUS\_PRINCIPAL y el tipo de usuario de la AWSAccount, esto indica que el bucket tiene una política de intercambio de recursos entre orígenes (CORS) establecida. ¿Este bucket debería tener una política CORS? Si no es así, asegúrese de que el bucket no sea inadvertidamente público y revise las recomendaciones de seguridad que aparecen a continuación en busca de soluciones alternativas al uso compartido de los recursos de S3. Para más información sobre CORS, consulte [Uso compartido de recursos entre orígenes \(CORS\)](#) en la Guía del usuario de S3.

4. Determine si el bucket de S3 contiene información confidencial.

Utilice [Amazon Macie](#) para determinar si el bucket de S3 contiene información confidencial, como información de identificación personal (PII), datos financieros o credenciales. Si la detección automática de información confidencial está habilitada para su cuenta de Macie, revise los detalles del bucket de S3 para comprender mejor su contenido. Si esta característica está deshabilitada en su cuenta de Macie, se recomienda que la active para agilizar la evaluación. Como alternativa, puede crear y ejecutar un trabajo de detección de información confidencial para inspeccionar los objetos del bucket de S3 en busca de datos confidenciales. Para más información, consulte [Discovering sensitive data with Macie](#).

Si se autorizó el acceso, puede ignorar el resultado. La <https://console.aws.amazon.com/guardduty/> consola le permite configurar reglas para suprimir por completo los hallazgos individuales

para que dejen de aparecer. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Si determina que los datos de S3 han sido expuestos o que un tercero no autorizado ha accedido a estos, revise las siguientes recomendaciones de seguridad de S3 para reforzar los permisos y restringir el acceso. Las soluciones de corrección adecuadas dependerán de las necesidades de su entorno específico.

## Recomendaciones basadas en las necesidades específicas de acceso al bucket de S3

La siguiente lista ofrece recomendaciones basadas en las necesidades específicas de acceso a los buckets de Amazon S3:

- Para disponer de una forma centralizada de limitar el acceso público a los datos de S3, utilice el bloqueo de acceso público de S3. La configuración de bloqueo del acceso público se puede habilitar para los puntos de acceso, los depósitos y AWS las cuentas mediante cuatro configuraciones diferentes para controlar la granularidad del acceso. Para obtener más información, consulte [Configuración de Block Public Access](#) en la Guía del usuario de Amazon S3.
- AWS Las políticas de acceso se pueden usar para controlar cómo los usuarios de IAM pueden acceder a sus recursos o cómo pueden acceder a sus depósitos. Para obtener más información, consulte [Uso de políticas de bucket y de suario](#) en la Guía del usuario de Amazon S3.

Además, puede utilizar puntos de conexión de la nube privada virtual (VPC) con políticas de bucket de S3 para restringir el acceso a puntos de conexión de VPC específicos. Para obtener más información, consulte [Control del acceso desde puntos de enlace de la VPC con políticas de bucket](#) en la Guía del usuario de Amazon S3.

- Para permitir temporalmente el acceso a sus objetos de S3 a entidades de confianza ajenas a su cuenta, puede crear una URL prefirmada a través de S3. Este acceso se crea con las credenciales de su cuenta y, según las credenciales utilizadas, puede durar de 6 horas a 7 días. Para obtener más información, consulte [Uso de URL prefirmadas para descarga y carga de objetos](#) en la Guía para usuarios de Amazon S3.
- Para los casos de uso que requieren el uso compartido de objetos de S3 entre distintos orígenes, puede utilizar los puntos de acceso de S3 para crear conjuntos de permisos que restrinjan el acceso únicamente a los que están dentro de su red privada. Para obtener más información, consulte [Administración del acceso a conjuntos de datos con puntos de acceso](#) en la Guía del usuario de Amazon S3.

- Para conceder acceso seguro a sus recursos de S3 a otras AWS cuentas, puede utilizar una lista de control de acceso (ACL). Para obtener más información, consulte la [descripción general de la lista de control de acceso \(ACL\)](#) en la Guía del usuario de Amazon S3.

Para obtener más información sobre las opciones de seguridad de S3, consulte [Prácticas recomendadas de seguridad para Amazon S3](#), en la Guía del usuario de Amazon S3.

## Corregir un objeto de S3 potencialmente malicioso

Cuando se GuardDuty genera [Tipo de resultado de la protección contra malware para S3](#), indica que un objeto recién cargado en su bucket de Amazon S3 contiene malware. El tipo de recurso es un objeto de S3.

Utilice los siguientes pasos recomendados para corregir potencialmente el resultado generado:

1. Identifique el objeto S3 potencialmente malicioso comprobando lo S3ObjectDetailsrelacionado con el hallazgo.
2. Aísle el objeto de S3 comprometido. Si habilitó el etiquetado en el momento de habilitar Malware Protection for S3 para el bucket de Amazon S3 asociado, GuardDuty debe haber asignado una etiqueta maliciosa a este objeto. Utilice el control de acceso basado en etiquetas (TBAC) para restringir el acceso a este objeto de S3. Para obtener más información, consulte [Utilizar el control de acceso basado en etiquetas \(TBAC\)](#).

Como alternativa, si ya no necesita este objeto, también puede optar por eliminarlo o trasladarlo a un bucket de S3 aislado. Para obtener información sobre las consideraciones para eliminar un objeto de S3, consulte [Eliminar objetos](#) en la Guía del usuario de Amazon S3.

## Corregir una instantánea de EBS potencialmente comprometida

Cuando GuardDuty genera un! Execution:EC2/MaliciousFile El tipo de búsqueda de instantáneas indica que se ha detectado malware en una instantánea de Amazon EBS. Realice los siguientes pasos para corregir la instantánea potencialmente comprometida:

1. Identifique la instantánea potencialmente comprometida
  1. Identifique la instantánea potencialmente comprometida. Si se busca una instantánea de EBS, se mostrará el ID de la instantánea afectada, su nombre de recurso de Amazon (ARN) y los detalles del análisis de malware asociado en los detalles de la GuardDuty búsqueda.

2. Revise los detalles del punto de recuperación mediante el siguiente comando:

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789 --recovery-point-arn "arn:aws:ec2:us-east-1::snapshot/snap-abcdef01234567890"
```

2. Restrinja el acceso a la instantánea comprometida

Revise y modifique las políticas de acceso a la bóveda de respaldo para restringir el acceso a los puntos de recuperación y suspender cualquier trabajo de restauración automática que pueda utilizar esta instantánea.

1. Revise los permisos de uso compartido actuales:

```
aws ec2 describe-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission
```

2. Eliminar el acceso a una cuenta específica:

```
aws ec2 modify-snapshot-attribute --snapshot-id snap-abcdef01234567890 --attribute createVolumePermission --operation-type remove --user-ids 111122223333
```

3. Para ver opciones de CLI adicionales, consulte la documentación de CLI [modify-snapshot-attribute](#).

3. Tome medidas correctivas

- Antes de proceder a la eliminación, asegúrese de haber identificado todas las dependencias y de disponer de las copias de seguridad adecuadas, en caso necesario.

## Corregir una AMI de EC2 potencialmente comprometida

Cuando GuardDuty genera un! Execution:EC2/MaliciousFile El tipo de búsqueda de AMI indica que se ha detectado malware en una Amazon Machine Image (AMI). Realice los siguientes pasos para corregir la AMI potencialmente comprometida:

1. Identifique la AMI potencialmente comprometida

1. Si se GuardDuty busca una AMI, se mostrará el ID de la AMI afectada, su nombre de recurso de Amazon (ARN) y los detalles del análisis de malware asociado en los detalles de la búsqueda.

## 2. Revise la imagen fuente de AMI:

```
aws ec2 describe-images --image-ids ami-021345abcdef6789
```

## 2. Restrinja el acceso a los recursos comprometidos

1. Revise y modifique las políticas de acceso al almacén de respaldo para restringir el acceso a los puntos de recuperación y suspender cualquier trabajo de restauración automática que pueda utilizar este punto de recuperación.
2. Eliminar permisos de los permisos de la AMI de origen

Primero vea los permisos existentes:

```
aws ec2 describe-image-attribute --image-id ami-abcdef01234567890 --attribute launchPermission
```

A continuación, elimine los permisos individuales:

```
aws ec2 modify-image-attribute --image-id ami-abcdef01234567890 --launch-permission '{"Remove":[{"UserId":"111122223333"}]}'
```

Para ver opciones de CLI adicionales, consulte [Compartir una AMI con cuentas específicas - Amazon Elastic Compute Cloud](#)

3. Si la fuente es una instancia EC2, consulte: Cómo [corregir una instancia de Amazon EC2 potencialmente comprometida](#).

## 3. Tome medidas correctivas

- Antes de proceder a la eliminación, asegúrese de haber identificado todas las dependencias y de disponer de las copias de seguridad adecuadas, en caso necesario.

# Corregir un punto de recuperación de EC2 potencialmente comprometido

Cuando GuardDuty genera un! Execution:EC2/MaliciousFile RecoveryPoint al encontrar el tipo, indica que se ha detectado malware en un recurso de EC2 Recovery Point Backup. Realice los siguientes pasos para corregir el punto de recuperación potencialmente comprometido:

## 1. Identifique el punto de recuperación de EC2 potencialmente comprometido

1. Si busca EC2 Recovery Point, aparecerá su nombre de recurso de Amazon (ARN) y los detalles del análisis de malware asociado en los detalles del GuardDuty hallazgo:

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789
--recovery-point-arn "arn:aws:backup:us-east-1:111122223333:recovery-
point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

2. Revise los detalles de recuperación para buscar la imagen original:

```
aws backup get-recovery-point-restore-metadata --backup-vault-
name 021345abcdef6789 --recovery-point-arn "arn:aws:backup:us-
east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

## 2. Restrinja el acceso a los recursos comprometidos

- Revise y modifique las políticas de acceso al almacén de respaldo para restringir el acceso a los puntos de recuperación y suspender cualquier trabajo de restauración automática que pueda utilizar este punto de recuperación. Si su entorno utiliza el etiquetado de recursos, etiquete el punto de recuperación de forma adecuada para indicar que se está investigando y, si es necesario, considere la posibilidad de pausar las copias de seguridad programadas.

Ejemplo:

```
aws backup tag-resource --resource-arn arn:aws:backup:us-
east-1:111122223333:recovery-point:a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --tags Investigation=Malware,DoNotDelete=True
```

## 3. Tome medidas correctivas

- Antes de proceder a la eliminación, asegúrese de haber identificado todas las dependencias y de disponer de las copias de seguridad adecuadas, en caso necesario.

# Corregir un punto de recuperación de S3 potencialmente comprometido

Cuando GuardDuty genera un! Execution:S3/MaliciousFile RecoveryPoint al encontrar el tipo, indica que se ha detectado malware en un recurso de S3 Recovery Point Backup. Realice los siguientes pasos para corregir el punto de recuperación potencialmente comprometido:

## 1. Identifique el punto de recuperación S3 potencialmente comprometido

1. GuardDuty Al buscar puntos de recuperación de S3, se mostrará el ARN del punto de recuperación afectado, el nombre del almacén de respaldo y los detalles del análisis de malware asociado en los detalles de búsqueda.
2. Revisa los detalles del punto de recuperación:

```
aws backup describe-recovery-point --backup-vault-name 021345abcdef6789  
--recovery-point-arn arn:aws:backup:us-east-1:123456789012:recovery-  
point:abcdef01234567890
```

## 2. Restrinja el acceso a los recursos comprometidos

- Revise y modifique las políticas de acceso al almacén de respaldo para restringir el acceso a los puntos de recuperación y suspender cualquier trabajo de restauración automática que pueda utilizar este punto de recuperación. Si su entorno utiliza el etiquetado de recursos, etiquete el punto de recuperación de forma adecuada para indicar que se está investigando y, si es necesario, considere la posibilidad de pausar las copias de seguridad programadas.

Ejemplo:

```
aws backup tag-resource --resource-arn arn:aws:backup:us-  
east-1:111122223333:recovery-point:abcdef01234567890 --  
tags Investigation=Malware,DoNotDelete=True
```

Para obtener más información, consulte: Referencia de [comandos CLI de tag-resource](#)

## 3. Tome medidas correctivas

- Antes de proceder a la eliminación, asegúrese de haber identificado todas las dependencias y de disponer de las copias de seguridad adecuadas, en caso necesario.

# Corregir un clúster de ECS potencialmente comprometido

El hallazgo de un clúster de ECS potencialmente comprometido indica que se ha detectado actividad sospechosa o maliciosa en su entorno de Amazon ECS. Esto podría incluir el acceso no autorizado, la ejecución de malware u otro comportamiento malicioso que ponga en riesgo las cargas de trabajo de sus contenedores.

Siga estos pasos para corregir un clúster de Amazon ECS que pueda estar en peligro:



1. Identifique el clúster de ECS potencialmente comprometido y la amenaza detectada (hallazgos)

Los detalles del clúster de ECS afectado se muestran en el panel de detalles de GuardDuty búsqueda.

2. Evalúe la fuente de threat/malware

Compruebe si hay malware en las imágenes del contenedor. Si se detecta malware, revise la imagen del contenedor que se está utilizando. Se utiliza [ListTasks](#) para identificar todas las demás tareas en ejecución que utilizan la misma imagen potencialmente comprometida.

3. Aísle las tareas afectadas

Detenga la amenaza bloqueando todo el tráfico de red (tanto entrante como saliente) dirigido a las tareas afectadas. Este aislamiento de la red ayuda a prevenir cualquier ataque continuo al cortar todas las conexiones a la tarea comprometida.

Nota: Si determina que este hallazgo se debe a expected/legitimate la actividad de su entorno, puede configurar una regla de supresión para evitar que se produzcan hallazgos similares. Para obtener información adicional, consulta [Reglas de supresión en GuardDuty](#).

## Corregir las credenciales potencialmente comprometidas AWS

Cuando se GuardDuty genera [Tipos de resultados de IAM](#), indica que sus AWS credenciales se han visto comprometidas. El tipo de recurso potencialmente comprometido es AccessKey.

Para corregir las credenciales potencialmente comprometidas de su AWS entorno, lleve a cabo los siguientes pasos:

1. Identifique la entidad de IAM potencialmente comprometida y la llamada a la API utilizada.

La llamada a la API utilizada se mostrará como API en los detalles de resultado. La entidad de IAM (ya sea un usuario o rol de IAM) y su información de identificación se enumerarán en la sección Recurso de los detalles del resultado. El tipo de entidad de IAM implicada puede determinarse mediante el campo Tipo de usuario, el nombre de la entidad de IAM estará en el campo Nombre de usuario. El tipo de entidad de IAM implicada en el resultado también puede determinarse mediante el ID de clave de acceso utilizado.

Para las claves que empiecen con AKIA:

Este tipo de clave es una credencial administrada por el cliente a largo plazo asociada con un usuario de IAM o Usuario raíz de la cuenta de AWS. Para obtener información sobre la administración de claves de acceso para usuarios de IAM, consulte [Administración de las claves de acceso de los usuarios de IAM](#).

Para las claves que empiecen con ASIA:

Este tipo de clave es una credencial temporal a corto plazo generada por AWS Security Token Service. Estas claves solo existen durante un período breve y no se pueden ver ni administrar en la consola AWS de administración. Los roles de IAM siempre utilizarán AWS STS credenciales, pero también se pueden generar para los usuarios de IAM. Para obtener más información, AWS STS consulte [IAM: credenciales de seguridad temporales](#).

Si se utilizó un rol, el campo Nombre de usuario indicará el nombre del rol utilizado. Para determinar cómo se solicitó la clave, AWS CloudTrail examine el `sessionIssuer` elemento de la entrada del CloudTrail registro. Para obtener más información, consulte [IAM](#) e información en. AWS STS CloudTrail

## 2. Revise los permisos de la entidad de IAM.

Abra la consola de IAM. Según el tipo de entidad utilizada, seleccione la pestaña Usuarios o Roles, y localice la entidad afectada. Para ello, escriba el nombre identificado en el campo de búsqueda. Utilice las pestañas Permisos y Acceso a Advisor para revisar los permisos efectivos para esa entidad.

## 3. Determine si las credenciales de entidad de IAM se utilizaron legítimamente.

Póngase en contacto con el usuario de las credenciales para determinar si la actividad fue intencionada.

Por ejemplo, averigüe si el usuario hizo lo siguiente:

- Invocó la operación de API que figuraba en el hallazgo GuardDuty
- Invocó la operación de la API en el momento que se muestra en el resultado de GuardDuty
- Invocó la operación de la API desde la dirección IP que se muestra en el resultado de GuardDuty

Si esta actividad es un uso legítimo de las AWS credenciales, puede ignorar la GuardDuty conclusión. La <https://console.aws.amazon.com/guardduty/> consola le permite configurar reglas

para suprimir por completo los hallazgos individuales y evitar que aparezcan. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

Si no puede confirmar si esta actividad constituye un uso legítimo, podría ser consecuencia de que la clave de acceso concreta, las credenciales de inicio de sesión del usuario de IAM o, posiblemente, toda la Cuenta de AWS, se encuentren comprometidas. Si sospecha que sus credenciales se han visto comprometidas, consulte la información de [My Cuenta de AWS may be compromised](#) para solucionar este problema.

## Corregir un contenedor independiente potencialmente comprometido

Cuando se GuardDuty generen [tipos de búsqueda que indiquen un contenedor potencialmente comprometido](#), su tipo de recurso será Contenedor. Si el comportamiento que causó el resultado era el previsto en el entorno, considere la posibilidad de utilizar [Reglas de supresión](#).

Para corregir las credenciales potencialmente comprometidas de su AWS entorno, lleve a cabo los siguientes pasos:

### 1. Aísle el contenedor potencialmente comprometido

Los siguientes pasos ayudarán a identificar la carga de trabajo del contenedor potencialmente malicioso:

- Abra la GuardDuty consola en. <https://console.aws.amazon.com/guardduty/>
- En la página Resultados, seleccione el resultado correspondiente para ver el panel de resultados.
- En el panel de resultados, en la sección Recurso afectado, puede ver el ID y el Nombre del contenedor.

Aísle este contenedor de otras cargas de trabajo de contenedores.

### 2. Pause el contenedor

Suspenda todos los procesos de su contenedor.

Para obtener información sobre cómo congelar el contenedor, consulte [Pausar un contenedor](#).

Detener el contenedor.

Si el paso anterior no funciona y el contenedor no se detiene, pare el funcionamiento del contenedor. Si ha activado la [Retención de instantáneas](#) función, GuardDuty conservará las instantáneas de los volúmenes de EBS que contengan software malicioso.

Para obtener información sobre cómo detener el contenedor, consulte [Detener un contenedor](#).

### 3. Evalúe la presencia de malware

Evalúe si el malware estaba en la imagen del contenedor.

Si se autorizó el acceso, puede ignorar el resultado. La <https://console.aws.amazon.com/guardduty/> consola le permite configurar reglas para suprimir por completo los hallazgos individuales y evitar que aparezcan. La GuardDuty consola te permite configurar reglas para suprimir por completo los hallazgos individuales y evitar que aparezcan. Para obtener más información, consulte [Reglas de supresión en GuardDuty](#).

## Corregir los resultados de EKS Protection

Amazon GuardDuty genera [resultados](#) que indican posibles problemas de seguridad de Kubernetes cuando la protección EKS está habilitada para tu cuenta. Para obtener más información, consulte [EKS Protection](#). En las siguientes secciones, se describen los pasos de corrección recomendados para estos escenarios. Las acciones de corrección específicas se describen en la entrada de ese tipo de resultado en concreto. Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [Tabla de tipos de resultados activos](#).

Si alguno de los tipos de resultados de EKS Protection se generó de forma expectante, puede considerar la posibilidad de agregar [Reglas de supresión en GuardDuty](#) para evitar futuras alertas.

Los distintos tipos de ataques y problemas de configuración pueden provocar que GuardDuty EKS Protection se detecte. Esta guía le ayuda a identificar las causas fundamentales de GuardDuty los hallazgos relacionados con su clúster y describe las pautas de corrección adecuadas. Las siguientes son las principales causas que conducen a los hallazgos de GuardDuty Kubernetes:

- [Posibles problemas de configuración](#)
- [Corregir usuarios de Kubernetes potencialmente comprometidos](#)
- [Corregir pods de Kubernetes potencialmente comprometidos](#)
- [Corregir nodos de Kubernetes potencialmente comprometidos](#)

- [Corregir imágenes de contenedores potencialmente comprometidas](#)

#### Note

Antes de la versión 1.14 de Kubernetes, el `system:unauthenticated` grupo estaba asociado a y de forma predeterminada. `system:discovery` `system:basic-user` ClusterRoles. Esto puede permitir el acceso no deseado de usuarios anónimos. Las actualizaciones del clúster no revocan estos permisos, lo que significa que, incluso si ha actualizado el clúster a la versión 1.14 o posterior, es posible que estos permisos sigan vigentes. Se recomienda que desasocie estos permisos del grupo `system:unauthenticated`.

Para obtener más información sobre la eliminación de estos permisos, consulte [Clústeres de Amazon EKS seguros con prácticas recomendadas](#) en la Guía del usuario de Amazon EKS.

## Posibles problemas de configuración

Si un resultado indica un problema de configuración, consulte la sección de corrección de ese resultado para obtener directrices sobre cómo resolver ese problema concreto. Para obtener más información, consulte los siguientes tipos de resultados que indican problemas de configuración:

- [Policy:Kubernetes/AnonymousAccessGranted](#)
- [Policy:Kubernetes/ExposedDashboard](#)
- [Policy:Kubernetes/AdminAccessToDefaultServiceAccount](#)
- [Policy:Kubernetes/KubeflowDashboardExposed](#)
- Cualquier hallazgo que termine en `SuccessfulAnonymousAccess`

## Corregir usuarios de Kubernetes potencialmente comprometidos

Un GuardDuty hallazgo puede indicar que un usuario de Kubernetes está en peligro cuando un usuario identificado en el hallazgo ha realizado una acción inesperada en la API. Puede identificar el usuario en la sección Detalles del usuario de Kubernetes de los detalles de un resultado en la consola o en `resource.kubernetesDetails.kubernetesUserDetails` del JSON de resultados. Estos detalles del usuario incluyen `user name`, `uid` y los grupos de Kubernetes a los que pertenece el usuario.

Si el usuario accedía a la carga de trabajo mediante una entidad de IAM, puede utilizar la sección `Access Key details` para identificar los detalles de un usuario o rol de IAM. Consulte los siguientes tipos de usuarios y sus directrices de corrección.

 Note

Puede utilizar Amazon Detective para investigar más el rol de IAM o el usuario identificado en el resultado. Mientras ves los detalles de la búsqueda en la GuardDuty consola, selecciona Investigar en Detective. A continuación, seleccione el AWS usuario o el rol de los elementos de la lista para investigarlo en Detective.

**Built-in Administrador de Kubernetes:** el usuario predeterminado asignado por Amazon EKS a la identidad de IAM que creó el clúster. Este tipo de usuario se identifica mediante el nombre de usuario `kubernetes-admin`.

Revocación del acceso de un administrador de Kubernetes integrado:

- Identifique el valor de `userType` en la sección `Access Key details`.
  - Si `userType` es Rol y el rol pertenece a un rol de instancia de EC2:
    - Identifique esa instancia y, a continuación, siga las instrucciones que se indican en [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).
  - Si `userType` es Usuario o es un rol que ha asumido un usuario:
    1. [Rote la clave de acceso](#) de ese usuario.
    2. Rote los secretos a los que haya accedido el usuario.
    3. Revise la información de [My Cuenta de AWS may be compromised para obtener más información](#).

**Usuario autenticado de OIDC:** usuario al que se ha concedido acceso a través de un proveedor de OIDC. Normalmente, un usuario de OIDC tiene una dirección de correo electrónico como nombre de usuario. Puede comprobar si el clúster usa OIDC con el siguiente comando: `aws eks list-identity-provider-configs --cluster-name your-cluster-name`

Revocación del acceso de un usuario autenticado de OIDC:

1. Rote las credenciales de ese usuario en el proveedor de OIDC.

2. Rote los secretos a los que haya accedido el usuario.

AWS Usuario ConfigMap definido por -Auth: usuario de IAM al que se le concedió acceso mediante una -auth. AWS ConfigMap Para obtener más información, consulte [Administración de usuarios o roles de IAM para su clúster](#) en la Guía del usuario de Amazon EKS. Puede revisar sus permisos con el siguiente comando: `kubectl edit configmaps aws-auth --namespace kube-system`

Para revocar el acceso de un usuario: AWS ConfigMap

1. Utilice el siguiente comando para abrir el ConfigMap.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifique la entrada de rol o usuario en la sección MapRoles o MapUsers con el mismo nombre de usuario que aparece en la sección de detalles de usuario de Kubernetes que encontró. GuardDuty Consulte el siguiente ejemplo, en el que se ha identificado al usuario administrador en un resultado.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
      standard-wo-NodeInstanceRole-1WP3NUE306UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Elimine ese usuario de. ConfigMap Consulte el siguiente ejemplo, en el que se ha eliminado el usuario administrador.

```
apiVersion: v1
data:
  mapRoles: |
```

```
- rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE306UCF
  username: system:node:{{EC2PrivateDNSName}}
  groups:
    - system:bootstrappers
    - system:nodes
mapUsers: |
- userarn: arn:aws:iam::111122223333:user/ops-user
  username: ops-user
  groups:
    - system:masters
```

4. Si userType es Usuario o es un rol que ha asumido un usuario:
  - a. [Rote la clave de acceso](#) de ese usuario.
  - b. Rote los secretos a los que haya accedido el usuario.
  - c. Revise la información de [Mi AWS cuenta puede estar comprometida](#) para obtener más detalles.

Si el resultado no tiene una sección `resource.accessKeyDetails`, el usuario es una cuenta de servicio de Kubernetes.

Cuenta de servicio: la cuenta de servicio proporciona una identidad para los pods y se puede identificar mediante un nombre de usuario con el siguiente formato:  
`system:serviceaccount:namespace:service_account_name`.

Para revocar el acceso a una cuenta de servicio:

1. Cambie las credenciales de la cuenta de servicio.
2. Consulte las directrices sobre el peligro de los pods en la siguiente sección.

## Corregir pods de Kubernetes potencialmente comprometidos

Si se GuardDuty especifican los detalles de un pod o recurso de carga de trabajo en la `resource.kubernetesDetails.kubernetesWorkloadDetails` sección, ese pod o recurso de carga de trabajo puede estar en peligro. Un GuardDuty hallazgo puede indicar que un solo pod se ha visto comprometido o que varios pods se han visto comprometidos a través de un recurso de nivel superior. Consulte los siguientes escenarios de peligro para obtener directrices sobre cómo identificar el pod o los pods que se han puesto en peligro.



## Pods individuales en peligro

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` es `Pods`, el resultado identifica un solo pod. El campo `name` es el nombre de los pods y el campo `namespace` es su espacio de nombres.

Para obtener información sobre la identificación del nodo de trabajo que ejecuta los pods, consulte [Identifique el pod y el nodo de trabajo infractores](#) en la Guía de prácticas recomendadas de Amazon EKS.

## Pods en peligro a través de un recurso de carga de trabajo

Si el campo `type` de la sección `resource.kubernetesDetails.kubernetesWorkloadDetails` identifica un recurso de carga de trabajo, como `Deployment`, es probable que todos los pods de ese recurso de carga de trabajo estén en peligro.

Para obtener información sobre cómo identificar todos los pods del recurso de carga de trabajo y los nodos en los que se ejecutan, consulte [Identifique los pods y los nodos de trabajo infractores utilizando el nombre de la carga de trabajo](#) en la Guía de prácticas recomendadas de Amazon EKS.

## Pods en peligro a través de una cuenta de servicio

Si un GuardDuty hallazgo identifica una cuenta de servicio en la sección `resource.kubernetesDetails.kubernetesUserDetails`, es probable que los pods que utilizan la cuenta de servicio identificada estén comprometidos. El nombre de usuario indicado en un resultado es una cuenta de servicio si tiene el siguiente formato: `system:serviceaccount:namespace:service_account_name`.

Para obtener información sobre la identificación de todos los pods que utilizan la cuenta de servicio y los nodos en los que se ejecutan, consulte [Identifique los pods y los nodos de trabajo infractores mediante el nombre de la cuenta de servicio](#) en la Guía de prácticas recomendadas de Amazon EKS.

Una vez que haya identificado todos los pods comprometidos y los nodos en los que se ejecutan, consulte [Aísle el pod creando una política de red que deniegue todo el tráfico de entrada y salida al pod](#) en la Guía de prácticas recomendadas de Amazon EKS.

Para corregir un pod potencialmente comprometido:

1. Identifique la vulnerabilidad que puso en peligro a los pods.
2. Implemente la corrección para esa vulnerabilidad e inicie nuevos pods de reemplazo.
3. Elimine los pods vulnerables.

Para obtener más información, consulte [Vuelva a implementar el pod o el recurso de carga de trabajo comprometido](#) en la Guía de prácticas recomendadas de Amazon EKS.

Si al nodo trabajador se le ha asignado una función de IAM que permita a los Pods acceder a otros AWS recursos, elimina esas funciones de la instancia para evitar que el ataque cause más daños. Del mismo modo, si al pod se le ha asignado un rol de IAM, evalúe si puede eliminar de forma segura las políticas de IAM del rol sin que ello afecte a otras cargas de trabajo.

## Corregir imágenes de contenedores potencialmente comprometidas

Cuando un GuardDuty hallazgo indica que un módulo está en peligro, la imagen utilizada para lanzarlo podría ser maliciosa o estar comprometida.

GuardDuty los hallazgos identifican la imagen del contenedor en el `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Para determinar si la imagen es malintencionada, analícela en busca de malware.

Para corregir una imagen de contenedor potencialmente comprometida:

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todos los pods que utilizan la imagen potencialmente comprometida.

Para obtener más información, consulte [Identificar los pods con imágenes y nodos de trabajo vulnerables o comprometidos](#) en la Guía de prácticas recomendadas de Amazon EKS.

3. Aísle los pods potencialmente comprometidos, rote las credenciales y recopile datos para su análisis. Para obtener más información, consulte [Aislar el pod mediante la creación de una política de red que deniegue todo el tráfico de entrada y salida al pod en la Guía](#) de prácticas recomendadas de Amazon EKS.
4. Elimine todos los pods que utilicen la imagen potencialmente comprometida.

## Corregir nodos de Kubernetes potencialmente comprometidos

Un GuardDuty hallazgo puede indicar que un nodo está en peligro si el usuario identificado en el hallazgo representa la identidad de un nodo o si el hallazgo indica el uso de un contenedor privilegiado.

La identidad del usuario es un nodo de trabajo si el campo `username` tiene el siguiente formato: `system:node:node name`. Por ejemplo, `system:node:ip-192-168-3-201.ec2.internal`. Esto indica que el adversario ha obtenido acceso al nodo y está utilizando las credenciales del nodo para comunicarse con el punto de conexión de la API de Kubernetes.

Un resultado indica el uso de un contenedor privilegiado si uno o varios de los contenedores enumerados en el resultado tienen el campo de resultado `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext` establecido en `True`.

Para corregir un nodo potencialmente comprometido:

1. Aísle el pod, rote sus credenciales y recopile datos para el análisis forense.

Para obtener más información, consulte [Aislar el pod mediante la creación de una política de red que deniegue todo el tráfico de entrada y salida al pod en la Guía](#) de prácticas recomendadas de Amazon EKS.

2. Identifique las cuentas de servicio utilizadas por todos los pods que se ejecutan en el nodo potencialmente comprometido. Revise sus permisos y rote las cuentas de servicio si es necesario.
3. Termine el nodo potencialmente comprometido.

## Corregir los resultados de la Supervisión en tiempo de ejecución

Cuando habilitas Runtime Monitoring para tu cuenta, Amazon GuardDuty puede generar datos [GuardDuty Tipos de búsqueda de Runtime Monitoring](#) que indiquen posibles problemas de seguridad en tu AWS entorno. Los posibles problemas de seguridad indican una instancia de Amazon EC2, una carga de trabajo de contenedor, un clúster de Amazon EKS o un conjunto de credenciales comprometidas en su AWS entorno. El agente de seguridad supervisa los eventos en tiempo de ejecución de varios tipos de recursos. Para identificar el recurso potencialmente comprometido, consulte el tipo de recurso en los detalles de búsqueda generados en la GuardDuty consola. En la siguiente sección se describen los pasos de corrección recomendados para cada tipo de recurso.

## Instance

Si el tipo de recurso en los detalles del resultado es Instancia, indica que una instancia de EC2 o un nodo de EKS están potencialmente en peligro.

- Para corregir un nodo de EKS en peligro, consulte [Corregir nodos de Kubernetes potencialmente comprometidos](#).
- Para corregir una instancia de EC2 en peligro, consulte [Corrección de problemas en una instancia de Amazon EC2 potencialmente comprometida](#).

## EKSCluster

Si el tipo de recurso en los detalles del resultado es EKSCluster, indica que un pod o un contenedor de un clúster de EKS están potencialmente en peligro.

- Para corregir un pod en peligro, consulte [Corregir pods de Kubernetes potencialmente comprometidos](#).
- Para corregir una imagen de contenedor en peligro, consulte [Corregir imágenes de contenedores potencialmente comprometidas](#).

## ECSCluster

Si el tipo de recurso en los detalles del resultado es ECSCluster, significa que una tarea de ECS o un contenedor dentro de una tarea de ECS está potencialmente comprometido.

### 1. Identifique el clúster de ECS afectado

El hallazgo GuardDuty de Runtime Monitoring proporciona los detalles del clúster de ECS en el panel de detalles del hallazgo o en la `resource.ecsClusterDetails` sección del JSON de búsqueda.

### 2. Identifique la tarea de ECS afectada

El resultado GuardDuty de Runtime Monitoring proporciona los detalles de la tarea de ECS en el panel de detalles del hallazgo o en la `resource.ecsClusterDetails.taskDetails` sección del JSON de búsqueda.

### 3. Aísle la tarea afectada

Para aislar la tarea impactada, deniegue todo el tráfico de entrada y salida a la tarea. Una regla que prohíba todo el tráfico puede ayudar a detener un ataque que ya está en marcha, ya que interrumpe todas las conexiones con la tarea.

#### 4. Corrija la tarea comprometida

- a. Identifique la vulnerabilidad que comprometió la tarea.
- b. Implemente la corrección de esa vulnerabilidad e inicie una nueva tarea de sustitución.
- c. Detenga la tarea vulnerable.

## Container

Si el tipo de recurso en los detalles del resultado es Contenedor, indica que un contenedor independiente está potencialmente en peligro.

- Para corregirlo, consulte [Corregir un contenedor independiente potencialmente comprometido](#).
- Si el resultado se genera en varios contenedores con la misma imagen de contenedor, consulte [Corregir imágenes de contenedores potencialmente comprometidas](#).
- Si el contenedor ha accedido al host de EC2 subyacente, es posible que las credenciales de la instancia asociadas se hayan puesto en peligro. Para obtener más información, consulte [Corregir las credenciales potencialmente comprometidas AWS](#).
- Si un agente potencialmente malintencionado ha accedido al nodo de EKS subyacente o a una instancia de EC2, consulte la corrección recomendada en las pestañas EKSCluster e Instancia.

## Corrección de imágenes de contenedor en peligro

Cuando un GuardDuty hallazgo indica que una tarea está en peligro, la imagen utilizada para lanzarla podría ser maliciosa o estar comprometida. GuardDuty los hallazgos identifican la imagen del contenedor en el `resource.ecsClusterDetails.taskDetails.containers.image` campo. Para determinar si la imagen es maliciosa o no, puede analizarla en busca de malware.

Para corregir una imagen de contenedor comprometida

1. Deje de usar la imagen inmediatamente y elimínela del repositorio de imágenes.
2. Identifique todas las tareas que utilizan esta imagen.
3. Detenga todas las tareas que utilizan la imagen comprometida. Actualice las definiciones de las tareas de modo que dejen de utilizar la imagen comprometida.

# Corregir una base de datos potencialmente comprometida

GuardDuty genera datos [Tipos de resultados de la protección de RDS](#) que indican un comportamiento de inicio de sesión potencialmente sospechoso y anómalo en su cuenta [Bases de datos compatibles](#) después de activarlo. [Protección de RDS](#) Mediante la actividad de inicio de sesión de RDS, GuardDuty analiza y perfila las amenazas identificando patrones inusuales en los intentos de inicio de sesión.

## Note

Para acceder a toda la información sobre un tipo de resultado, selecciónelo en la [GuardDuty tipos de búsqueda activos](#).

Siga estos pasos recomendados para corregir una base de datos de Amazon Aurora potencialmente comprometida en su AWS entorno.

## Temas

- [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos](#)
- [Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos](#)
- [Corrección de credenciales potencialmente en peligro](#)
- [Restricción del acceso a la red](#)

## Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión correctos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión correctos.

### 1. Identifique la base de datos y el usuario afectados.

El GuardDuty resultado generado proporciona el nombre de la base de datos afectada y los detalles de usuario correspondientes. Para obtener más información, consulte [Detalles de los resultados](#).

## 2. Confirme si este comportamiento es esperado o inesperado.

En la siguiente lista se especifican los posibles escenarios que pueden haber provocado GuardDuty la generación de un hallazgo:

- Un usuario que inicia sesión en su base de datos después de un largo periodo de tiempo.
- Un usuario que inicia sesión en su base de datos de forma ocasional (por ejemplo, un analista financiero que inicia sesión cada trimestre).
- Un agente potencialmente sospechoso que participa en un intento de inicio de sesión correcto podría poner en peligro la base de datos.

## 3. Comience este paso si el comportamiento es inesperado.

### 1. Restrinja el acceso a la base de datos.

Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte [Corrección de credenciales potencialmente en peligro](#) y [Restricción del acceso a la red](#).

### 2. Evalúe el impacto y determine a qué información se accedió.

- Si están disponibles, revise los registros de auditoría para identificar los datos a los que se puede haber accedido. Para obtener más información, consulte [Supervisión de eventos, registros y flujos en un clúster de bases de datos de Amazon Aurora](#) en la Guía del usuario de Amazon Aurora.
- Determine si se accedió a información confidencial o protegida o si se modificó.

## Corrección de una base de datos potencialmente en peligro con eventos de inicio de sesión fallidos

Los siguientes pasos recomendados pueden ayudarlo a corregir una base de datos de Aurora potencialmente en peligro que presenta un comportamiento atípico en relación con los eventos de inicio de sesión fallidos.

### 1. Identifique la base de datos y el usuario afectados.

El GuardDuty resultado generado proporciona el nombre de la base de datos afectada y los detalles de usuario correspondientes. Para obtener más información, consulte [Detalles de los resultados](#).

### 2. Identifique el origen de los intentos de inicio de sesión fallidos.

La GuardDuty búsqueda generada proporciona la dirección IP y la organización de la ASN (si se trata de una conexión pública) en la sección Actor del panel de búsqueda.

Un sistema autónomo (AS) es un grupo de uno o varios prefijos de IP (listas de direcciones IP accesibles en una red) administrado por uno o más operadores de red que mantienen una política de enrutamiento única y claramente definida. Los operadores de red necesitan números de sistemas autónomos (ASN) para controlar el enrutamiento en sus redes e intercambiar información de enrutamiento con otros proveedores de servicios de internet (ISP).

### 3. Confirme que este comportamiento es inesperado.

Examine si esta actividad representa un intento de obtener acceso adicional no autorizado a la base de datos de la siguiente manera:

- Si el origen es interno, compruebe si una aplicación está mal configurada y si está intentando conectarse repetidamente.
- Si se trata de un agente externo, compruebe si la base de datos correspondiente es pública o está mal configurada y, por lo tanto, permite que posibles actores malintencionados utilicen nombres de usuario comunes por fuerza bruta.

### 4. Comience este paso si el comportamiento es inesperado.

#### 1. Restrinja el acceso a la base de datos.

Restrinja el acceso a la base de datos para las cuentas sospechosas y el origen de esta actividad de inicio de sesión. Para obtener más información, consulte [Corrección de credenciales potencialmente en peligro](#) y [Restricción del acceso a la red](#).

#### 2. Analice la causa raíz y determine los pasos que podrían haber llevado a esta actividad.

Configure una alerta para recibir una notificación cuando una actividad modifique una política de red y cree un estado no seguro. Para obtener más información, consulte [Firewall policies in AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall .

## Corrección de credenciales potencialmente en peligro

Un GuardDuty hallazgo puede indicar que las credenciales de usuario de una base de datos afectada se han visto comprometidas cuando el usuario identificado en el hallazgo ha realizado una operación inesperada en la base de datos. Puede identificar el usuario en la sección Detalles del usuario de base de datos de RDS del panel de resultados de la consola o en



`resource.rdsDbUserDetails` del JSON de resultados. Estos detalles del usuario incluyen el nombre de usuario, la aplicación utilizada, la base de datos a la que se ha accedido, la versión de SSL y el método de autenticación.

- Para revocar el acceso o rotar las contraseñas de usuarios específicos que participan en el resultado, consulte [Seguridad con Amazon Aurora MySQL](#) o [Seguridad con Amazon Aurora PostgreSQL](#) en la Guía del usuario de Amazon Aurora.
- Úselo AWS Secrets Manager para almacenar de forma segura y rotar automáticamente los secretos de las bases de datos de Amazon Relational Database Service (RDS). Para obtener más información, consulte [Tutoriales de AWS Secrets Manager](#) en la Guía del usuario de AWS Secrets Manager .
- Utilice la autenticación de bases de datos de IAM para administrar el acceso de los usuarios a las bases de datos sin necesidad de contraseñas. Para obtener más información, consulte [Autenticación de bases de datos de IAM](#) en la Guía del usuario de Amazon Aurora.

Para obtener más información, consulte [Prácticas recomendadas de seguridad para Amazon Relational Database Service](#) en la Guía del usuario de Amazon RDS.

## Restricción del acceso a la red

Un GuardDuty hallazgo puede indicar que se puede acceder a una base de datos más allá de las aplicaciones o de la Nube Privada Virtual (VPC). Si la dirección IP remota del resultado es un origen de conexión inesperado, audite los grupos de seguridad. Encontrará una lista de los grupos de seguridad adjuntos a la base de datos en la sección Grupos de seguridad de la <https://console.aws.amazon.com/rds/console> o en el JSON `resource.rdsDbInstanceDetails.dbSecurityGroups` de los resultados. Para obtener más información sobre la configuración de los grupos de seguridad, consulte [Control de acceso con grupos de seguridad](#) en la Guía del usuario de Amazon RDS.

Si utiliza un firewall, restrinja el acceso a la red a la base de datos; para ello, reconfigure las listas de control de acceso a la red (NACL). Para obtener más información, consulte [Firewall in AWS Network Firewall](#) en la Guía para desarrolladores de AWS Network Firewall .

## Corregir una función de Lambda potencialmente comprometida

Cuando se GuardDuty genera [Tipos de resultados de la protección de Lambda](#), la función Lambda puede verse comprometida. Si se esperaba la actividad GuardDuty que provocó este hallazgo,

puede considerar la posibilidad de [Reglas de supresión](#) utilizarla. Recomendamos completar los siguientes pasos para corregir una función de Lambda comprometida:

### Corrección de los resultados de la protección de Lambda

1. Identifique la versión de la función Lambda potencialmente comprometida.

Una GuardDuty búsqueda de Lambda Protection proporciona el nombre, el nombre del recurso de Amazon (ARN), la versión de la función y el ID de revisión asociados a la función de Lambda que aparecen en los detalles de la búsqueda.

2. Identifique el origen de la actividad potencialmente sospechosa.

- a. Revise el código asociado a la versión de la función de Lambda implicada en el resultado.
- b. Revise las bibliotecas y capas importadas de la versión de la función de Lambda implicada en el resultado.
- c. Si ha activado [AWS Lambda las funciones de digitalización en Amazon Inspector](#), revise las [conclusiones de Amazon Inspector](#) asociadas a la función Lambda implicada en la búsqueda.
- d. Revise los AWS CloudTrail registros para identificar el factor principal que provocó la actualización de la función y asegúrese de que la actividad estaba autorizada o prevista.

3. Corrija la función de Lambda potencialmente comprometida.

- a. Deshabilite los desencadenadores de ejecución de la función de Lambda implicada en el resultado. Para obtener más información, consulte [DeleteFunctionEventInvokeConfig](#).
- b. Revise el código de Lambda y actualice las importaciones de bibliotecas y las [capas de la función de Lambda](#) para eliminar las bibliotecas y las capas potencialmente sospechosas.
- c. Mitigue los resultados de Amazon Inspector relacionados con la función de Lambda implicada en el resultado.

# Supervisión del GuardDuty uso y estimación de los costes

GuardDuty proporciona métricas de uso que rastrean el procesamiento de los planes de protección, las fuentes de datos logs/events y las vCPU supervisadas en GuardDuty tiempo de ejecución a lo largo del tiempo.

En esta página:

- [Métricas CloudWatch de uso de Amazon](#)
- [Comprensión GuardDuty del uso](#)
- [Estimación del costo GuardDuty](#)

## Métricas CloudWatch de uso de Amazon

GuardDuty publica las métricas de uso en Amazon CloudWatch, lo que te permite:

- Realiza un seguimiento del uso real a lo largo del tiempo
- Cree paneles y alarmas personalizados
- Exporte los datos de uso para estimar los costos en la calculadora AWS de precios

GuardDuty Las métricas de uso se publican en función de la configuración de tu cuenta:

- En el caso de las cuentas independientes (que no formen parte de una organización), puedes ver las estadísticas de uso de tu cuenta en Amazon CloudWatch
- En el caso de las cuentas que forman parte de una organización, las métricas se publican en la cuenta del administrador delegado (el GuardDuty administrador de la organización) y muestran el uso agregado de toda la organización

GuardDuty las métricas de uso se publican en Amazon en CloudWatch un plazo de 24 horas.

## Detalles de las métricas

GuardDuty publica las siguientes métricas Hourly de uso en Amazon CloudWatch en el espacio de AWS/GuardDuty nombres:

| Plan de protección                 | Origen de datos        | Nombre de métrica   | Unidad                | Descripción                                                          |
|------------------------------------|------------------------|---------------------|-----------------------|----------------------------------------------------------------------|
| Detección de amenazas fundamental  | CloudTrailEvents       | AnalyzedCount       | Recuento              | Número de eventos de CloudTrail gestionados analizados               |
| Detección fundamental de amenazas  | VPCFlowLogDNSLogEvents | AnalyzedBytes       | Bytes                 | Volumen de registros de flujo de VPC y registros de DNS analizados   |
| EKS Protection                     | KubernetesAuditLogs    | AnalyzedCount       | Recuento              | Número de eventos del registro de auditoría de Amazon EKS analizados |
| S3 Protection                      | S3DataEvents           | AnalyzedCount       | Recuento              | Número de eventos de datos de S3 analizados                          |
| Supervisión en tiempo de ejecución | RuntimeMonitoringEC2   | Monitored VcpuHours | Recuento (vCPU-Hours) | Horas de vCPU de EC2 monitorizadas mediante Runtime Monitoring       |
| Supervisión en tiempo de ejecución | RuntimeMonitoringEKS   | Monitored VcpuHours | Recuento (vCPU-Hours) | Horas de vCPU de Amazon EKS monitorizadas mediante                   |

|                                    |                          |                    |                       | Runtime Monitoring                                              |
|------------------------------------|--------------------------|--------------------|-----------------------|-----------------------------------------------------------------|
| Supervisión en tiempo de ejecución | RuntimeMonitoringFargate | MonitoredVcpuHours | Recuento (vCPU-Hours) | Horas de vCPU de Fargate monitoreadas por Runtime Monitoring    |
| Malware Protection for EC2         | OnDemandEBSSnapshot      | ScannedBytes       | Bytes                 | Volumen de datos de instantáneas de EBS escaneados bajo demanda |
| Malware Protection for EC2         | OnDemandEBSVolume        | ScannedBytes       | Bytes                 | Volumen de datos de volumen de EBS escaneados bajo demanda      |
| Malware Protection for EC2         | MalwareProtectionEBS     | ScannedBytes       | Bytes                 | Volumen de datos de EBS escaneados por Malware Protection       |
| Protección de RDS                  | RDS                      | MonitoredAcuHours  | Recuento () ACU-Hours | Unidades de capacidad Aurora de Amazon RDS monitorizadas        |
| Protección de RDS                  | RDS sin límites          | MonitoredAcuHours  | Recuento () ACU-Hours | Horas de ACU Amazon RDS Aurora Limitless monitorizadas          |

|                      |                    |                     |                        |                                               |
|----------------------|--------------------|---------------------|------------------------|-----------------------------------------------|
| Protección de RDS    | AuroraScaleout     | Monitored AcuHours  | Recuento () ACU-Hours  | Horas de ACU Aurora Scaleout monitoreadas     |
| Protección de RDS    | RDS                | Monitored VcpuHours | Recuento (v) CPU-Hours | Horas de vCPU de Amazon RDS monitorizadas     |
| Protección de Lambda | LambdaNet workLogs | AnalyzedBytes       | Bytes                  | Volumen de registros de red Lambda analizados |

### Dimensiones de las métricas

- GuardDuty Cuentas independientes: las métricas incluyen dimensiones `AccountId`, `DataSource`
- Organization-level (Administrador delegado): Las métricas incluyen la dimensión `DataSource`

## Protección contra malware para S3

GuardDuty Malware Protection for S3 el plan de protección publica las siguientes métricas de uso en Amazon CloudWatch en el espacio de `AWS/GuardDuty/MalwareProtection` nombres:

| Nombre de métrica  | Unidad   | Descripción                                                                                                            |
|--------------------|----------|------------------------------------------------------------------------------------------------------------------------|
| CompletedScanCount | Recuento | Cantidad de análisis de malware de objetos S3 que se completaron en un periodo determinado.                            |
| FailedScanCount    | Recuento | Cantidad de análisis de objetos de S3 maliciosos en los que se produjo un error en un intervalo de tiempo determinado. |

|                    |          |                                                                                                                                 |
|--------------------|----------|---------------------------------------------------------------------------------------------------------------------------------|
| SkippedScanCount   | Recuento | Cantidad de análisis de malware de objetos de S3 que se omitieron en un periodo determinado.                                    |
| InfectedScanCount  | Recuento | La cantidad de análisis de malware en objetos de S3 que detectaron objetos potencialmente maliciosos en un periodo determinado. |
| CompletedScanBytes | Recuento | La cantidad de bytes de objetos de S3 analizados en un período de tiempo determinado.                                           |

### Dimensiones de las métricas

- Todas las métricas incluyen Malware Protection Plan Id, Resource Name dimensiones
- SkippedScanCount la métrica Skipped Reason se incluye como dimensión adicional

## Comprensión GuardDuty del uso

### GuardDuty Procesamiento de eventos

Cuando está activado, consume GuardDuty automáticamente los eventos y los registros directamente desde las fuentes de registro seleccionadas Región de AWS. GuardDuty ingiere eventos de fuentes de datos separadas e independientes para ofrecer un valor de seguridad integral.

#### Important

La configuración del registro de servicio individual o las reglas de filtrado (para los registros de flujo de VPC, los registros de DNS, los CloudTrail eventos, los eventos de datos de S3, los registros de auditoría de Kubernetes y los registros de red Lambda) no afectan al procesamiento realizado por logs/events GuardDuty

## GuardDuty Los cargos de procesamiento de registros de flujo de VPC para las instancias monitoreadas por GuardDuty Runtime Monitoring

En el caso de las instancias supervisadas por GuardDuty Runtime Monitoring (mediante el agente EC2 Runtime o el agente Amazon EKS Runtime), no GuardDuty se cobrará por el procesamiento de los registros de flujo de VPC siempre y cuando el agente [envíe activamente los datos de los eventos de tiempo de ejecución](#). Si el agente deja de transmitir los datos del evento, GuardDuty vuelve a cargar mediante los registros de flujo de VPC.

Al habilitar Runtime Monitoring, se reduce el uso de los registros de flujo de VPC en las métricas de CloudWatch uso de GuardDuty Amazon. Al deshabilitar la supervisión del tiempo de ejecución, se restaura el uso de los registros de flujo de la VPC.

## Estimación del costo GuardDuty

GuardDuty ofrece una prueba gratuita de 30 días por AWS cuenta para la mayoría de los planes de protección. Durante este período de prueba, puede:

- Supervise su uso real a través de las métricas GuardDuty de uso
- Calcule sus costos mensuales con la calculadora AWS de precios en función de los patrones de uso observados

Los siguientes planes de protección incluyen una prueba gratuita de 30 días:

- Detección fundamental de amenazas
- S3 Protection
- EKS Protection
- Supervisión en tiempo de ejecución
- Protección de RDS
- Protección de Lambda
- Protección contra malware para EC2 (solo para GuardDuty-initiated escaneos cuando están habilitados con Foundational Threat Detection)



## Uso de la calculadora de precios AWS

Puedes usar la [calculadora de AWS precios](#) para estimar tus GuardDuty costos mensuales en función de los patrones de uso observados. Para crear una estimación de GuardDuty:

1. Abre la [calculadora AWS de precios](#).
2. Elija Crear presupuesto.
3. En la página Añadir servicio, busca Amazon GuardDuty y selecciona Configurar.
4. Selecciona la ubicación Región de AWS que GuardDuty está habilitada.
5. En la sección Configuración del servicio, introduce tu uso estimado para cada plan de protección en función de las métricas de uso observadas en Amazon CloudWatch o en la GuardDuty consola.
6. Selecciona Añadir a mi estimación para ver el coste mensual proyectado.

### Note

Algunas métricas GuardDuty de uso se muestran en bytes. Al introducir valores en la calculadora de AWS precios, es posible que tengas que convertir los bytes a la unidad adecuada (MB, GB o TB). Usa las siguientes conversiones:

- 1 MB = 1.048.576 bytes
- 1 GB = 1.073.741.824 bytes
- 1 TB = 1.099.511.627.776 bytes

## Clientes de Security Hub

Security Hub ofrece un modelo de precios simplificado para la detección de GuardDuty amenazas con su plan adicional Threat Analytics, que consolida la medición de múltiples GuardDuty DataSources Al utilizar el plan Security Hub Threat Analytics (Security Hub con GuardDuty):

- Se GuardDuty DataSources consolidan varios
- En particular, para simplificar, los eventos de Amazon EKS Audit Logs y los eventos de S3 Data se convierten a GB mediante una tasa de conversión fija.

Para crear una estimación del coste del Security Hub, consulte la [documentación del AWS Security Hub](#).

Nota: GuardDuty el estado de prueba gratuita de 30 días es independiente de la integración de Security Hub. Activación o desactivación de Security Hub:

- No otorga una nueva prueba gratuita si ya ha utilizado el período GuardDuty de prueba
- No interrumpe ni reinicia una prueba gratuita en curso
- No amplía los períodos de prueba existentes

# Nombres de funciones de los planes de protección en la GuardDuty API

Cuando habilitas Amazon GuardDuty por primera vez, comienza a procesarse [Orígenes de datos fundamentales](#) en tu AWS entorno. GuardDuty usa estas fuentes de datos para procesar un flujo independiente de eventos, como registros de flujo de VPC, registros de DNS y eventos AWS CloudTrail de administración. A continuación, analiza estos eventos para identificar posibles amenazas de seguridad y genera resultados en su cuenta.

Cuando uno o más planes de protección están habilitados, GuardDuty utiliza datos adicionales de otros AWS servicios de su AWS entorno para supervisar y analizar posibles amenazas a la seguridad. Estos orígenes de datos adicionales se denominan características.

## Cambio de orígenes de datos a características

Cuando agrega GuardDuty protecciones adicionales, como S3 Protection, Runtime Monitoring, Lambda Protection y otras, puede configurar la GuardDuty función correspondiente al plan de protección. Históricamente, en las API se utilizaban `dataSources` las denominadas GuardDuty protecciones. Sin embargo, después de marzo de 2023, los nuevos planes de GuardDuty protección ahora se configuran como `features` y `noDataSources`. GuardDuty sigue siendo compatible con la configuración de los planes de protección lanzados antes de marzo de 2023, por ejemplo, `dataSources` a través de la API, pero los nuevos planes de protección solo están disponibles a partir de `features`. Para obtener información sobre los planes de protección que se ven afectados, consulte [GuardDuty Cambios en la API](#).

Si gestiona los planes de GuardDuty configuración y protección a través de la consola, este cambio no le afectará directamente y no tendrá que tomar ninguna medida. Este cambio afecta al comportamiento de las API que se invocan para habilitar GuardDuty o proteger los planes internos GuardDuty. Si usa API o AWS CLI para habilitar o editar la configuración de un plan de protección, debe usar el nombre de la función asociada. Para obtener más información, consulte [Asignación de `dataSources` a `features`](#).

## GuardDuty Cambios en la API en marzo de 2023

Las GuardDuty API configuran funciones de protección que no pertenecen a la lista de [GuardDuty fuentes de datos fundamentales](#). Un objeto de característica contiene detalles de la característica,

como el nombre y el estado de la característica, y puede contener configuración adicional para algunos de los planes de protección. Esta migración afecta a las siguientes API de la Amazon GuardDuty API Reference:

- [CreateDetector](#)
- [GetDetector](#)
- [UpdateDetector](#)
- [GetMemberDetectors](#)
- [UpdateMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [GetRemainingFreeTrialDays](#)
- [GetUsageStatistics](#)

## Características en comparación con los orígenes de datos

Históricamente, todas las GuardDuty funciones se transferían a través de un `dataSources` objeto de la API. A partir de marzo de 2023, GuardDuty prefiere el `features` objeto en lugar del `dataSources` objeto de la API. Todos los orígenes de datos anteriores tienen las características correspondientes, pero es posible que las características más recientes no tengan los orígenes de datos correspondientes.

En la siguiente lista se muestra la comparación entre los objetos `dataSources` y `features` cuando se pasan a través de una API:

- El objeto `dataSources` contiene objetos para cada tipo de protección y su estado. El `features` objeto es una lista de funciones disponibles que corresponden a cada tipo de protección incluido GuardDuty.

A partir de marzo de 2023, la activación de las funciones será la única forma de configurar GuardDuty las nuevas funciones en su AWS entorno.

- El `dataSources` esquema de la solicitud o respuesta de la API es el mismo en todos los Región de AWS lugares GuardDuty disponibles. Sin embargo, es posible que no todas las características estén disponibles en todas las regiones. Por lo tanto, los nombres de las características disponibles pueden variar según la región.

## Comprender cómo funcionan las API con características

Las GuardDuty API seguirán devolviendo un `dataSources` objeto, según proceda, y también devolverán un `features` objeto que contenga la misma información en un formato diferente. GuardDuty las funciones lanzadas antes de marzo de 2023 estarán disponibles a través de `dataSources` object y `features` object. GuardDuty las funciones lanzadas desde marzo de 2023 solo estarán disponibles a través del `features` objeto. No puedes crear ni actualizar un detector, ni describir el AWS Organizations uso que haces de ambos `dataSources` y de la notación de `features` objetos en la misma solicitud de API. Para habilitar los tipos de GuardDuty protección, tendrás que migrar tus fuentes de datos existentes al `features` objeto mediante las mismas API que ahora también incluyen el `features` objeto.

### Note

GuardDuty no añadirá una nueva fuente de datos después de esta modificación.

GuardDuty ha dejado de utilizar las fuentes de datos asociadas a los planes de protección. Sin embargo, sigue admitiendo los [GuardDuty fuentes de datos fundamentales](#). GuardDuty Las prácticas recomendadas recomiendan usar funciones para habilitar o editar la configuración de cualquier plan de protección de su cuenta.

## Incorporar cambios de características en las API

- Si administra GuardDuty las configuraciones mediante API, SDK o CloudFormation plantillas y desea habilitar posibles GuardDuty funciones nuevas, tendrá que modificar el código y la plantilla, respectivamente. Para obtener más información, consulta las API actualizadas en la [Amazon GuardDuty API Reference](#).
- En el GuardDuty caso de las funciones configuradas antes de esta actualización, puede seguir utilizando las API, los SDK o la CloudFormation plantilla. Sin embargo, le recomendamos que cambie para usar el objeto `feature`.

Todos los orígenes de datos tienen un objeto de característica equivalente. Para obtener más información, consulte [Asignación de `dataSources` a `features`](#).

- Actualmente, `additionalConfiguration` en el objeto `features` solo está disponible para ciertos tipos de protecciones.

- Para estos tipos de protección, si la función `AdditionalConfiguration status` está configurada en `ENABLED` pero la configuración de la función no `status` está establecida en `ENABLED`, no GuardDuty se realizará ninguna acción en este caso.
- Esto afecta a las siguientes API:
  - [UpdateDetector](#)
  - [UpdateMemberDetectors](#)
  - [UpdateOrganizationConfiguration](#)

## Asignación de **dataSources** a **features**

En la siguiente tabla se muestra la asignación de los tipos de protecciones, `dataSources` y `features`.

| GuardDuty tipo de protección                                      | Nombre del origen de datos *                                          | Nombre de la característica                                    |
|-------------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------|
| <a href="#">Logs de flujo de VPC</a>                              | <code>flowLogs</code> (solo lectura; no se puede modificar)           | <code>FLOW_LOGS</code> (solo lectura; no se puede modificar)   |
| <a href="#">Registros de consultas de DNS de Route53 Resolver</a> | <code>dnsLogs</code> (solo lectura; no se puede modificar)            | <code>DNS_LOGS</code> (solo lectura; no se puede modificar)    |
| <a href="#">CloudTrail eventos</a>                                | <code>cloudTrail</code> (solo lectura; no se puede modificar)         | <code>CLOUD_TRAIL</code> (solo lectura; no se puede modificar) |
| <a href="#">S3</a>                                                | <code>s3Logs</code>                                                   | <code>S3_DATA_EVENTS</code>                                    |
| <a href="#">EKS Protection</a>                                    | <code>kubernetes.auditlogs</code>                                     | <code>EKS_AUDIT_LOGS</code>                                    |
| <a href="#">Protección contra malware para EC2</a>                | <code>malwareProtection.scanEc2InstanceWithFindings.ebsVolumes</code> | <code>EBS_MALWARE_PROTECTION</code>                            |

| GuardDuty tipo de protección                                       | Nombre del origen de datos <sup>*</sup>                                                                  | Nombre de la característica                                             |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <a href="#">Eventos de inicio de sesión de RDS</a>                 |                                                                                                          | RDS_LOGIN_EVENTS                                                        |
| Supervisión en tiempo de ejecución de EKS                          |                                                                                                          | EKS_RUNTIME_MONITORING                                                  |
| <a href="#">Supervisión en tiempo de ejecución</a>                 |                                                                                                          | RUNTIME_MONITORING                                                      |
| GuardDuty agente de seguridad para clústeres de Amazon EKS         | GuardDuty solo proporciona compatibilidad con la activación de funciones para estos tipos de protección. | EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT     |
|                                                                    |                                                                                                          | RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT         |
|                                                                    |                                                                                                          | RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT |
| GuardDuty agente de seguridad para ECS-Fargate clústeres de Amazon |                                                                                                          | RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT |

| GuardDuty tipo de protección                                | Nombre del origen de datos <sup>*</sup> | Nombre de la característica                                     |
|-------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------------------|
| GuardDuty agente de seguridad para instancias de Amazon EC2 |                                         | RUNTIME_MONITORING_additionalConfiguration.EC2_AGENT_MANAGEMENT |
| <a href="#">Protección de Lambda</a>                        |                                         | LAMBDA_NETWORK_LOGS                                             |

<sup>\*</sup> GetUsageStatistics usa sus propios nombres de dataSource. Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#) o [GetUsageStatistics](#).



# Seguridad en Amazon GuardDuty

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de [AWS cumplimiento, los programas](#) de . Para obtener más información sobre los programas de cumplimiento aplicables GuardDuty, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento](#) y .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza GuardDuty. Le muestra cómo configurarlo para GuardDuty cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus GuardDuty recursos.

## Contenido

- [Protección de datos en Amazon GuardDuty](#)
- [Registrar llamadas a GuardDuty la API de Amazon con AWS CloudTrail](#)
- [Identity and Access Management para Amazon GuardDuty](#)
- [Validación de conformidad para Amazon GuardDuty](#)
- [Resiliencia en Amazon GuardDuty](#)
- [Seguridad de infraestructuras en Amazon GuardDuty](#)
- [Amazon GuardDuty y puntos de enlace de VPC de interfaz \(\)AWS PrivateLink](#)

# Protección de datos en Amazon GuardDuty

El [modelo de](#) se aplica a la protección de datos en Amazon GuardDuty. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre privacidad de datos](#) y los . Para obtener más información sobre la protección de datos en Europa, consulte el [Centro del Reglamento General de Protección de Datos \(RGPD\)](#).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja GuardDuty o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos

de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

## Cifrado en reposo

Todos los datos de los GuardDuty clientes se cifran en reposo mediante soluciones AWS de cifrado.

GuardDuty los datos, como los hallazgos, se cifran en reposo mediante AWS Key Management Service (AWS KMS) utilizando AWS claves gestionadas por el cliente.

## Cifrado en tránsito

GuardDuty analiza los datos de registro de otros servicios. Cifra todos los datos en tránsito de estos servicios con HTTPS y KMS. Una vez que GuardDuty extrae la información que necesita de los registros, estos se descartan. Para obtener más información sobre cómo se GuardDuty utiliza la información de otros servicios, consulte [las fuentes de GuardDuty datos](#).

GuardDuty los datos se cifran en tránsito entre los servicios.

## Desactivación del uso de los datos para mejorar el servicio

Puede optar por no utilizar sus datos para desarrollar GuardDuty y mejorar otros servicios de AWS seguridad mediante la política de AWS Organizations exclusión. Puede optar por excluirse incluso si actualmente GuardDuty no recopila dichos datos. Para más información sobre cómo excluirse, consulte [Políticas de exclusión de servicios de IA](#) en la Guía del usuario de AWS Organizations .

### Note

Para poder utilizar la política de exclusión voluntaria, sus AWS cuentas deben estar gestionadas de forma centralizada por AWS Organizations. Si aún no ha creado una organización para sus AWS cuentas, consulte [Creación y administración de una organización](#) en la Guía del AWS Organizations usuario.

La exclusión tiene los siguientes efectos:

- GuardDuty eliminará los datos que recopiló y almacenó con fines de mejora del servicio antes de su exclusión voluntaria (si la hubiera).

- Una vez que opte por no participar, ya no GuardDuty recopilará ni almacenará estos datos con fines de mejora del servicio.

En los siguientes temas se explica cómo cada una de las funciones GuardDuty incluidas en ella puede gestionar sus datos para mejorar el servicio.

## Contenido

- [GuardDuty Supervisión del tiempo de ejecución](#)
- [GuardDuty Protección contra el malware](#)

## GuardDuty Supervisión del tiempo de ejecución

GuardDuty Runtime Monitoring ofrece detección de amenazas en tiempo de ejecución para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) AWS Fargate , solo para Amazon Elastic Container Service (Amazon ECS) y para las instancias de Amazon Elastic Compute Cloud (Amazon EC2) de su entorno. AWS Tras activar Runtime Monitoring e implementar el agente de GuardDuty seguridad para su recurso, GuardDuty comienza a monitorear y analizar los eventos de tiempo de ejecución asociados a su recurso. Estos tipos de eventos en tiempo de ejecución incluyen eventos de proceso, eventos de contenedor, eventos DNS y más. Para obtener más información, consulte [Tipos de eventos de tiempo de ejecución recopilados que utilizan GuardDuty](#).

GuardDuty recopila tanto los comandos (como `curlsystemctl`, `ycron`) como sus argumentos asociados (como `start`, `stop`, `disable`) de sus cargas de trabajo. Por ejemplo, cuando alguien ejecuta `systemctl stop service-name`, GuardDuty captura tanto el comando como `systemctl` sus argumentos `stop service-name`. Esta información detallada ayuda GuardDuty a detectar amenazas sofisticadas mediante el análisis de los patrones de comandos y la correlación de varios eventos. Por ejemplo, GuardDuty puede identificar cuándo un atacante intenta deshabilitar los servicios de seguridad o ejecuta archivos maliciosos conocidos. Si bien utiliza estos datos de GuardDuty forma activa para la detección de amenazas, actualmente no utiliza estos comandos y argumentos para mejorar el servicio (es posible que lo haga en el futuro). Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte [Preguntas frecuentes sobre privacidad de datos](#).

## GuardDuty Protección contra el malware

GuardDuty Malware Protection analiza y detecta el malware contenido en los volúmenes de EBS adjuntos a sus cargas de trabajo de instancias y contenedores de Amazon EC2 potencialmente comprometidas, los archivos recién cargados en los buckets de Amazon S3 seleccionados y los recursos de respaldo. Actualmente, GuardDuty no recopila ni utiliza el malware detectado para mejorar el servicio. Sin embargo, en el futuro, cuando GuardDuty Malware Protection identifique un archivo de volumen de EBS, un archivo de respaldo o un archivo S3 como malicioso o dañino, GuardDuty Malware Protection recopilará y almacenará este archivo para desarrollar y mejorar sus detecciones de malware y el GuardDuty servicio. Este archivo también se puede utilizar para desarrollar y mejorar otros servicios de seguridad de AWS. Su confianza, la privacidad y la seguridad de su contenido son nuestra máxima prioridad y garantizamos que nuestro uso cumpla con nuestros compromisos con usted. Para obtener más información, consulte [Preguntas frecuentes sobre privacidad de datos](#).

## Registrar llamadas a GuardDuty la API de Amazon con AWS CloudTrail

Amazon GuardDuty está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en GuardDuty. CloudTrail captura todas las llamadas a las API GuardDuty como eventos, incluidas las llamadas desde la GuardDuty consola y las llamadas en código a las GuardDuty API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos los eventos de GuardDuty. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar el destinatario de la solicitud GuardDuty, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información sobre CloudTrail cómo configurarla y habilitarla, consulte la [Guía del AWS CloudTrail usuario](#).

## GuardDuty información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad de eventos admitida GuardDuty, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo [ver eventos con el historial de CloudTrail eventos](#).

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta GuardDuty, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte lo siguiente:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con CloudTrail](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se hizo con las credenciales de inicio de sesión del usuario raíz o del usuario de IAM
- si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte [Elemento userIdentity de CloudTrail](#).

## GuardDuty eventos del plano de control en CloudTrail

De forma predeterminada, CloudTrail registra todas las operaciones de la GuardDuty API proporcionadas en la [referencia de la GuardDuty API de Amazon](#) como eventos en CloudTrail archivos.

## GuardDuty eventos de datos en CloudTrail

[GuardDuty Supervisión del tiempo de ejecución](#) utiliza un agente de GuardDuty seguridad desplegado en sus clústeres de Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate instancias de Amazon Elastic Compute Cloud (Amazon EC2) Compute Cloud (Amazon EC2) y tareas aws-guardduty-agent (únicamente Amazon Elastic Container Service (Amazon ECS)) para

recopilar complementos [Tipos de eventos de tiempo de ejecución recopilados](#) () AWS que recopilan sus cargas de trabajo y luego las envían para detectar y analizar amenazas. GuardDuty

## Registro y supervisión de eventos de datos

Si lo desea, puede configurar los AWS CloudTrail registros para ver los eventos de datos de su agente de seguridad. GuardDuty

Para crearlos y configurarlos CloudTrail, consulte [los eventos de datos](#) en la Guía del AWS CloudTrail usuario y siga las instrucciones para registrar los eventos de datos con los selectores de eventos avanzados del Consola de administración de AWS. Al registrar el registro de seguimiento, asegúrese de hacer los siguientes cambios:

- Para el tipo de evento de datos, elija GuardDutydetector.
- En Plantilla de selector de registros, elija Registrar todos los eventos.
- Amplíe la Vista JSON para la configuración. Debería ser similar al siguiente JSON:

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Tras activar el selector de la ruta, diríjase a la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>. Puede descargar los eventos de datos del bucket de S3 que eligió al momento de configurar los CloudTrail registros.

## Ejemplo: entradas de archivos de GuardDuty registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra el evento del plano de datos.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
    "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-instance/i-123412341234example",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "111122223333:aws:ec2-instance",
        "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
        "accountId": "111122223333",
        "userName": "aws:ec2-instance"
      },
      "attributes": {
        "creationDate": "2023-03-05T04:00:21Z",
        "mfaAuthenticated": "false"
      }
    },
    "ec2RoleDelivery": "2.0"
  },
  "eventTime": "2023-03-05T06:03:49Z",
  "eventSource": "guardduty.amazonaws.com",
  "eventName": "SendSecurityTelemetry",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "54.240.230.177",
  "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
```



```

    "requestParameters": null,
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbbb",
    "readOnly": false,
    "resources": [{
      "accountId": "111122223333",
      "type": "AWS::GuardDuty::Detector",
      "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data",
    "tlsDetails": {
      "tlsVersion": "TLSv1.2",
      "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
      "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
    }
  }
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la CreateIPThreatIntelSet acción (evento del plano de control).

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::444455556666:user/Alice",
    "accountId": "444455556666",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-06-14T22:54:20Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",

```

```
        "userName": "Alice"
      }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
      "name": "Example",
      "format": "TXT",
      "activate": false,
      "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
      "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
  }
}
```

A partir de la información de este evento, puede determinar que la solicitud se realizó para crear una lista de amenazas Example en GuardDuty. También puede ver que la solicitud la hizo una usuaria llamada Alice el 14 de junio de 2018.

## Identity and Access Management para Amazon GuardDuty

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. GuardDuty La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [Cómo GuardDuty funciona Amazon con IAM](#)
- [Identity-based ejemplos de políticas para Amazon GuardDuty](#)
- [Uso de roles vinculados a servicios para Amazon GuardDuty](#)
- [AWS políticas gestionadas para Amazon GuardDuty](#)
- [Solución de problemas de GuardDuty identidad y acceso a Amazon](#)

## Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Solución de problemas de GuardDuty identidad y acceso a Amazon](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo GuardDuty funciona Amazon con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [Identity-based ejemplos de políticas para Amazon GuardDuty](#)).

## Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

## Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomienda encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

## Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

## Roles de IAM

Un [Rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

## Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

### Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

### Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

## Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

## Cómo GuardDuty funciona Amazon con IAM

Antes de utilizar IAM para gestionar el acceso GuardDuty, infórmate sobre las funciones de IAM disponibles. GuardDuty

## Funciones de IAM que puedes usar con Amazon GuardDuty

| Característica de IAM                             | GuardDuty soporte |
|---------------------------------------------------|-------------------|
| <a href="#">Identity-based políticas</a>          | Sí                |
| <a href="#">Resource-based políticas</a>          | No                |
| <a href="#">Acciones de políticas</a>             | Sí                |
| <a href="#">Recursos de políticas</a>             | Sí                |
| <a href="#">Claves de condición de política</a>   | Sí                |
| <a href="#">ACL</a>                               | No                |
| <a href="#">ABAC (etiquetas en políticas)</a>     | Parcial           |
| <a href="#">Credenciales temporales</a>           | Sí                |
| <a href="#">Permisos de entidades principales</a> | Sí                |
| <a href="#">Roles de servicio</a>                 | Sí                |
| <a href="#">Service-linked roles</a>              | Sí                |

Para obtener una visión general de cómo GuardDuty funcionan otros AWS servicios con la mayoría de las funciones de IAM, consulte [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

### Identity-based políticas para GuardDuty

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de la política de JSON de IAM](#) en la Guía del usuario de IAM.

### Identity-based ejemplos de políticas para GuardDuty

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. [Identity-based ejemplos de políticas para Amazon GuardDuty](#)

### Resource-based políticas dentro GuardDuty

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

### Acciones políticas para GuardDuty

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de GuardDuty acciones, consulta [Acciones definidas por Amazon GuardDuty](#) en la Referencia de autorización de servicio.



Las acciones políticas GuardDuty utilizan el siguiente prefijo antes de la acción:

```
guardduty
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
    "guardduty:action1",  
    "guardduty:action2"  
]
```

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte [Identity-based ejemplos de políticas para Amazon GuardDuty](#)

## Recursos de políticas para GuardDuty

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (\*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de GuardDuty recursos y sus ARN, consulte [Recursos definidos por Amazon GuardDuty](#) en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por Amazon](#). GuardDuty

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte [Identity-based ejemplos de políticas para Amazon GuardDuty](#)

## Claves de condición de la política para GuardDuty

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

Para ver una lista de claves de GuardDuty estado, consulta [Claves de estado de Amazon GuardDuty](#) en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones definidas por Amazon GuardDuty](#).

Para ver ejemplos de políticas GuardDuty basadas en la identidad, consulte. [Identity-based ejemplos de políticas para Amazon GuardDuty](#)

## Listas de control de acceso (ACL) en GuardDuty

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

## Attribute-based control de acceso (ABAC) con GuardDuty

Compatibilidad con ABAC (etiquetas en las políticas): parcial

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [Definición de permisos con la autorización de ABAC](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

## Uso de credenciales temporales con GuardDuty

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente al utilizar la federación o al cambiar de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte [Credenciales de seguridad temporales en IAM](#) y [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

## Cross-service permisos principales para GuardDuty

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama y la que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Sesiones de acceso directo](#).

## Funciones de servicio para GuardDuty

Compatible con roles de servicio: sí

Un rol de servicio es un [rol de IAM](#) que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Crear un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

### Warning

Cambiar los permisos de un rol de servicio podría interrumpir GuardDuty la funcionalidad. Edite las funciones de servicio solo cuando se GuardDuty proporcionen instrucciones para hacerlo.

## Service-linked roles para GuardDuty

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de funciones GuardDuty vinculadas al servicio, consulte. [Uso de roles vinculados a servicios para Amazon GuardDuty](#)

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta [Servicios de AWS que funcionan con IAM](#). Busque un servicio en la tabla que incluya una columna Yes en el Service-linked rol. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

## Identity-based ejemplos de políticas para Amazon GuardDuty

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de GuardDuty. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por GuardDuty, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de Amazon GuardDuty](#) en la Referencia de autorización de servicio.

### Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola GuardDuty](#)
- [Permisos necesarios para habilitarla GuardDuty](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Política de IAM personalizada para conceder acceso de solo lectura a GuardDuty](#)
- [Denegar el acceso a los resultados GuardDuty](#)
- [Utilizar una política de IAM personalizada para limitar el acceso a los recursos GuardDuty](#)

## Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar GuardDuty los recursos de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## Uso de la consola GuardDuty

Para acceder a la GuardDuty consola de Amazon, debes tener un conjunto mínimo de permisos. Estos permisos deben permitirte enumerar y ver detalles sobre los GuardDuty recursos de tu cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la GuardDuty consola, asocie también la GuardDuty ConsoleAccess política ReadOnly AWS gestionada a las entidades. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM:

## Permisos necesarios para habilitarla GuardDuty

Para conceder los permisos que deben tener varias identidades de IAM (usuarios, grupos y roles), adjunte la [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) política requerida para GuardDuty habilitarlos.

## Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la AWS CLI API o. AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
```

```

        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

## Política de IAM personalizada para conceder acceso de solo lectura a GuardDuty

Para conceder acceso de solo lectura, GuardDuty puede utilizar la política gestionada.

**AmazonGuardDutyReadOnlyAccess**

Para crear una política personalizada que conceda a un rol, usuario o grupo de IAM acceso de solo lectura GuardDuty, puedes usar la siguiente declaración:

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",

```

```

        "guardduty:ListInvitations",
        "guardduty:ListDetectors",
        "guardduty:GetDetector",
        "guardduty:ListFindings",
        "guardduty:GetFindings",
        "guardduty:ListIPSets",
        "guardduty:GetIPSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:GetThreatIntelSet",
        "guardduty:GetMasterAccount",
        "guardduty:GetInvitationsCount",
        "guardduty:GetFindingsStatistics",
        "guardduty:DescribeMalwareScans",
        "guardduty:UpdateMalwareScanSettings",
        "guardduty:GetMalwareScanSettings"
    ],
    "Resource": "*"
}
]
}

```

## Denegar el acceso a los resultados GuardDuty

Puede usar la siguiente política para denegar el acceso a los GuardDuty hallazgos a un rol, usuario o grupo de IAM. Los usuarios no pueden ver los resultados ni sus detalles, pero pueden acceder a todas las demás GuardDuty operaciones:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:CreateDetector",
        "guardduty>DeleteDetector",
        "guardduty:UpdateDetector",
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:CreateIPSet",

```



```

        "guardduty:DeleteIPSet",
        "guardduty:UpdateIPSet",
        "guardduty:GetIPSet",
        "guardduty:ListIPSets",
        "guardduty:CreateThreatIntelSet",
        "guardduty:DeleteThreatIntelSet",
        "guardduty:UpdateThreatIntelSet",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListThreatIntelSets",
        "guardduty:ArchiveFindings",
        "guardduty:UnarchiveFindings",
        "guardduty:CreateSampleFindings",
        "guardduty:CreateMembers",
        "guardduty:InviteMembers",
        "guardduty:GetMembers",
        "guardduty:DeleteMembers",
        "guardduty:DisassociateMembers",
        "guardduty:StartMonitoringMembers",
        "guardduty:StopMonitoringMembers",
        "guardduty:ListMembers",
        "guardduty:GetMasterAccount",
        "guardduty:DisassociateFromMasterAccount",
        "guardduty:AcceptAdministratorInvitation",
        "guardduty:ListInvitations",
        "guardduty:GetInvitationsCount",
        "guardduty:DeclineInvitations",
        "guardduty:DeleteInvitations"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
    }
},
{

```

```
        "Effect": "Allow",
        "Action": [
            "iam:PutRolePolicy",
            "iam:DeleteRolePolicy"
        ],
        "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
    }
}
```

## Utilizar una política de IAM personalizada para limitar el acceso a los recursos GuardDuty

Para definir el acceso de un usuario en GuardDuty función del ID del detector, puedes utilizar todas [las acciones de la GuardDuty API](#) en tus políticas de IAM personalizadas, excepto las siguientes operaciones:

- guardduty:CreateDetector
- guardduty:DeclineInvitations
- guardduty>DeleteInvitations
- guardduty:GetInvitationsCount
- guardduty:ListDetectors
- guardduty:ListInvitations

Utilice las siguientes operaciones en una política de IAM para definir el acceso de un usuario en GuardDuty función del ID y el ID del IPset: ThreatIntelSet

- guardduty>DeleteIPSet
- guardduty>DeleteThreatIntelSet
- guardduty:GetIPSet
- guardduty:GetThreatIntelSet
- guardduty:UpdateIPSet
- guardduty:UpdateThreatIntelSet

En los siguientes ejemplos se muestra cómo crear políticas con algunas de las operaciones anteriores:

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateDetector`, con el ID de detector 1234567 en la región us-east-1:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateDetector"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
    }
  ]
}
```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con el ID de detector 1234567 y el ID de IPSet 000000 en la región us-east-1:

 Note

Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas. GuardDuty Para obtener más información, consulte [Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-
east-1:123456789012:detector/1234567/ipset/000000"
    }
  ]
}

```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con cualquier ID de detector y el ID de IPSet 000000 en la región us-east-1:

#### Note

Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas GuardDuty. Para obtener más información, consulte [Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP](#).

## JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
    }
  ]
}

```

- Esta política permite a un usuario ejecutar la operación `guardduty:UpdateIPSet`, con su ID de detector y cualquier ID de IPSet en la región us-east-1:

**Note**

Asegúrese de que el usuario tenga los permisos necesarios para acceder a las listas de direcciones IP confiables y a las listas de amenazas GuardDuty. Para obtener más información, consulte [Configuración de requisitos previos para las listas de entidades y las listas de direcciones IP](#).

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:UpdateIPSet"
      ],
      "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/ipset/*"
    }
  ]
}
```

## Uso de roles vinculados a servicios para Amazon GuardDuty

Amazon GuardDuty usa roles AWS Identity and Access Management vinculados a [servicios \(IAM\)](#). Un rol vinculado a un servicio (SLR) es un tipo único de rol de IAM al que se vincula directamente. GuardDuty Service-linked Los roles están predefinidos GuardDuty e incluyen todos los permisos necesarios para llamar a GuardDuty otros AWS servicios en su nombre.

Con el rol vinculado a un servicio, puedes configurarlo manualmente GuardDuty sin tener que añadir los permisos necesarios. GuardDuty define los permisos de su función vinculada al servicio y, a menos que los permisos se definan de otra manera, solo GuardDuty puede asumir la función. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede asociar a ninguna otra entidad de IAM.

GuardDuty admite el uso de funciones vinculadas al servicio en todas las regiones en las que esté disponible. GuardDuty Para obtener más información, consulte [Regiones y puntos de conexión](#).

Puede eliminar el rol GuardDuty vinculado al servicio solo después de haberlo desactivado por primera vez GuardDuty en todas las regiones en las que esté habilitado. Esto protege sus GuardDuty recursos porque no puede eliminar el permiso de acceso a ellos sin darse cuenta.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los [AWS servicios que funcionan con IAM en la Guía del usuario de IAM](#) y busque los servicios que tengan la columna Sí en la columna Función. Service-Linked Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

## Service-linked permisos de rol para GuardDuty

GuardDuty usa el rol vinculado al servicio (SLR) denominado.

`AWSServiceRoleForAmazonGuardDuty` La SLR permite realizar GuardDuty las siguientes tareas. También permite GuardDuty incluir los metadatos recuperados pertenecientes a la instancia EC2 en los hallazgos que se GuardDuty puedan generar sobre la potencial amenaza. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDuty` confía en el servicio `guardduty.amazonaws.com` para asumir el rol.

Las políticas de permisos ayudan a GuardDuty realizar las siguientes tareas:

- Utilice las acciones de Amazon EC2 para administrar y recuperar información sobre las instancias de EC2, imágenes y componentes de red, como VPC, subredes y puertas de enlace de tránsito.
- Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias EC2 que tienen una etiqueta de inclusión (:).  
`GuardDutyManaged true`
- Use AWS Organizations acciones para describir las cuentas asociadas y el identificador de la organización.
- Utilizar las acciones de Amazon S3 para recuperar información sobre buckets y objetos de S3.
- Utilice AWS Lambda acciones para recuperar información sobre las funciones y etiquetas de Lambda.
- Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los [complementos de Amazon EKS](#) en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a GuardDuty ellas.

- Utilice IAM para crear el [Service-linked permisos de rol para Malware Protection for EC2](#) después de que se haya habilitado Malware Protection for EC2.
- Utilice las acciones de Amazon ECS para gestionar y recuperar información sobre los clústeres de Amazon ECS, recuperar información sobre las tareas y las definiciones de tareas y gestionar la configuración de la cuenta de Amazon ECS con `guardddutyActivate`. Las acciones relacionadas con Amazon ECS también recuperan la información sobre las etiquetas asociadas GuardDuty.

El rol se configura con la siguiente [política administrada por AWS](#), que se denomina `AmazonGuardDutyServiceRolePolicy`.

Para revisar los permisos de esta política, consulte [AmazonGuardDutyServiceRolePolicy](#) en la Guía de referencia de la política administrada de AWS .

A continuación se presenta la política de confianza que se asocia al rol vinculado a servicio `AWSServiceRoleForAmazonGuardDuty`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "guarddduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para obtener más información sobre actualizaciones a la política `AmazonGuardDutyServiceRolePolicy`, consulte [GuardDuty actualizaciones de las políticas gestionadas AWS](#). Para obtener alertas automáticas sobre cambios en esta política, suscríbase a la fuente RSS en la página de [Historial de revisión](#).

## Crear un rol vinculado a un servicio para GuardDuty

El rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio se crea automáticamente cuando lo habilitas GuardDuty por primera vez o lo habilitas GuardDuty en una región compatible en la que antes no lo tenías habilitado. También puede crear el rol vinculado al servicio manualmente mediante la consola de IAM, la API de IAM o la misma AWS CLI.

### Important

El rol vinculado al servicio que se crea para la cuenta de administrador GuardDuty delegado no se aplica a las cuentas de los miembros. GuardDuty

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio se cree correctamente, el director de IAM GuardDuty con el que utilices debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

### Note

Sustituya *account ID* el ejemplo siguiente por su ID real. Cuenta de AWS

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```



```

        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Condition": {
        "StringLike": {
            "iam:AWSServiceName": "guardduty.amazonaws.com"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
]
}

```

Para obtener más información acerca de cómo crear un rol manualmente, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

### Edición de un rol vinculado a un servicio para GuardDuty

GuardDuty no permite editar el rol vinculado al `AWSServiceRoleForAmazonGuardDuty` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

### Eliminar un rol vinculado a un servicio para GuardDuty

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

**⚠ Important**

Si ha habilitado Malware Protection for EC2, la eliminación de `AWSServiceRoleForAmazonGuardDuty` no elimina `AWSServiceRoleForAmazonGuardDutyMalwareProtection` automáticamente. Si desea eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulte [Eliminar un rol vinculado al servicio para Malware Protection for EC2](#).

Primero debe deshabilitarlo GuardDuty en todas las regiones en las que esté habilitado para eliminar el `AWSServiceRoleForAmazonGuardDuty`. Si el GuardDuty servicio no está deshabilitado al intentar eliminar el rol vinculado al servicio, se producirá un error en la eliminación. Para obtener más información, consulte [Suspender o deshabilitar GuardDuty](#).

Cuando lo inhabilitas GuardDuty, `AWSServiceRoleForAmazonGuardDuty` no se elimina automáticamente. Si lo GuardDuty vuelves a activar, empezará a usar lo existente `AWSServiceRoleForAmazonGuardDuty`.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Usa la consola de IAM, AWS CLI, la o la API de IAM para eliminar la función vinculada al `AWSServiceRoleForAmazonGuardDuty` servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

### Compatible Regiones de AWS

Amazon GuardDuty admite el uso del rol `AWSServiceRoleForAmazonGuardDuty` vinculado al servicio en todas las Regiones de AWS lugares disponibles GuardDuty. Para ver una lista de las regiones en las GuardDuty que está disponible actualmente, consulta los [GuardDuty puntos de conexión y las cuotas de Amazon](#) en Referencia general de Amazon Web Services.

### Service-linked permisos de rol para Malware Protection for EC2

Malware Protection for EC2 utiliza el rol vinculado al servicio (SLR) denominado `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Esta cámara réflex permite a Malware Protection for EC2 realizar escaneos sin agentes para detectar malware en su cuenta. GuardDuty Permite GuardDuty crear una instantánea del volumen de EBS en su cuenta y compartirla con la cuenta de servicio. GuardDuty Tras GuardDuty evaluar la instantánea, incluye los metadatos de la carga de trabajo del contenedor y de la instancia de EC2.

recuperados en las conclusiones sobre Malware Protection for EC2. El rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection` confía en el servicio `malware-protection.guardduty.amazonaws.com` para asumir el rol.

Las políticas de permisos de este rol ayudan a Malware Protection for EC2 a realizar las siguientes tareas:

- Utilice las acciones de Amazon Elastic Compute Cloud (Amazon EC2) para recuperar información sobre las instancias de Amazon EC2, los volúmenes y las instantáneas. Malware Protection for EC2 también concede permiso para acceder a los metadatos de clúster de Amazon EKS y Amazon ECS.
- Crear instantáneas para los volúmenes de EBS cuya etiqueta `GuardDutyExcluded` no esté configurada como `true`. De forma predeterminada, las instantáneas se crean con una etiqueta `GuardDutyScanId`. No elimine esta etiqueta. Si lo hace, Malware Protection for EC2 no tendrá acceso a las instantáneas.

 Important

Si lo configura `true`, el GuardDuty servicio no podrá acceder a estas instantáneas en el futuro. `GuardDutyExcluded` Esto se debe a que las demás instrucciones de esta función vinculada al servicio GuardDuty impiden realizar ninguna acción en las instantáneas para las que está establecido. `GuardDutyExcluded true`

- Permitir compartir y eliminar instantáneas solo si la etiqueta `GuardDutyScanId` existe y la etiqueta `GuardDutyExcluded` no está establecida en `true`.

 Note

No permite que Malware Protection for EC2 haga públicas las instantáneas.

- Acceda a las claves administradas por el cliente, excepto a las que tengan una `GuardDutyExcluded` etiqueta configurada como `true`, `CreateGrant` para crear un volumen de EBS cifrado y acceder a él desde la instantánea cifrada que se comparte con la cuenta de servicio. GuardDuty Para obtener una lista de las cuentas de GuardDuty servicio de cada región, consulte [GuardDuty cuentas de servicio de Región de AWS](#).
- Acceda a los CloudWatch registros de los clientes para crear el grupo de registros de Malware Protection for EC2 y coloque los registros de eventos de análisis de malware en el `/aws/guardduty/malware-scan-events` grupo de registros.

- Permitir que el cliente decida si quiere conservar en su cuenta las instantáneas en las que se detectó el malware. Si el análisis detecta malware, la función vinculada al servicio permite añadir dos etiquetas GuardDuty a las instantáneas: `y. GuardDutyFindingDetected` y `GuardDutyExcluded`

 Note

La etiqueta `GuardDutyFindingDetected` especifica que las instantáneas contienen malware.

- Determine si un volumen está cifrado con una clave gestionada por EBS. GuardDuty realiza la `DescribeKey` acción para determinar la EBS-managed clave `key Id` de su cuenta.
- Obtenga la instantánea de los volúmenes de EBS cifrados con Clave administrada de AWS, de la suya Cuenta de AWS y cópiela en la. [GuardDuty cuenta de servicio](#) Para ello, utilizamos los permisos `GetSnapshotBlock` y `ListSnapshotBlocks` GuardDuty luego escaneará la instantánea en la cuenta de servicio. En la actualidad, es posible que la compatibilidad con Malware Protection for EC2 para escanear volúmenes de EBS cifrados con Clave administrada de AWS ella no esté disponible en todos los. Regiones de AWS Para obtener más información, consulte [Region-specific disponibilidad de funciones](#).
- Permita que Amazon EC2 llame AWS KMS en nombre de Malware Protection para que EC2 realice varias acciones criptográficas en las claves administradas por el cliente. Acciones como `kms:ReEncryptTo` y `kms:ReEncryptFrom` son obligatorias para compartir las instantáneas cifradas con las claves administradas por el cliente. Solo se puede acceder a las claves para las que la etiqueta `GuardDutyExcluded` no esté establecida en `true`.

El rol se configura con la siguiente [política administrada por AWS](#), que se denomina `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Para revisar los permisos de esta política, consulte [AmazonGuardDutyMalwareProtectionServiceRolePolicy](#) en la Guía de referencia de la política administrada de AWS .

La siguiente política de confianza se ha adjuntado al rol vinculado a servicios `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "malware-protection.guardduty.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

### Crear un rol vinculado al servicio para Malware Protection for EC2

El rol vinculado al servicio `AWSServiceRoleForAmazonGuardDutyMalwareProtection` se crea automáticamente cuando se habilita Malware Protection for EC2 por primera vez o al habilitar Malware Protection for EC2 en una región compatible en la que no estaba habilitado. También puede crear el rol vinculado al servicio `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente con la consola de IAM, la CLI de IAM o la API de IAM.

#### Note

De forma predeterminada, si eres nuevo en Amazon GuardDuty, Malware Protection for EC2 se activa automáticamente.

#### Important

El rol vinculado al servicio que se crea para la cuenta de GuardDuty administrador delegado no se aplica a las cuentas de los miembros. GuardDuty

Debe configurar permisos para permitir a una entidad principal de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculado al servicio se cree

correctamente, la identidad de IAM que utilices GuardDuty debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a un usuario, un grupo o un rol de :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "guardduty:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:GetRole",
      "Resource": "arn:aws:iam::*:role/*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
  ]
}
```

```
} ]
```

Para obtener más información sobre cómo crear un rol manualmente, consulte [Crear un rol vinculado a servicios](#) en la Guía del usuario de IAM.

### Editar un rol vinculado al servicio para Malware Protection for EC2

Malware Protection for EC2 no permite editar el rol vinculado al servicio `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

### Eliminar un rol vinculado al servicio para Malware Protection for EC2

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no conservará una entidad no utilizada que no se monitoree ni se mantenga de forma activa.

#### Important

Para poder eliminar `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, primero debe desactivar Malware Protection for EC2 en todas las regiones en las que esté habilitada.

Si Malware Protection for EC2 está habilitada al intentar eliminar el rol vinculado al servicio, el rol no se eliminará. Asegúrese de desactivar primero Malware Protection for EC2 en la cuenta.

Si selecciona Desactivar para detener el servicio de Malware Protection for EC2, `AWSServiceRoleForAmazonGuardDutyMalwareProtection` no se elimina automáticamente. Si, a continuación, selecciona Activar para volver a iniciar el servicio Malware Protection for EC2, GuardDuty empezará a utilizar el existente. `AWSServiceRoleForAmazonGuardDutyMalwareProtection`

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de IAM para eliminar el rol vinculado al `AWSServiceRoleForAmazonGuardDutyMalwareProtection` servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Compatible Regiones de AWS

Amazon GuardDuty admite el uso de la función

`AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada al servicio en todos los Regiones de AWS lugares donde esté disponible Malware Protection for EC2.

Para ver una lista de las regiones en las GuardDuty que está disponible actualmente, consulta los [GuardDuty puntos de conexión y las cuotas de Amazon](#) en. Referencia general de Amazon Web Services

### Note

La protección contra malware para EC2 no está disponible actualmente en AWS GovCloud (US-East) y AWS GovCloud (US-West).

## AWS políticas gestionadas para Amazon GuardDuty

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios añaden permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a



todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

El elemento de la política `Version` especifica las reglas de sintaxis del lenguaje que se van a utilizar para procesar esta política. Las siguientes políticas incluyen la versión actual que IAM admite. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Versión](#).

## AWS política gestionada: AmazonGuardDutyFullAccess\_v2 (recomendada)

Puede asociar la política AmazonGuardDutyFullAccess\_v2 a las identidades de IAM. Esta política permitirá al usuario el acceso total para realizar todas GuardDuty las acciones y acceder a los recursos necesarios. Between AmazonGuardDutyFullAccess\_v2 y AmazonGuardDutyFullAccess, GuardDuty recomienda adjuntarlo AmazonGuardDutyFullAccess\_v2 porque ofrece una mayor seguridad y restringe las acciones administrativas a los directores de GuardDuty servicio.

### Detalles del permiso

La política AmazonGuardDutyFullAccess\_v2 incluye los siguientes permisos:

- GuardDuty— Permite a los usuarios el acceso total a todas las acciones. GuardDuty
- IAM:
  - Permite a los usuarios crear un rol GuardDuty vinculado al servicio.
  - Permite ver y gestionar las funciones de IAM y sus políticas para. GuardDuty
  - Permite a los usuarios transferir un rol a GuardDuty. GuardDuty utiliza esta función para activar la protección contra malware para S3 y analizar los objetos de S3 en busca de malware. GuardDuty también utiliza esta función para iniciar los análisis de Malware Protection for AWS Backup.
  - El permiso para llevar a cabo una acción `iam:GetRole` en `AWSServiceRoleForAmazonGuardDutyMalwareProtection` establece si el rol vinculado al servicio (SLR) para Malware Protection for EC2 existe en una cuenta.
- Organizations:
  - Permite a los usuarios leer (ver) GuardDuty la estructura de la organización y las cuentas.
  - Permite a los usuarios designar un administrador delegado y gestionar los miembros de una GuardDuty organización.

Para revisar los permisos de esta política, consulte [AmazonGuardDutyFullAccess\\_v2](#) en la Guía de referencia de políticas AWS administradas.

## AWS política gestionada: AmazonGuardDutyFullAccess

Puede asociar la política AmazonGuardDutyFullAccess a las identidades de IAM.

### Important

Para mejorar la seguridad y restringir los permisos a los directores de GuardDuty servicio, le recomendamos que utilice [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#).

Esta política otorga permisos administrativos que permiten al usuario tener acceso total para realizar todas GuardDuty las acciones y recursos.

### Detalles del permiso

Esta política incluye los siguientes permisos.

- GuardDuty— Permite a los usuarios el acceso total a todas GuardDuty las acciones.
- IAM:
  - Permite a los usuarios crear el rol GuardDuty vinculado al servicio.
  - Permite que una cuenta de administrador se habilite GuardDuty para las cuentas de los miembros.
  - Permite a los usuarios transferir un rol a GuardDuty. GuardDuty utiliza esta función para activar la protección contra malware para S3 y analizar los objetos de S3 en busca de malware. GuardDuty también utiliza esta función para iniciar los análisis de Malware Protection for AWS Backup.
- Organizations— Permite a los usuarios designar un administrador delegado y gestionar los miembros de una GuardDuty organización.

El permiso para llevar a cabo una acción `iam:GetRole` en `AWSServiceRoleForAmazonGuardDutyMalwareProtection` establece si el rol vinculado al servicio (SLR) para Malware Protection for EC2 existe en una cuenta.

Para revisar los permisos de esta política, consulte [AmazonGuardDutyFullAccess](#) en la Guía de referencia de la política administrada de AWS .

## AWS política gestionada: AmazonGuardDutyReadOnlyAccess

Puede asociar la política AmazonGuardDutyReadOnlyAccess a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten al usuario ver las GuardDuty conclusiones y los detalles de su GuardDuty organización.

### Detalles de los permisos

Esta política incluye los siguientes permisos.

- **GuardDuty**— Permite a los usuarios ver los GuardDuty resultados y realizar operaciones de API que comiencen con `GetList`, o. `Describe`
- **Organizations**— Permite a los usuarios recuperar información sobre GuardDuty la configuración de la organización, incluidos los detalles de la cuenta de administrador delegado.

Para revisar los permisos de esta política, consulte [AmazonGuardDutyReadOnlyAccess](#) en la Guía de referencia de la política administrada de AWS .

## AWS política gestionada: AmazonGuardDutyServiceRolePolicy

No puede asociar AmazonGuardDutyServiceRolePolicy a sus entidades IAM. Esta política AWS gestionada está asociada a un rol vinculado al servicio que permite GuardDuty realizar acciones en su nombre. Para obtener más información, consulte [Service-linked permisos de rol para GuardDuty](#).

## GuardDuty actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas GuardDuty desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del GuardDuty documento.

| Cambio                                                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                      | Fecha               |
|-----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual | Se agregó <code>s3:ListBucket</code> permiso para recuperar listados de bucket de S3 <code>ecs:DescribeTasks</code> y <code>ecs:DescribeTaskDefinition</code> permisos para recuperar información sobre las tareas y definiciones de tareas de Amazon ECS.                                                                                                                       | 23 de abril de 2026 |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual | Se agregó el <code>cloudtrail:CreateServiceLinkedChannel</code> permiso para habilitar un mecanismo adicional para consumir AWS CloudTrail eventos.<br><br><pre>{     "Sid": "CloudTrailCreateServiceLinkedChannelSid",     "Effect": "Allow",     "Action": [         "cloudtrail:CreateServiceLinkedChannel"     ],     "Resource": "arn:aws:cloudtrail:*:*:channel/aws-</pre> | 25 de marzo de 2026 |

| Cambio                               | Descripción                                                                                                                                                                                                                                                                                                                                                                                 | Fecha               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                      | <pre>service-channel/guardduty/*",      "Condition": {          "StringEquals": {              "aws:ResourceAccount": "\${aws:PrincipalAccount}"          }      }  }</pre>                                                                                                                                                                                                                 |                     |
| AmazonGuardDutyFullAccess : obsoleta | <p>Esta política se ha reemplazado por una política de ámbito reducido denominada AmazonGuardDutyFullAccess_v2 .</p> <p>Después del 13 de marzo de 2026, no podrás adjuntar la AmazonGuardDutyFullAccess política a ningún usuario, grupo o función nuevos. Para obtener más información, consulte <a href="#">AWS política gestionada: AmazonGuardDutyFullAccess_v2 (recomendada)</a>.</p> | 13 de marzo de 2026 |

| Cambio                                                                              | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Fecha                   |
|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">AmazonGuardDutyFullAccess_v2</a> : actualización de una política actual | <div>Se agregó un permiso que le permite transferir una función de IAM GuardDuty al habilitar Malware Protection for AWS Backup.</div> <div><pre>{      "Sid":     "AllowPassRoleToMalwareProtection",      "Effect":     "Allow",      "Action": [          "iam:PassRole"      ],      "Resource":     "arn:aws:iam::*:role/*",      "Condition": {          "StringEquals": {              "iam:PassedToService": [                  "malware-protection-plan.guardduty.amazonaws.com",</pre></div> | 19 de noviembre de 2025 |

| Cambio | Descripción                                                               | Fecha |
|--------|---------------------------------------------------------------------------|-------|
|        | <pre>"malware-protectio n.guardduty.amazon aws.com"      ]   } }  }</pre> |       |

| Cambio                                                                           | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Fecha                   |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">AmazonGuardDutyFullAccess</a> : actualización de una política actual | <div>Se agregó un permiso que le permite transferir una función de IAM GuardDuty al habilitar Malware Protection for AWS Backup.</div> <div><pre>{<br/><br/>    "Sid":<br/>    "AllowPassRoleToMa<br/>lwareProtection",<br/><br/>    "Effect":<br/>    "Allow",<br/><br/>    "Action": [<br/><br/>        "iam:PassRole"<br/><br/>    ],<br/><br/>    "Resource":<br/>    "arn:aws:iam::*:role/<br/>*",<br/><br/>    "Conditio<br/>n": {<br/><br/>        "StringEquals": {<br/><br/>            "iam:PassedToServi<br/>ce": [<br/><br/>                "malware-protectio<br/>n-plan.guardduty.a<br/>mazonaws.com",</pre></div> | 19 de noviembre de 2025 |



| Cambio                                                                                  | Descripción                                                                                                                                                                                                                                                                                    | Fecha                |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
|                                                                                         | <pre>"malware-protection.guardduty.amazonaws.com"      ]    }  }</pre>                                                                                                                                                                                                                         |                      |
| <a href="#">AmazonGuardDutyFullAccess_v2</a> agregó una nueva política.                 | Se agregó una nueva política AmazonGuardDutyFullAccess_v2. Esto se recomienda porque sus permisos mejoran la seguridad al restringir las acciones administrativas a los directores de GuardDuty servicio en función de las funciones y políticas de IAM y de la integración. AWS Organizations | 4 de junio de 2025   |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual | Se agregó el permiso <code>ec2:DescribeVpcs</code> . Esto permite GuardDuty realizar un seguimiento de las actualizaciones de la VPC, por ejemplo, recuperar el CIDR de la VPC.                                                                                                                | 22 de agosto de 2024 |

| Cambio                                                                           | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Fecha               |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AmazonGuardDutyFullAccess</a> : actualización de una política actual | <div>Se ha añadido un permiso que permite transferir una función de IAM al activar la protección contra GuardDuty malware para S3.</div> <div><pre>{     "Sid":     "AllowPassRoleToMalwareProtectionPlan",     "Effect":     "Allow",     "Action": [      "iam:PassRole"     ],     "Resource":     "arn:aws:iam::*:role/*",     "Condition": {      "StringEquals": {      "iam:PassedToService": "malware-protection-plan.guardduty.amazonaws.com"     }     } }</pre></div> | 10 de junio de 2024 |

| Cambio                                                                                           | Descripción                                                                                                                                                                                                                                                                                                                                                                                                      | Fecha                |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">AmazonGuardDutySer<br/>viceRolePolicy</a> : actualización de una política existente. | Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias de EC2 que tienen una etiqueta de inclusión (:). GuardDuty Managed <code>true</code> | 26 de marzo de 2024  |
| <a href="#">AmazonGuardDutySer<br/>viceRolePolicy</a> : actualización de una política existente. | GuardDuty ha añadido un nuevo permiso <code>organization:DescribeOrganization</code> para recuperar el ID de organización de la cuenta de Amazon VPC compartida y configurar la política de puntos finales de Amazon VPC con el ID de la organización.                                                                                                                                                           | 9 de febrero de 2024 |

| Cambio                                                                                                       | Descripción                                                                                                                                                                                                                                                                                                           | Fecha                   |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">AmazonGuardDutyMalwareProtectionServiceRolePolicy</a> : actualización de una política existente. | Malware Protection for EC2 ha añadido dos permisos: <code>GetSnapshotBlock</code> el de obtener una instantánea de un volumen de EBS (cifrada mediante Clave administrada de AWS) Cuenta de AWS y copiarla a la cuenta de GuardDuty servicio antes de iniciar el análisis de malware. <code>ListSnapshotBlocks</code> | 25 de enero de 2024     |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual                      | Se han añadido nuevos permisos que permiten GuardDuty añadir la configuración de la cuenta de <code>guarddutyActivate</code> Amazon ECS y realizar, enumerar y describir operaciones en los clústeres de Amazon ECS.                                                                                                  | 26 de noviembre de 2023 |
| <a href="#">AmazonGuardDutyReadOnlyAccess</a> : actualización de una política actual                         | GuardDuty se agregó una nueva política <code>organizations</code> para <code>ListAccounts</code> .                                                                                                                                                                                                                    | 16 de noviembre de 2023 |
| <a href="#">AmazonGuardDutyFullAccess</a> : actualización de una política actual                             | GuardDuty agregó una nueva política <code>organizations</code> para <code>ListAccounts</code> .                                                                                                                                                                                                                       | 16 de noviembre de 2023 |
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual                      | GuardDuty agregó nuevos permisos para admitir la próxima función de monitoreo de tiempo de ejecución de GuardDuty EKS.                                                                                                                                                                                                | 8 de marzo de 2023      |

| Cambio                                                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Fecha                 |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual | <p>GuardDuty ha añadido nuevos permisos que permiten GuardDuty crear un <a href="#">Service-linked rol para Malware Protection for EC2</a>. Esto ayudará a GuardDuty agilizar el proceso de activación de la protección contra malware para EC2.</p> <p>GuardDuty ahora puede realizar la siguiente acción de IAM:</p> <pre> {   "Effect": "Allow",   "Action": "iam:CreateServiceLinkedRole",   "Resource": "*",   "Condition": {     "StringEquals": {       "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"     }   } }</pre> | 21 de febrero de 2023 |
| <a href="#">AmazonGuardDutyFullAccess</a> : actualización de una política actual        | <p>GuardDuty ARN actualizado para <code>iam:GetRole</code> .<br/> <code>*AWSServiceRoleForAmazonGuardDutyMalwareProtection</code></p>                                                                                                                                                                                                                                                                                                                                                                                                               | 26 de julio de 2022   |

| Cambio                                                                             | Descripción                                                                                                                                                                                                                                                                                                    | Fecha               |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AmazonGuardDutyFullAccess:</a><br>actualización de una política actual | <p>GuardDuty se agregó uno nuevo AWSServiceName para permitir la creación de un rol vinculado al servicio mediante el servicio GuardDuty Malware Protection iam:CreateServiceLinkedRole for EC2.</p> <p>GuardDuty ahora puede realizar la iam:GetRole acción para obtener información para. AWSServiceRole</p> | 26 de julio de 2022 |

| Cambio                                                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Fecha               |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AmazonGuardDutyServiceRolePolicy</a> : actualización de una política actual | <p>GuardDuty se han añadido nuevos permisos que permiten GuardDuty utilizar las acciones de red de Amazon EC2 para mejorar los resultados.</p> <p>GuardDuty ahora puede realizar las siguientes acciones de EC2 para obtener información sobre cómo se comunican sus instancias de EC2. Esta información se utiliza para mejorar la precisión de los resultados.</p> <ul style="list-style-type: none"> <li>• <code>ec2:DescribeVpcEndpoints</code></li> <li>• <code>ec2:DescribeSubnets</code></li> <li>• <code>ec2:DescribeVpcPeeringConnections</code></li> <li>• <code>ec2:DescribeTransitGatewayAttachments</code></li> </ul> | 3 de agosto de 2021 |
| GuardDuty comenzó a rastrear los cambios                                                | GuardDuty comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 3 de agosto de 2021 |

## Solución de problemas de GuardDuty identidad y acceso a Amazon

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas más comunes que puedes encontrar al trabajar con un GuardDuty IAM.

## Temas

- [No estoy autorizado a realizar ninguna acción en GuardDuty](#)
- [No estoy autorizado a realizar iam:PassRole.](#)
- [Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis GuardDuty recursos.](#)

## No estoy autorizado a realizar ninguna acción en GuardDuty

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM mateojackson intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *my-example-widget*, pero no tiene los permisos ficticios guardduty: *GetWidget*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
guardduty:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario mateojackson debe actualizarse para permitir el acceso al recurso *my-example-widget* mediante la acción guardduty: *GetWidget*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

## No estoy autorizado a realizar iam:PassRole.

Si recibe un error que indica que no tiene autorización para realizar la acción iam:PassRole, las políticas deben actualizarse a fin de permitirle pasar un rol a GuardDuty.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado marymajor intenta utilizar la consola para realizar una acción en GuardDuty. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```



En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis GuardDuty recursos.

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si GuardDuty es compatible con estas funciones, consulte [Cómo GuardDuty funciona Amazon con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo [proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

## Validación de conformidad para Amazon GuardDuty

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

## Resiliencia en Amazon GuardDuty

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la [infraestructura AWS global](#).

## Seguridad de infraestructuras en Amazon GuardDuty

Como servicio gestionado, Amazon GuardDuty está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a GuardDuty través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Paquetes de cifrado con perfecto secreto directo (PFS), como el DHE (Ephemeral) o el ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

# Amazon GuardDuty y puntos de enlace de VPC de interfaz ( )AWS PrivateLink

Puede establecer una conexión privada entre su VPC y Amazon GuardDuty mediante la creación de un punto de enlace de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a GuardDuty las API sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión AWS Direct Connect. [AWS PrivateLink](#) Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con GuardDuty las API. El tráfico entre tu VPC y GuardDuty no sale de la red de Amazon.

Cada punto de conexión de la interfaz está representado por una o más [interfaces de red elásticas](#) en las subredes.

Para obtener más información, consulte [Puntos de conexión de VPC de interfaz \(AWS PrivateLink\)](#) en la Guía de AWS PrivateLink .

## Consideraciones sobre los puntos GuardDuty finales de VPC

Antes de configurar un punto final de la VPC de la interfaz GuardDuty, asegúrese de revisar las [propiedades y limitaciones del punto final de la interfaz](#) en la AWS PrivateLink Guía.

GuardDuty admite realizar llamadas a todas sus acciones de API desde su VPC.

## Creación de un punto final de VPC de interfaz para GuardDuty

Puede crear un punto de enlace de VPC para el GuardDuty servicio mediante la consola de Amazon VPC o el ( ). AWS Command Line Interface AWS CLI Para obtener más información, consulte [Creación de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

Cree un punto final de VPC para GuardDuty usar el siguiente nombre de servicio:

- com.amazonaws. *region*.guardduty
- com.amazonaws. *region*.guardduty-fips (punto final de FIPS)

Si habilita el DNS privado para el punto final, puede realizar solicitudes a la API para GuardDuty utilizar su nombre de DNS predeterminado para la región, por ejemplo. `guardduty.us-east-1.amazonaws.com`

Para obtener más información, consulte [Acceso a un servicio a través de un punto de conexión de interfaz](#) en la Guía de AWS PrivateLink .

## Crear una política de puntos de conexión de VPC para GuardDuty

Puede asociar una política de punto de conexión con su punto de conexión de VPC que controla el acceso a GuardDuty. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte [Control del acceso a los servicios con puntos de conexión de VPC](#) en la Guía de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones GuardDuty

El siguiente es un ejemplo de una política de puntos finales para GuardDuty. Cuando se adjunta a un punto final, esta política otorga acceso a las GuardDuty acciones enumeradas a todos los principales de todos los recursos.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "guardduty:listDetectors",
        "guardduty:getDetector",
        "guardduty:getFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

## Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes

que se compartan con usted. Para obtener información sobre el uso compartido de VPC, consulte [Compartir su VPC con otras cuentas](#) en la Guía del usuario de Amazon VPC.

# GuardDuty integración con los servicios AWS de seguridad

GuardDuty se puede integrar con otros servicios AWS de seguridad. Estos servicios pueden procesar datos GuardDuty para permitirle ver los hallazgos de nuevas formas. Revisa las siguientes opciones de integración para obtener más información sobre cómo está configurado ese servicio para funcionar. GuardDuty

## Integrarse GuardDuty con AWS Security Hub CSPM

AWS Security Hub CSPM recopila datos de seguridad de sus AWS cuentas, servicios y productos de socios externos compatibles para evaluar el estado de seguridad de su entorno de acuerdo con los estándares y las mejores prácticas del sector. Además de evaluar su postura de seguridad, Security Hub CSPM crea una ubicación central para encontrar información sobre todos sus AWS servicios integrados y productos de AWS socios. La activación del Security Hub CSPM permitirá que el Security Hub CSPM ingiera automáticamente los datos de los GuardDuty hallazgos. GuardDuty

Para obtener más información sobre el uso de Security Hub CSPM con GuardDuty , consulte.

[Integrating with AWS Security Hub CSPM](#)

## Integración GuardDuty con Amazon Detective

Amazon Detective utiliza los datos de registro de todas sus AWS cuentas para crear visualizaciones de datos para sus recursos y direcciones IP que interactúan con su entorno. Las visualizaciones de Detective le ayudan a investigar los problemas de seguridad de forma rápida y sencilla. Puede pasar de la GuardDuty búsqueda de detalles a la información en la consola de Detectives una vez que ambos servicios estén habilitados.

Para obtener más información sobre el uso de Detective con, GuardDuty consulte [Integración con Amazon Detective](#).

## Integrating with AWS Security Hub CSPM

[AWS Security Hub CSPM](#) brinda una visión completa de su estado de seguridad en AWS y ayuda a comprobar su entorno con las prácticas recomendadas y los estándares del sector de seguridad. Security Hub CSPM recopila datos de seguridad de todas AWS las cuentas, servicios y productos de socios externos compatibles y le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

La GuardDuty integración de Amazon con el Security Hub CSPM le permite enviar los resultados desde GuardDuty al Security Hub CSPM. Luego, Security Hub CSPM puede incluir esos hallazgos en su análisis de su postura de seguridad.

## Contenido

- [Cómo GuardDuty envía Amazon los resultados a AWS Security Hub CSPM](#)
  - [Tipos de hallazgos que se GuardDuty envían a Security Hub \(CSPM\)](#)
    - [Latencia para el envío de nuevos resultados](#)
    - [Reintentos cuando el CSPM de Security Hub no está disponible](#)
    - [Actualización de resultados existentes en el CSPM de Security Hub](#)
- [GuardDuty Visualización de los resultados en AWS Security Hub CSPM](#)
  - [Interpretar los nombres de GuardDuty búsqueda en AWS Security Hub CSPM](#)
  - [Hallazgo típico de GuardDuty](#)
- [Habilitación y configuración de la integración](#)
- [Uso de GuardDuty controles en Security Hub \(CSPM\)](#)
- [Cómo detener la publicación de resultados en el CSPM de Security Hub](#)

## Cómo GuardDuty envía Amazon los resultados a AWS Security Hub CSPM

En AWS Security Hub CSPM, los problemas de seguridad se registran como hallazgos. Algunos hallazgos provienen de problemas detectados por otros AWS servicios o por socios externos. El CSPM de Security Hub también cuenta con un conjunto de reglas que utiliza para detectar problemas de seguridad y generar resultados.

El CSPM de Security Hub proporciona herramientas para administrar resultados procedentes de todos estos orígenes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Para obtener más información, consulte [Visualización de resultados](#) en la Guía del usuario de AWS Security Hub . También puede realizar un seguimiento del estado de una investigación de un resultado. Para obtener más información, consulte [Adopción de medidas en función de los resultados](#) en la Guía del usuario de AWS Security Hub .

Todos los resultados del CSPM de Security Hub utilizan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado. Consulte [Formato de resultados de seguridad de AWS \(ASFF\)](#) en la Guía del usuario de AWS Security Hub .

Amazon GuardDuty es uno de los AWS servicios que envía los resultados a Security Hub CSPM.

## Tipos de hallazgos que se GuardDuty envían a Security Hub (CSPM)

Una vez que habilita GuardDuty el CSPM de Security Hub en la misma cuenta dentro de la misma Región de AWS, GuardDuty comienza a enviar todos los hallazgos generados al Security Hub CSPM. Estos resultados se envían al Security Hub CSPM mediante el [AWS Security Finding Format \(ASFF\)](#). En ASFF, el campo Types proporciona el tipo de resultado.

### Latencia para el envío de nuevos resultados

Cuando GuardDuty crea un nuevo hallazgo, normalmente se envía al Security Hub CSPM en un plazo de cinco minutos.

### Reintentos cuando el CSPM de Security Hub no está disponible

Si el CSPM de Security Hub no está disponible, GuardDuty vuelve a intentar enviar las conclusiones hasta que las reciba.

### Actualización de resultados existentes en el CSPM de Security Hub

Tras enviar un hallazgo al Security Hub CSPM, GuardDuty envía actualizaciones para reflejar las observaciones adicionales de la actividad de búsqueda al Security Hub CSPM. Las nuevas observaciones de estos hallazgos se envían a Security Hub CSPM en función de la [Paso 5: Frecuencia de exportación de los resultados](#) configuración de su. Cuenta de AWS

Cuando archiva o desarchiva un hallazgo, GuardDuty no lo envía a Security Hub CSPM. Cualquier hallazgo desarchivado manualmente que luego se active no GuardDuty se envía a Security Hub CSPM.

## GuardDuty Visualización de los resultados en AWS Security Hub CSPM

Inicie sesión en Consola de administración de AWS y abra la AWS Security Hub CSPM consola en <https://console.aws.amazon.com/securityhub/>.

Ahora puede utilizar cualquiera de las siguientes formas de ver los GuardDuty resultados en la consola CSPM de Security Hub:

### Opción 1: Uso de integraciones en Security Hub CSPM

1. En el panel de navegación de la izquierda, seleccione Integraciones.
2. En la página de integraciones, comprueba el estado de Amazon: GuardDuty.



- Si el estado es Aceptación de resultados, seleccione Ver resultados junto a Aceptación de resultados.
- Si no es así, para obtener más información sobre cómo funcionan las integraciones, consulte las [integraciones de CSPM de Security Hub en la Guía del usuario](#).AWS Security Hub

## Opción 2: Uso de los hallazgos en Security Hub CSPM

1. En el panel de navegación izquierdo, elija Resultados.
2. En la página de hallazgos, añada el filtro Nombre del producto e introdúzcalo **GuardDuty** para ver solo GuardDuty los hallazgos.

## Interpretar los nombres de GuardDuty búsqueda en AWS Security Hub CSPM

GuardDuty envía los resultados al Security Hub CSPM mediante el [formato de búsqueda AWS de seguridad \(ASFF\)](#). En ASFF, el campo Types proporciona el tipo de resultado. Los tipos de ASFF utilizan un esquema de nomenclatura diferente al de los tipos. GuardDuty En la siguiente tabla se detallan todos los tipos de GuardDuty hallazgos con su homólogo ASFF tal y como aparecen en Security Hub CSPM.

### Note

Para algunos tipos de GuardDuty búsqueda, Security Hub CSPM asigna diferentes nombres de búsqueda de ASFF en función de si la función de recurso del detalle de búsqueda era ACTOR o TARGET. Para obtener más información, consulte [Detalles de los resultados](#).

| GuardDuty tipo de búsqueda                                | Tipo de resultado de ASFF                               |
|-----------------------------------------------------------|---------------------------------------------------------|
| <a href="#">AttackSequence:IAM/CompromisedCredentials</a> | TTPs/AttackSequence:IAM/CompromisedC<br>redentials      |
| <a href="#">AttackSequence:S3/CompromisedData</a>         | TTPs/AttackSequence:S3/CompromisedData                  |
| <a href="#">Backdoor:EC2/C&amp;CActivity.B</a>            | TTPs/Command and Control/Backdoor:EC2-<br>C&CActivity.B |

| GuardDuty tipo de búsqueda                                   | Tipo de resultado de ASFF                                             |
|--------------------------------------------------------------|-----------------------------------------------------------------------|
| <a href="#">Backdoor:EC2/C&amp;CActivity.B!DNS</a>           | TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS               |
| <a href="#">Backdoor:EC2/DenialOfService.Dns</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns             |
| <a href="#">Backdoor:EC2/DenialOfService.Tcp</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp             |
| <a href="#">Backdoor:EC2/DenialOfService.Udp</a>             | TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp             |
| <a href="#">Backdoor:EC2/DenialOfService.UdpOnTcpPorts</a>   | TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts   |
| <a href="#">Backdoor:EC2/DenialOfService.UnusualProtocol</a> | TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol |
| <a href="#">Backdoor:EC2/Spambot</a>                         | TTPs/Command and Control/Backdoor:EC2-Spambot                         |
| <a href="#">Behavior:EC2/NetworkPortUnusual</a>              | Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual                  |
| <a href="#">Behavior:EC2/TrafficVolumeUnusual</a>            | Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual                |
| <a href="#">Backdoor:Lambda/C&amp;CActivity.B</a>            | TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B                |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B</a>           | TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B               |
| <a href="#">Backdoor:Runtime/C&amp;CActivity.B!DNS</a>       | TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS           |
| <a href="#">CredentialAccess:IAMUser/AnomalousBehavior</a>   | TTPs/Credential Access/IAMUser-AnomalousBehavior                      |

| GuardDuty tipo de búsqueda                                                    | Tipo de resultado de ASFF                                                          |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <a href="#">CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed</a> | TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed                 |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller</a>                 | TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller                |
| <a href="#">CredentialAccess:Kubernetes/MaliciousIPCaller.Custom</a>          | TTPs/CredentialAccess/CredentialAccess:Kubernetes-MaliciousIPCaller.Custom         |
| <a href="#">CredentialAccess:Kubernetes/SuccessfulAnonymousAccess</a>         | TTPs/CredentialAccess/CredentialAccess:Kubernetes-SuccessfulAnonymousAccess        |
| <a href="#">CredentialAccess:Kubernetes/TorIPCaller</a>                       | TTPs/CredentialAccess/CredentialAccess:Kubernetes-TorIPCaller                      |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.FailedLogin</a>            | TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin          |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce</a>   | TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulBruteForce |
| <a href="#">CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin</a>        | TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.SuccessfulLogin      |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.FailedLogin</a>            | TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.FailedLogin          |
| <a href="#">CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin</a>        | TTPs/Credential Access/CredentialAccess:RDS-MaliciousIPCaller.SuccessfulLogin      |
| <a href="#">CredentialAccess:RDS/TorIPCaller.FailedLogin</a>                  | TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.FailedLogin                |
| <a href="#">CredentialAccess:RDS/TorIPCaller.SuccessfulLogin</a>              | TTPs/Credential Access/CredentialAccess:RDS-TorIPCaller.SuccessfulLogin            |
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B</a>                              | TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B                          |

| GuardDuty tipo de búsqueda                                          | Tipo de resultado de ASFF                                                                                                            |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CryptoCurrency:EC2/BitcoinTool.B!DNS</a>                | TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS                                                                        |
| <a href="#">CryptoCurrency:Lambda/BitcoinTool.B</a>                 | TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B<br><br>Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B</a>                | TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B                                                                        |
| <a href="#">CryptoCurrency:Runtime/BitcoinTool.B!DNS</a>            | TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS                                                                    |
| <a href="#">DefenseEvasion:EC2/UnusualDNSResolver</a>               | TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver                                                                                         |
| <a href="#">DefenseEvasion:EC2/UnusualDoHActivity</a>               | TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity                                                                                         |
| <a href="#">DefenseEvasion:EC2/UnusualDoTActivity</a>               | TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity                                                                                         |
| <a href="#">DefenseEvasion:IAMUser/AnomalousBehavior</a>            | TTPs/Defense Evasion/IAMUser-AnomalousBehavior                                                                                       |
| <a href="#">DefenseEvasion:IAMUser/BedrockLoggingDisabled</a>       | TTPs/Defense Evasion/DefenseEvasion:IAMUser-BedrockLoggingDisabled                                                                   |
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCaller</a>         | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller                                                                      |
| <a href="#">DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom</a>  | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-MaliciousIPCaller.Custom                                                               |
| <a href="#">DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess</a> | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-SuccessfulAnonymousAccess                                                              |

| GuardDuty tipo de búsqueda                                                 | Tipo de resultado de ASFF                                                       |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <a href="#">DefenseEvasion:Kubernetes/TorIPCaller</a>                      | TTPs/DefenseEvasion/DefenseEvasion:Kubernetes-TorIPCaller                       |
| <a href="#">DefenseEvasion:Runtime/FilelessExecution</a>                   | TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution                   |
| <a href="#">DefenseEvasion:Runtime/KernelModuleLoaded</a>                  | TTPs/Defense Evasion/DefenseEvasion:Runtime-KernelModuleLoaded                  |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Proc</a>               | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Proc               |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.Ptrace</a>             | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.Ptrace             |
| <a href="#">DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite</a> | TTPs/Defense Evasion/DefenseEvasion:Runtime-ProcessInjection.VirtualMemoryWrite |
| <a href="#">DefenseEvasion:Runtime/PtraceAntiDebugging</a>                 | TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging                  |
| <a href="#">DefenseEvasion:Runtime/SuspiciousCommand</a>                   | TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand                    |
| <a href="#">Discovery:IAMUser/AnomalousBehavior</a>                        | TTPs/Discovery/IAMUser-AnomalousBehavior                                        |
| <a href="#">Discovery:Kubernetes/AnomalousBehavior.PermissionChecked</a>   | TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked                   |
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller</a>                     | TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller                           |
| <a href="#">Discovery:Kubernetes/MaliciousIPCaller.Custom</a>              | TTPs/Discovery/Discovery:Kubernetes-MaliciousIPCaller.Custom                    |
| <a href="#">Discovery:Kubernetes/SuccessfulAnonymousAccess</a>             | TTPs/Discovery/Discovery:Kubernetes-SuccessfulAnonymousAccess                   |

| GuardDuty tipo de búsqueda                                              | Tipo de resultado de ASFF                                    |
|-------------------------------------------------------------------------|--------------------------------------------------------------|
| <a href="#">Discovery:Kubernetes/TorIPCaller</a>                        | TTPs/Discovery/Discovery:Kubernetes-TorIPCaller              |
| <a href="#">Discovery:RDS/MaliciousIPCaller</a>                         | TTPs/Discovery/RDS-MaliciousIPCaller                         |
| <a href="#">Discovery:RDS/TorIPCaller</a>                               | TTPs/Discovery/RDS-TorIPCaller                               |
| <a href="#">Discovery:Runtime/SuspiciousCommand</a>                     | TTPs/Discovery/Discovery:Runtime-SuspiciousCommand           |
| <a href="#">Discovery:S3/AnomalousBehavior</a>                          | TTPs/Discovery:S3-AnomalousBehavior                          |
| <a href="#">Discovery:S3/BucketEnumeration.Unusual</a>                  | TTPs/Discovery:S3-BucketEnumeration.Unusual                  |
| <a href="#">Discovery:S3/MaliciousIPCaller.Custom</a>                   | TTPs/Discovery:S3-MaliciousIPCaller.Custom                   |
| <a href="#">Discovery:S3/TorIPCaller</a>                                | TTPs/Discovery:S3-TorIPCaller                                |
| <a href="#">Discovery:S3/MaliciousIPCaller</a>                          | TTPs/Discovery:S3-MaliciousIPCaller                          |
| <a href="#">Exfiltration:IAMUser/AnomalousBehavior</a>                  | TTPs/Exfiltration/IAMUser-AnomalousBehavior                  |
| <a href="#">Execution:Kubernetes/ExecInKubeSystemPod</a>                | TTPs/Execution/Execution:Kubernetes-ExecInKubeSystemPod      |
| <a href="#">Execution:Kubernetes/AnomalousBehavior.ExecInPod</a>        | TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod        |
| <a href="#">Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed</a> | TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Custom</a>                | TTPs/Impact/Impact:EC2-MaliciousDomainRequest.Custom         |
| <a href="#">Impact:Kubernetes/MaliciousIPCaller</a>                     | TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller              |

| GuardDuty tipo de búsqueda                                                                            | Tipo de resultado de ASFF                                                                  |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <a href="#">Impact:Kubernetes/MaliciousIPCaller.Custom</a>                                            | TTPs/Impact/Impact:Kubernetes-MaliciousIPCaller.Custom                                     |
| <a href="#">Impact:Kubernetes/SuccessfulAnonymousAccess</a>                                           | TTPs/Impact/Impact:Kubernetes-SuccessfulAnonymousAccess                                    |
| <a href="#">Impact:Kubernetes/TorIPCaller</a>                                                         | TTPs/Impact/Impact:Kubernetes-TorIPCaller                                                  |
| <a href="#">Persistence:Kubernetes/ContainerWithSensitiveMount</a>                                    | TTPs/Persistence/Persistence:Kubernetes-ContainerWithSensitiveMount                        |
| <a href="#">Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount</a> | TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer</a> | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller</a>                                              | TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller                                  |
| <a href="#">Persistence:Kubernetes/MaliciousIPCaller.Custom</a>                                       | TTPs/Persistence/Persistence:Kubernetes-MaliciousIPCaller.Custom                           |
| <a href="#">Persistence:Kubernetes/SuccessfulAnonymousAccess</a>                                      | TTPs/Persistence/Persistence:Kubernetes-SuccessfulAnonymousAccess                          |
| <a href="#">Persistence:Kubernetes/TorIPCaller</a>                                                    | TTPs/Persistence/Persistence:Kubernetes-TorIPCaller                                        |
| <a href="#">Execution:EC2/MaliciousFile</a>                                                           | TTPs/Execution/Execution:EC2-MaliciousFile                                                 |
| <a href="#">Execution:ECS/MaliciousFile</a>                                                           | TTPs/Execution/Execution:ECS-MaliciousFile                                                 |
| <a href="#">Execution:Kubernetes/MaliciousFile</a>                                                    | TTPs/Execution/Execution:Kubernetes-MaliciousFile                                          |

| GuardDuty tipo de búsqueda                                     | Tipo de resultado de ASFF                                     |
|----------------------------------------------------------------|---------------------------------------------------------------|
| <a href="#">Execution:Container/MaliciousFile</a>              | TTPs/Execution/Execution:Container-MaliciousFile              |
| <a href="#">Execution:EC2/SuspiciousFile</a>                   | TTPs/Execution/Execution:EC2-SuspiciousFile                   |
| <a href="#">Execution:ECS/SuspiciousFile</a>                   | TTPs/Execution/Execution:ECS-SuspiciousFile                   |
| <a href="#">Execution:Kubernetes/SuspiciousFile</a>            | TTPs/Execution/Execution:Kubernetes-SuspiciousFile            |
| <a href="#">Execution:Container/SuspiciousFile</a>             | TTPs/Execution/Execution:Container-SuspiciousFile             |
| <a href="#">Execution:EC2/MaliciousFile!Snapshot</a>           | TTPs/Execution/Execution:EC2-MaliciousFile!Snapshot           |
| <a href="#">Execution:EC2/MaliciousFile!AMI</a>                | TTPs/Execution/Execution:EC2-MaliciousFile!AMI                |
| <a href="#">Execution:EC2/MaliciousFile!RecoveryPoint</a>      | TTPs/Execution/Execution:EC2-MaliciousFile!RecoveryPoint      |
| <a href="#">Execution:S3/MaliciousFile!RecoveryPoint</a>       | TTPs/Execution/Execution:S3-MaliciousFile!RecoveryPoint       |
| <a href="#">Execution:Runtime/MaliciousFileExecuted</a>        | TTPs/Execution/Execution:Runtime-MaliciousFileExecuted        |
| <a href="#">Execution:Runtime/MaliciousFileExecuted.Custom</a> | TTPs/Execution/Execution:Runtime-MaliciousFileExecuted.Custom |
| <a href="#">Execution:Runtime/NewBinaryExecuted</a>            | TTPs/Execution/Execution:Runtime-NewBinaryExecuted            |
| <a href="#">Execution:Runtime/NewLibraryLoaded</a>             | TTPs/Execution/Execution:Runtime-NewLibraryLoaded             |



| GuardDuty tipo de búsqueda                                    | Tipo de resultado de ASFF                                 |
|---------------------------------------------------------------|-----------------------------------------------------------|
| <a href="#">Execution:Runtime/ReverseShell</a>                | TTPs/Execution/Execution:Runtime-ReverseShell             |
| <a href="#">Execution:Runtime/SuspiciousCommand</a>           | TTPs/Execution/Execution:Runtime-SuspiciousCommand        |
| <a href="#">Execution:Runtime/SuspiciousShellCreated</a>      | TTPs/Execution/Execution:Runtime-SuspiciousShellCreated   |
| <a href="#">Execution:Runtime/SuspiciousTool</a>              | TTPs/Execution/Execution:Runtime-SuspiciousTool           |
| <a href="#">Exfiltration:S3/AnomalousBehavior</a>             | TTPs/Exfiltration:S3-AnomalousBehavior                    |
| <a href="#">Exfiltration:S3/ObjectRead.Unusual</a>            | TTPs/Exfiltration:S3-ObjectRead.Unusual                   |
| <a href="#">Exfiltration:S3/MaliciousIPCaller</a>             | TTPs/Exfiltration:S3-MaliciousIPCaller                    |
| <a href="#">Impact:EC2/AbusedDomainRequest.Reputation</a>     | TTPs/Impact:EC2-AbusedDomainRequest.Reputation            |
| <a href="#">Impact:EC2/BitcoinDomainRequest.Reputation</a>    | TTPs/Impact:EC2-BitcoinDomainRequest.Reputation           |
| <a href="#">Impact:EC2/MaliciousDomainRequest.Reputation</a>  | TTPs/Impact:EC2-MaliciousDomainRequest.Reputation         |
| <a href="#">Impact:EC2/PortSweep</a>                          | TTPs/Impact/Impact:EC2-PortSweep                          |
| <a href="#">Impact:EC2/SuspiciousDomainRequest.Reputation</a> | TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation        |
| <a href="#">Impact:EC2/WinRMBruteForce</a>                    | TTPs/Impact/Impact:EC2-WinRMBruteForce                    |
| <a href="#">Impact:IAMUser/AnomalousBehavior</a>              | TTPs/Impact/IAMUser-AnomalousBehavior                     |
| <a href="#">Impact:Runtime/AbusedDomainRequest.Reputation</a> | TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation |

| GuardDuty tipo de búsqueda                                        | Tipo de resultado de ASFF                                     |
|-------------------------------------------------------------------|---------------------------------------------------------------|
| <a href="#">Impact:Runtime/BitcoinDomainRequest.Reputation</a>    | TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation    |
| <a href="#">Impact:Runtime/CryptoMinerExecuted</a>                | TTPs/Impact/Impact:Runtime-CryptoMinerExecuted                |
| <a href="#">Impact:Runtime/MaliciousDomainRequest.Reputation</a>  | TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation  |
| <a href="#">Impact:Runtime/SuspiciousDomainRequest.Reputation</a> | TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputation |
| <a href="#">Impact:S3/AnomalousBehavior.Delete</a>                | TTPs/Impact:S3-AnomalousBehavior.Delete                       |
| <a href="#">Impact:S3/AnomalousBehavior.Permission</a>            | TTPs/Impact:S3-AnomalousBehavior.Permission                   |
| <a href="#">Impact:S3/AnomalousBehavior.Write</a>                 | TTPs/Impact:S3-AnomalousBehavior.Write                        |
| <a href="#">Impact:S3/ObjectDelete.Unusual</a>                    | TTPs/Impact:S3-ObjectDelete.Unusual                           |
| <a href="#">Impact:S3/PermissionsModification.Unusual</a>         | TTPs/Impact:S3-PermissionsModification.Unusual                |
| <a href="#">Impact:S3/MaliciousIPCaller</a>                       | TTPs/Impact:S3-MaliciousIPCaller                              |
| <a href="#">InitialAccess:IAMUser/AnomalousBehavior</a>           | TTPs/Initial Access/IAMUser-AnomalousBehavior                 |
| <a href="#">Object:S3/MaliciousFile</a>                           | TTPs/Object/Object:S3-MaliciousFile                           |
| <a href="#">PenTest:IAMUser/KaliLinux</a>                         | TTPs/PenTest:IAMUser/KaliLinux                                |
| <a href="#">PenTest:IAMUser/ParrotLinux</a>                       | TTPs/PenTest:IAMUser/ParrotLinux                              |
| <a href="#">PenTest:IAMUser/PentooLinux</a>                       | TTPs/PenTest:IAMUser/PentooLinux                              |
| <a href="#">PenTest:S3/KaliLinux</a>                              | TTPs/PenTest:S3-KaliLinux                                     |

| GuardDuty tipo de búsqueda                                           | Tipo de resultado de ASFF                                                                                          |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <a href="#">PenTest:S3/ParrotLinux</a>                               | TTPs/PenTest:S3-ParrotLinux                                                                                        |
| <a href="#">PenTest:S3/PentooLinux</a>                               | TTPs/PenTest:S3-PentooLinux                                                                                        |
| <a href="#">Persistence:IAMUser/AnomalousBehavior</a>                | TTPs/Persistence/IAMUser-AnomalousBehavior                                                                         |
| <a href="#">Persistence:IAMUser/NetworkPermissions</a>               | TTPs/Persistence/Persistence:IAMUser-NetworkPermissions                                                            |
| <a href="#">Persistence:IAMUser/ResourcePermissions</a>              | TTPs/Persistence/Persistence:IAMUser-ResourcePermissions                                                           |
| <a href="#">Persistence:IAMUser/UserPermissions</a>                  | TTPs/Persistence/Persistence:IAMUser-UserPermissions                                                               |
| <a href="#">Persistence:Runtime/SuspiciousCommand</a>                | TTPs/Persistence/Persistence:Runtime-SuspiciousCommand                                                             |
| <a href="#">Policy:IAMUser/RootCredentialUsage</a>                   | TTPs/Policy:IAMUser-RootCredentialUsage                                                                            |
| <a href="#">Policy:IAMUser/ShortTermRootCredentialUsage</a>          | TTPs/Policy:IAMUser-ShortTermRootCredentialUsage                                                                   |
| <a href="#">Policy:Kubernetes/AdminAccessToDefaultServiceAccount</a> | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AdminAccessToDefaultServiceAccount |
| <a href="#">Policy:Kubernetes/AnonymousAccessGranted</a>             | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-AnonymousAccessGranted             |
| <a href="#">Policy:Kubernetes/ExposedDashboard</a>                   | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-ExposedDashboard                   |

| GuardDuty tipo de búsqueda                                                          | Tipo de resultado de ASFF                                                                                |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <a href="#">Policy:Kubernetes/KubeflowDashboardExposed</a>                          | Software and Configuration Checks/AWS Security Best Practices/Policy:Kubernetes-KubeflowDashboardExposed |
| <a href="#">Policy:S3/AccountBlockPublicAccessDisabled</a>                          | TTPs/Policy:S3-AccountBlockPublicAccessDisabled                                                          |
| <a href="#">Policy:S3/BucketAnonymousAccessGranted</a>                              | TTPs/Policy:S3-BucketAnonymousAccessGranted                                                              |
| <a href="#">Policy:S3/BucketBlockPublicAccessDisabled</a>                           | Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled                                          |
| <a href="#">Policy:S3/BucketPublicAccessGranted</a>                                 | TTPs/Policy:S3-BucketPublicAccessGranted                                                                 |
| <a href="#">PrivilegeEscalation:IAMUser/AnomalousBehavior</a>                       | TTPs/Privilege Escalation/IAMUser-AnomalousBehavior                                                      |
| <a href="#">PrivilegeEscalation:IAMUser/AdministrativePermissions</a>               | TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions                          |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated</a> | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleBindingCreated                                 |
| <a href="#">PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated</a>        | TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-RoleCreated                                        |
| <a href="#">PrivilegeEscalation:Kubernetes/PrivilegedContainer</a>                  | TTPs/PrivilegeEscalation/PrivilegeEscalation:Kubernetes-PrivilegedContainer                              |
| <a href="#">PrivilegeEscalation:Runtime/ContainerMountsHostDirectory</a>            | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory                       |
| <a href="#">PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified</a>             | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified                        |
| <a href="#">PrivilegeEscalation:Runtime/DockerSocketAccessed</a>                    | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed                               |

| GuardDuty tipo de búsqueda                                      | Tipo de resultado de ASFF                                                       |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------|
| <a href="#">PrivilegeEscalation:Runtime/ElevationToRoot</a>     | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ElevationToRoot           |
| <a href="#">PrivilegeEscalation:Runtime/RuncContainerEscape</a> | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape       |
| <a href="#">PrivilegeEscalation:Runtime/SuspiciousCommand</a>   | Software and Configuration Checks/PrivilegeEscalation:Runtime-SuspiciousCommand |
| <a href="#">PrivilegeEscalation:Runtime/UserfaultfdUsage</a>    | TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage          |
| <a href="#">Recon:EC2/PortProbeEMRUnprotectedPort</a>           | TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort                            |
| <a href="#">Recon:EC2/PortProbeUnprotectedPort</a>              | TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort                               |
| <a href="#">Recon:EC2/Portscan</a>                              | TTPs/Discovery/Recon:EC2-Portscan                                               |
| <a href="#">Recon:IAMUser/MaliciousIPCaller</a>                 | TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller                                  |
| <a href="#">Recon:IAMUser/MaliciousIPCaller.Custom</a>          | TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom                           |
| <a href="#">Recon:IAMUser/NetworkPermissions</a>                | TTPs/Discovery/Recon:IAMUser-NetworkPermissions                                 |
| <a href="#">Recon:IAMUser/ResourcePermissions</a>               | TTPs/Discovery/Recon:IAMUser-ResourcePermissions                                |
| <a href="#">Recon:IAMUser/TorIPCaller</a>                       | TTPs/Discovery/Recon:IAMUser-TorIPCaller                                        |
| <a href="#">Recon:IAMUser/UserPermissions</a>                   | TTPs/Discovery/Recon:IAMUser-UserPermissions                                    |

| GuardDuty tipo de búsqueda                                   | Tipo de resultado de ASFF                                           |
|--------------------------------------------------------------|---------------------------------------------------------------------|
| <a href="#">ResourceConsumption:IAMUser/ComputeResources</a> | Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources |
| <a href="#">Stealth:IAMUser/CloudTrailLoggingDisabled</a>    | TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled      |
| <a href="#">Stealth:IAMUser/LoggingConfigurationModified</a> | TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified   |
| <a href="#">Stealth:IAMUser/PasswordPolicyChange</a>         | TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange           |
| <a href="#">Stealth:S3/ServerAccessLoggingDisabled</a>       | TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled         |
| <a href="#">Trojan:EC2/BlackholeTraffic</a>                  | TTPs/Command and Control/Trojan:EC2-BlackholeTraffic                |
| <a href="#">Trojan:EC2/BlackholeTraffic!DNS</a>              | TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS            |
| <a href="#">Trojan:EC2/DGADomainRequest.B</a>                | TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B              |
| <a href="#">Trojan:EC2/DGADomainRequest.C!DNS</a>            | TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS          |
| <a href="#">Trojan:EC2/DNSDataExfiltration</a>               | TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration             |
| <a href="#">Trojan:EC2/DriveBySourceTraffic!DNS</a>          | TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS             |
| <a href="#">Trojan:EC2/DropPoint</a>                         | Effects/Data Exfiltration/Trojan:EC2-DropPoint                      |
| <a href="#">Trojan:EC2/DropPoint!DNS</a>                     | Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS                  |

| GuardDuty tipo de búsqueda                                      | Tipo de resultado de ASFF                                                |
|-----------------------------------------------------------------|--------------------------------------------------------------------------|
| <a href="#">Trojan:EC2/PhishingDomainRequest!DNS</a>            | TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS            |
| <a href="#">Trojan:Lambda/BlackholeTraffic</a>                  | TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic                  |
| <a href="#">Trojan:Lambda/DropPoint</a>                         | Effects/Data Exfiltration/Trojan:Lambda-DropPoint                        |
| <a href="#">Trojan:Runtime/BlackholeTraffic</a>                 | TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic                 |
| <a href="#">Trojan:Runtime/BlackholeTraffic!DNS</a>             | TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS             |
| <a href="#">Trojan:Runtime/DGADomainRequest.C!DNS</a>           | TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS           |
| <a href="#">Trojan:Runtime/DriveBySourceTraffic!DNS</a>         | TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS              |
| <a href="#">Trojan:Runtime/DropPoint</a>                        | Effects/Data Exfiltration/Trojan:Runtime-DropPoint                       |
| <a href="#">Trojan:Runtime/DropPoint!DNS</a>                    | Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS                   |
| <a href="#">Trojan:Runtime/PhishingDomainRequest!DNS</a>        | TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS        |
| <a href="#">UnauthorizedAccess:EC2/MaliciousIPCaller.Custom</a> | TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom |
| <a href="#">UnauthorizedAccess:EC2/MetadataDNSRebind</a>        | TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind                            |
| <a href="#">UnauthorizedAccess:EC2/RDPBruteForce</a>            | TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce                 |

| GuardDuty tipo de búsqueda                                                           | Tipo de resultado de ASFF                                                                      |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| <a href="#">UnauthorizedAccess:EC2/SSHBruteForce</a>                                 | TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce                                       |
| <a href="#">UnauthorizedAccess:EC2/TorClient</a>                                     | Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient                                  |
| <a href="#">UnauthorizedAccess:EC2/TorRelay</a>                                      | Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay                                   |
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLogin</a>                              | Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin                                |
| <a href="#">UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B</a>                     | TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B                                          |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS</a>  | Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS  |
| <a href="#">UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS</a> | Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller</a>                         | TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller                                              |
| <a href="#">UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom</a>                  | TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom                                       |
| <a href="#">UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS</a> | Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-ResourceCredentialExfiltration.OutsideAWS |
| <a href="#">UnauthorizedAccess:IAMUser/TorIPCaller</a>                               | TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller                                |



| GuardDuty tipo de búsqueda                                         | Tipo de resultado de ASFF                                                   |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <a href="#">UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom</a> | TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom |
| <a href="#">UnauthorizedAccess:Lambda/TorClient</a>                | Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient            |
| <a href="#">UnauthorizedAccess:Lambda/TorRelay</a>                 | Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay             |
| <a href="#">UnauthorizedAccess:Runtime/MetadataDNSRebind</a>       | TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind                           |
| <a href="#">UnauthorizedAccess:Runtime/TorRelay</a>                | Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay            |
| <a href="#">UnauthorizedAccess:Runtime/TorClient</a>               | Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient           |
| <a href="#">UnauthorizedAccess:S3/MaliciousIPCaller.Custom</a>     | TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom                         |
| <a href="#">UnauthorizedAccess:S3/TorIPCaller</a>                  | TTPs/UnauthorizedAccess:S3-TorIPCaller                                      |

## Hallazgo típico de GuardDuty

GuardDuty envía las conclusiones al Security Hub CSPM mediante el [formato de búsqueda AWS de seguridad \(ASFF\)](#).

A continuación se muestra un ejemplo de un hallazgo típico de GuardDuty

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws:securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws:guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
```

```

"AwsAccountId": "193043430472",
"Types": [
  "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
],
"FirstObservedAt": "2020-08-22T09:15:57Z",
"LastObservedAt": "2020-09-30T11:56:49Z",
"CreatedAt": "2020-08-22T09:34:34.146Z",
"UpdatedAt": "2020-09-30T12:14:00.206Z",
"Severity": {
  "Product": 2,
  "Label": "MEDIUM",
  "Normalized": 40
},
"Title": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356.",
"Description": "199.241.229.197 is performing SSH brute force attacks against
i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
instance by guessing the SSH password.",
"SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
"ProductFields": {
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
"Unknown",
  "aws/guardduty/service/archived": "false",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
"199.241.229.197",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
  "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
  "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
"46717",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
  "aws/guardduty/service/serviceName": "guardduty",
  "aws/guardduty/service/evidence": "",
  "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
"172.31.43.6",
  "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
  "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",

```

```

    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
"INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
"SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/guardduty/
arn:aws:guardduty:us-east-1:193043430472:detector/d4b040365221be2b54a6264dc9a4bc64/
finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubect1"
      },
    },
    "Details": {
      "AwsEc2Instance": {
        "Type": "t2.micro",
        "ImageId": "ami-02354e95b39ca8dec",
        "IPv4Addresses": [
          "18.234.130.16",
          "172.31.43.6"
        ],
        "VpcId": "vpc-a0c2d7c7",
        "SubnetId": "subnet-4975b475",
        "LaunchedAt": "2020-08-03T23:21:57Z"
      }
    }
  ]
}

```

```
    }  
  }  
}  
],  
"WorkflowState": "NEW",  
"Workflow": {  
  "Status": "NEW"  
},  
"RecordState": "ACTIVE"  
}
```

## Habilitación y configuración de la integración

Para usar la integración con AWS Security Hub CSPM, debe habilitar Security Hub CSPM. Para obtener información acerca de cómo habilitar Security Hub CSPM, consulte [Configuración de Security Hub](#) en la Guía del usuario de AWS Security Hub .

Al habilitar tanto GuardDuty el CSPM como el Security Hub, la integración se habilita automáticamente. GuardDuty comienza inmediatamente a enviar los resultados al Security Hub CSPM.

## Uso de GuardDuty controles en Security Hub (CSPM)

AWS Security Hub CSPM utiliza controles de seguridad para evaluar sus AWS recursos y comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad. Puede utilizar los controles relacionados con los GuardDuty recursos y los planes de protección seleccionados. Para obtener más información, consulta [GuardDuty los controles de Amazon](#) en la Guía del AWS Security Hub usuario.

Para obtener una lista de todos los controles de los AWS servicios y recursos, consulte la [referencia de controles CSPM de Security Hub](#) en la Guía del AWS Security Hub usuario.

## Cómo detener la publicación de resultados en el CSPM de Security Hub

Para dejar de enviar resultados a Security Hub CSPM, puede utilizar la consola de Security Hub CSPM o la API.

Consulte [Deshabilitar y habilitar el flujo de hallazgos desde una integración \(consola\)](#) o [Inhabilitar el flujo de hallazgos desde una integración \(API de Security Hub, AWS CLI\)](#) en la Guía del AWS Security Hub usuario.

# Integración con Amazon Detective

[Amazon Detective](#) le ayuda a analizar e investigar rápidamente los eventos de seguridad en una o más AWS cuentas mediante la generación de visualizaciones de datos que representan la forma en que sus recursos se comportan e interactúan a lo largo del tiempo. El Detective crea visualizaciones de los GuardDuty hallazgos.

Detective recopila los detalles de resultados de todos los tipos de resultados y proporciona acceso a los perfiles de las entidades para investigar las diferentes entidades que están involucradas en el resultado. Una entidad puede ser un Cuenta de AWS AWS recurso dentro de una cuenta o una dirección IP externa que ha interactuado con sus recursos. La GuardDuty consola admite el cambio a Amazon Detective desde las siguientes entidades, según el tipo de búsqueda: Cuenta de AWS rol de IAM, usuario o sesión de rol, agente de usuario, usuario federado, instancia de Amazon EC2 o dirección IP.

## Contenido

- [Habilitación de la integración](#)
- [Pasar de un hallazgo a Amazon Detective GuardDuty](#)
- [Uso de la integración con un entorno de GuardDuty múltiples cuentas](#)

## Habilitación de la integración

Para utilizar Amazon Detective con GuardDuty , primero debes activar Amazon Detective. Para más información sobre cómo habilitar Detective, consulte [Primeros pasos con Amazon Detective](#) en la Guía de administración de Amazon Detective.

Al activar ambos GuardDuty y Detective, la integración se habilita automáticamente. Una vez activado, Detective asimilará inmediatamente los datos de tus GuardDuty hallazgos.

### Note

GuardDuty envía los hallazgos al Detective en función de la frecuencia de exportación de GuardDuty los hallazgos. De forma predeterminada, la frecuencia de exportación de las actualizaciones de los resultados existentes es de 6 horas. Para garantizar que Detective reciba las actualizaciones más recientes de sus hallazgos, se recomienda cambiar la frecuencia de exportación a 15 minutos en cada región en la que utilice Detective GuardDuty.

Para obtener más información, consulte [Paso 5: Establecer la frecuencia de exportación de los resultados activos actualizados](#).

## Pasar de un hallazgo a Amazon Detective GuardDuty

1. Inicie sesión en la <https://console.aws.amazon.com/guardduty/console>.
2. Elija un único resultado de la tabla de resultados.
3. Seleccione Investigar con Detective en el panel de detalles de los resultados.
4. Elija un aspecto del resultado para investigarlo con Amazon Detective. Esto abre la consola de Detective para ese resultado o entidad.

Si la tabla dinámica no se comporta como se esperaba, consulte [Troubleshooting the pivot](#) en la Guía del usuario de Amazon Detective.

### Note

Si archivas un GuardDuty hallazgo en la consola de Detectives, ese hallazgo también se archiva en la GuardDuty consola.

## Uso de la integración con un entorno de GuardDuty múltiples cuentas

Si gestiona un entorno de varias cuentas en GuardDuty, debe añadir sus cuentas de miembro a Amazon Detective para ver las visualizaciones de datos de Detective de los hallazgos y entidades de esas cuentas.

Se recomienda utilizar la misma cuenta de GuardDuty administrador que la cuenta de administrador de Detective. Para obtener más información sobre cómo añadir cuentas de miembros en Detective, consulte [Administración de cuentas](#) en la Guía del usuario de Amazon Detective.

### Note

Detective es un servicio regional, lo que significa que debe habilitar Detective y agregar sus cuentas de miembros en cada región en la que quiera utilizar la integración.

# Suspender o deshabilitar GuardDuty

Puedes usar la GuardDuty consola para suspender o deshabilitar el GuardDuty servicio. No se te cobrará por usarlo GuardDuty cuando el servicio esté suspendido.

- Todas las cuentas de los miembros deben disociarse o eliminarse antes de poder suspenderlas o deshabilitarlas GuardDuty.
- Si las suspende GuardDuty, dejará de supervisar la seguridad de su AWS entorno ni generará nuevos hallazgos. Sus hallazgos actuales permanecen intactos y no se ven afectados por la GuardDuty suspensión. Puedes optar por volver a activarla GuardDuty más adelante.
- Cuando la inhabilitas GuardDuty en una cuenta, solo se deshabilitará para la que esté seleccionada Región de AWS actualmente. Si desea deshabilitarla por completo GuardDuty, debe deshabilitarla en cada región en la que esté habilitada.
- Si la desactiva GuardDuty, los resultados y la GuardDuty configuración existentes se perderán y no se podrán recuperar. Si quieres guardar tus hallazgos actuales, debes exportarlos antes de confirmar la desactivación GuardDuty. Para obtener más información sobre cómo exportar resultados, consulte [Exportar los resultados generados a Amazon S3](#).
- Si has activado la protección contra malware para S3 en uno o más depósitos protegidos de tu cuenta, la suspensión o desactivación GuardDuty no afectará al estado de un depósito protegido en virtud de Malware Protection for S3. Incluso después de suspenderla o inhabilitarla GuardDuty, tu cuenta seguirá incurriendo en los costes de uso asociados a la función Malware Protection para S3. Para obtener información sobre cómo desactivar la protección contra malware para S3, consulte [Desactivar la protección contra malware para S3 para un bucket protegido](#).

Para suspender o deshabilitar GuardDuty

1. Abra la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>.
2. En el panel de navegación, seleccione Configuración.
3. En la GuardDuty sección Suspend, selecciona Suspend GuardDuty o Desactivar GuardDuty y, a continuación, confirma la acción.

Para volver a activarla GuardDuty tras la suspensión

1. Abre la GuardDuty consola en <https://console.aws.amazon.com/guardduty/>
2. En el panel de navegación, seleccione Configuración.

### 3. Elija Re-enable GuardDuty.



# Suscripción a los anuncios de Amazon GuardDuty SNS

En esta sección se proporciona información sobre la suscripción a Amazon SNS (Simple Notification Service) GuardDuty para recibir anuncios sobre tipos de búsqueda publicados recientemente, actualizaciones de los tipos de búsqueda existentes y otros cambios de funcionalidad. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS.

El GuardDuty SNS envía anuncios sobre las actualizaciones del GuardDuty servicio AWS a cualquier cuenta suscrita. Para recibir notificaciones sobre los resultados de su cuenta, consulte [Procesando GuardDuty las conclusiones con Amazon EventBridge](#).

## Note

Su usuario de IAM debe disponer de los permisos `sns::subscribe` para suscribirse a un tema de SNS.

Puede suscribir una cola de Amazon SQS a este tema de notificación, pero debe utilizar un ARN de tema que esté en la misma región. Para obtener más información, consulte [Tutorial: Subscribing an Amazon SQS queue to an Amazon SNS topic](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

También puedes usar una AWS Lambda función para activar eventos cuando se reciben notificaciones. Para obtener más información, consulte [Invocación de funciones de Lambda mediante notificaciones de Amazon SNS](#) en la Guía para desarrolladores de Amazon Simple Queue Service.

Los ARN de tema de Amazon SNS para cada región se muestran a continuación.

| Región de AWS                                   | ARN del tema de Amazon SNS                                |
|-------------------------------------------------|-----------------------------------------------------------|
| Este de EE. UU. (Norte de Virginia) – us-east-1 | arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements |
| Este de EE. UU. (Ohio) - us-east-2              | arn:aws:sns:us-east-2:118283430703:G                      |

| Región de AWS                                      | ARN del tema de Amazon SNS                                   |
|----------------------------------------------------|--------------------------------------------------------------|
| Oeste de EE. UU. (Norte de California) - us-west-1 | arn:aws:sns:us-west-1:144182107116:GuardDutyAnnouncements    |
| Oeste de EE. UU. (Oregón) - us-west-2              | arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements    |
| Canadá (Central) - ca-central-1                    | arn:aws:sns:ca-central-1:107430051933:GuardDutyAnnouncements |
| Canadá Oeste (Calgary) - ca-west-1                 | arn:aws:sns:ca-west-1:440427180217:GuardDutyAnnouncements    |
| Europa (Estocolmo) - eu-north-1                    | arn:aws:sns:eu-north-1:973841112453:GuardDutyAnnouncements   |
| Europa (Irlanda) - eu-west-1                       | arn:aws:sns:eu-west-1:965013871422:GuardDutyAnnouncements    |

| Región de AWS                           | ARN del tema de Amazon SNS                                     |
|-----------------------------------------|----------------------------------------------------------------|
| Europa (Londres) - eu-west-2            | arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements      |
| Europa (París) - eu-west-3              | arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements      |
| Europa (Fráncfort) - eu-central-1       | arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements   |
| Europa (Zúrich) - eu-central-2          | arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements   |
| Asia Pacífico (Hong Kong) - ap-east-1   | arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements      |
| Asia-Pacífico (Tokio) (ap-northeast-1 ) | arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements |
| Asia Pacífico (Seúl) - ap-northeast-2   | arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements |

| Región de AWS                             | ARN del tema de Amazon SNS                                           |
|-------------------------------------------|----------------------------------------------------------------------|
| Asia Pacífico (Singapur) - ap-southeast-1 | arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements       |
| Asia-Pacífico (Sídney) - ap-southeast-2   | arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements       |
| Asia Pacífico (Bombay) - ap-south-1       | arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements           |
| Sudamérica (São Paulo) - sa-east-1        | arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements            |
| AWS GovCloud (US-West) - us-gov-west-1    | arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements |
| China (Pekín) - cn-north-1                | arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements        |
| China (Ningxia) - cn-northwest-1          | arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements    |

| Región de AWS                                         | ARN del tema de Amazon SNS                                                  |
|-------------------------------------------------------|-----------------------------------------------------------------------------|
| Oriente Medio (Baréin) - me-south-1                   | <code>arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements</code>     |
| Oriente Medio (Emiratos Árabes Unidos) - me-central-1 | <code>arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements</code>   |
| Europa (Milán) - eu-south-1                           | <code>arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements</code>     |
| Europa (España) - eu-south-2                          | <code>arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements</code>     |
| AWS GovCloud (US-East) - us-gov-east-1                | <code>arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements</code>  |
| Asia-Pacífico (Osaka): ap-northeast-3                 | <code>arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements</code> |
| Asia-Pacífico (Yakarta) - ap-southeast-3              | <code>arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements</code> |

| Región de AWS                              | ARN del tema de Amazon SNS                                     |
|--------------------------------------------|----------------------------------------------------------------|
| Asia Pacífico (Hyderabad) - ap-south-2     | arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements     |
| Asia Pacífico (Melbourne) - ap-southeast-4 | arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements |
| Asia Pacífico (Malasia) - ap-southeast-5   | arn:aws:sns:ap-southeast-5:343218181797:GuardDutyAnnouncements |
| Israel (Tel Aviv) - il-central-1           | arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements   |
| Asia Pacífico (Tailandia) - ap-southeast-7 | arn:aws:sns:ap-southeast-7:863518448376:GuardDutyAnnouncements |
| México (Central) - mx-central-1            | arn:aws:sns:mx-central-1:060795916546:GuardDutyAnnouncements   |
| Asia-Pacífico (Taipéi) - ap-east-2         | arn:aws:sns:ap-east-2:604225987917:GuardDutyAnnouncements      |

Para suscribirse al correo electrónico de notificación de GuardDuty actualización en el Consola de administración de AWS

1. Abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
2. En la lista de regiones, elija la misma región que la del ARN del tema al que desea suscribirse. En este ejemplo se utiliza la región `us-west-2`.
3. En el panel de navegación izquierdo, elija Subscriptions (Suscripciones), Create subscription (Crear suscripción).
4. En el cuadro de diálogo Create Subscription (Crear suscripción), en Topic ARN (ARN del tema), pegue el ARN del tema: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. En Protocolo, elige Correo electrónico. En Endpoint (Punto de enlace), escriba una dirección de correo electrónico que pueda utilizar para recibir la notificación.
6. Seleccione Crear suscripción.
7. En tu aplicación de correo electrónico, abre el mensaje de AWS Notificaciones y abre el enlace para confirmar la suscripción.

El navegador web muestra una respuesta de confirmación de Amazon SNS.

Para suscribirse al correo electrónico de notificación de GuardDuty actualización con el AWS CLI

1. Ejecute el siguiente comando con la AWS CLI:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. En tu aplicación de correo electrónico, abre el mensaje de AWS Notificaciones y abre el enlace para confirmar la suscripción.

El navegador web muestra una respuesta de confirmación de Amazon SNS.

## Formato de los mensajes de Amazon SNS

Un ejemplo de mensaje de notificación GuardDuty general:

```
{
```

```

    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\", \"type\":\"GENERAL\", \"message\": [{ \"title\": \"Updated AmazonGuardDutyFullAccess_v2 policy\", \"body\": \"Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.\", \"links\": [ \"https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmaonGuardDutyFullAccess-v2\" ] ] }\",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCQaeBG7HZhR1AbpyVka7JSNR0/6ssyrljlg==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
  }

```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```

{
  "version": "1",
  "type": "GENERAL",
  "message": [
    {
      "title": "Updated AmazonGuardDutyFullAccess policy",
      "body": "Added permission that allows you to pass an IAM role to GuardDuty when you enable Malware Protection for S3.",
      "links": [
        "https://docs.aws.amazon.com//guardduty/latest/ug/security-iam-awsmanpol.html#security-iam-awsmanpol-AmaonGuardDutyFullAccess-v2"
      ]
    }
  ]
}

```

A continuación se muestra un ejemplo de mensaje de notificación de GuardDuty actualización sobre nuevos hallazgos:



```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FINDINGS\", \"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\", \"findingDescription\":\"This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance is acting as a client on a Tor network. A common use for a Tor client is to circumvent network monitoring and filter for access to unauthorized or illicit content. Tor clients can also generate nefarious Internet traffic, including attacking SSH servers. This activity can indicate that your EC2 instance is compromised.\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCtPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrljlg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
  "version": "1",
  "type": "NEW_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "findingDescription": "This finding informs you that an EC2 instance in your AWS environment is making connections to a Tor Guard or an Authority node. Tor is software for enabling anonymous communication. Tor Guards and Authority nodes act as initial gateways into a Tor network. This traffic can indicate that this EC2 instance
```

```
is acting as a client on a Tor network. A common use for a Tor client is to circumvent
network monitoring and filter for access to unauthorized or illicit content. Tor
clients can also generate nefarious Internet traffic, including attacking SSH servers.
This activity can indicate that your EC2 instance is compromised."
```

```
  ]]
}
```

A continuación se muestra un ejemplo de mensaje de notificación de GuardDuty actualización sobre las actualizaciones de GuardDuty funciones:

```
{
  "Type" : "Notification",
  "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message" : "{\"version\":\"1\", \"type\":\"NEW_FEATURES\", \"featureDetails\": [{\"featureDescription\":\"Customers with high-volumes of global CloudTrail events should see a net positive impact on their GuardDuty costs.\"}, {\"featureLink\":\"https://docs.aws.amazon.com/guarddduty/latest/ug/guarddduty_data-sources.html#guarddduty_controlplane\"}]}",
  "Timestamp" : "2018-03-09T00:25:43.483Z",
  "SignatureVersion" : "1",
  "Signature" : "XWox8GDGLRiCgD0Xlo/fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblsdea3BjqdChcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS+4AQD/V/QjrhsEnlj+GaiW+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7HpV/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI+BVvkin6AL7PhksvdQ7FAGHfXsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```
{
  "version": "1",
  "type": "NEW_FEATURES",
  "featureDetails": [{
    "featureDescription": "Customers with high-volumes of global CloudTrail events
    should see a net positive impact on their GuardDuty costs.",
```

```

    "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_controlplane"
  ]]
}

```

A continuación, se muestra un ejemplo GuardDuty de mensaje de notificación de actualización sobre los resultados actualizados:

```

{
  "Type": "Notification",
  "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
  "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
  "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
  \"findingDetails\": [{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\", \"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
  \"description\":\"Increased severity value from 5 to 8.\"}]]\",
  "Timestamp": "2018-03-09T00:25:43.483Z",
  "SignatureVersion": "1",
  "Signature": "XWox8GDGLRiCgD0Xlo/
fG9Lu/88P8S0FL6M6oQY0mUFzkucuhoblSdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6Gop0zFGnCTPMR0jCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDksc0tPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAGhFxsit+6p8Gy0vKCqaeBG7HZhR1AbpyVka7JSNR0/6ssyrlj1g==",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
  "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}

```

El valor Mensaje analizado (sin las comillas de escape) se muestra a continuación:

```

{
  "version": "1",
  "type": "UPDATED_FINDINGS",
  "findingDetails": [{
    "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
    "findingType": "UnauthorizedAccess:EC2/TorClient",
    "description": "Increased severity value from 5 to 8."
  }]
}

```

```
}
```

# GuardDuty Cuotas de Amazon

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es Region-specific. Puede solicitar aumentos para algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas GuardDuty, abra la [consola Service Quotas](#). En el panel de navegación, elige Servicios de AWSy selecciona Amazon GuardDuty.

Para solicitar un aumento de cuota, consulte [Solicitud de un aumento de cuota](#) en la Guía de usuario de Service Quotas.

Tienes Cuenta de AWS las siguientes cuotas de Amazon GuardDuty por región.

## Note

- Para conocer las cuotas específicas de GuardDuty Malware Protection para EC2, consulte [Cuotas en la protección contra malware de EC2](#).
- Para conocer las cuotas específicas de la protección contra malware para S3, consulte [Cuotas en la protección contra malware para S3](#).

## GuardDuty cuotas por región

| Recurso    | Valor predeterminado | Comentarios                                                                                                                                   |
|------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Detectores | 1                    | <p>El número máximo de recursos del detector que puede crear por cuenta de AWS por región.</p> <p>No puede solicitar un aumento de cuota.</p> |
| Filtros    | 100                  | El número máximo de filtros guardados por AWS cuenta y región.                                                                                |

| Recurso                                                                  | Valor predeterminado | Comentarios                                                                                                                                                                     |
|--------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                          |                      | No puede solicitar un aumento de cuota.                                                                                                                                         |
| Periodo de conservación de resultados                                    | 90 días              | <p>El número máximo de días que se guarda un resultado.</p> <p>No puede solicitar un aumento de cuota.</p>                                                                      |
| Direcciones IP y rangos de CIDR por lista de direcciones IP de confianza | 2,000                | <p>Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una misma lista de direcciones IP de confianza.</p> <p>No puede solicitar un aumento de cuota.</p> |
| Direcciones IP y rangos de CIDR por lista de direcciones IP de amenazas  | 250.000              | <p>Número máximo de direcciones IP y rangos de CIDR que se pueden incluir en una lista de direcciones IP de amenazas.</p> <p>No puede solicitar un aumento de cuota.</p>        |

| Recurso                                       | Valor predeterminado | Comentarios                                                                                                                                                    |
|-----------------------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lista de entidades por amenaza                | 1 000                | <p>El número máximo de entidades que puede incluir en una sola lista de entidades de amenaza.</p> <p>No puede solicitar un aumento de cuota.</p>               |
| Entidades por lista de entidades de confianza | 1 000                | <p>El número máximo de entidades que puede incluir en una lista de entidades de confianza.</p> <p>No puede solicitar un aumento de cuota.</p>                  |
| Tamaño máximo de archivo                      | 35 MB                | <p>El tamaño máximo del archivo utilizado para cargar una lista de entidades o una lista de direcciones IP.</p> <p>No puede solicitar un aumento de cuota.</p> |
| Cuentas de los miembros (por invitación)      | 5000                 | <p>El número máximo de cuentas de miembro asociadas a una cuenta de administrador.</p> <p>No puede solicitar un aumento de cuota.</p>                          |

| Recurso             | Valor predeterminado | Comentarios                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cuentas de miembros | 50 000               | <p>El número máximo de cuentas de miembro asociadas a una cuenta de administrador a través de AWS Organizations. Esto incluye las cuentas de miembro que se agregan a la organización mediante invitación.</p> <p>Este valor predeterminado depende de la cuota actual para las cuentas de miembro en AWS Organizations. La cantidad de cuentas de miembros GuardDuty que se agreguen no AWS Organizations puede superar la cantidad de cuentas de miembros de su organización. Para obtener información sobre el número de Cuentas de AWS de miembros de una organización, consulte <a href="#">los valores máximo y mínimo</a> en la Guía del</p> |



| Recurso                                                           | Valor predeterminado | Comentarios                                                                                                                                                              |
|-------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                   |                      | AWS Organizations usuario.                                                                                                                                               |
| Conjuntos de información sobre amenazas (lista de direcciones IP) | 6                    | <p>Número máximo de listas de direcciones IP de amenazas que puede añadir por Cuenta de AWS y por región.</p> <p>No puede solicitar un aumento de cuota.</p>             |
| Conjuntos de IP de confianza (lista de direcciones IP)            | 1                    | <p>El número máximo de listas de direcciones IP de confianza que se pueden cargar y activar Cuenta de AWS por región.</p> <p>No puede solicitar un aumento de cuota.</p> |
| Listas de entidades de amenazas                                   | 6                    | <p>Número máximo de listas de entidades de amenazas que se pueden añadir por Cuenta de AWS y por región.</p> <p>No puede solicitar un aumento de cuota.</p>              |

| Recurso                         | Valor predeterminado | Comentarios                                                                                                                                                         |
|---------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lista de entidades de confianza | 1                    | <p>El número máximo de listas de entidades de confianza que se pueden cargar y activar Cuenta de AWS por región.</p> <p>No puede solicitar un aumento de cuota.</p> |

# GuardDuty Managed Instances Support

En la siguiente tabla se indica el soporte que GuardDuty ofrecen sus distintas funciones para los distintos tipos de instancias administradas.

| Tipo de función administrada                                    | Soporte <a href="#">de monitoreo de tiempo de ejecución</a> | <a href="#">Protección contra malware para compatibilidad con EC2</a> |
|-----------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------|
| <a href="#">Modo automático de Amazon EKS</a>                   | Soportado                                                   | compatible                                                            |
| <a href="#">Instancia AWS Fargate gestionada por Amazon ECS</a> | No se admite                                                | compatible                                                            |
| <a href="#">Instancia gestionada por Lambda</a>                 | No se admite                                                | No se admite                                                          |

# Solución de problemas de Amazon GuardDuty

Cuando recibas problemas relacionados con la realización de una acción específica GuardDuty, consulta los temas de esta sección.

## Temas

- [Exportar resultados a Amazon S3: error de acceso](#)
- [Problemas de la protección contra malware para EC2](#)
- [Problemas de supervisión en tiempo de ejecución](#)
- [Otras cuestiones de solución de problemas](#)

## Exportar resultados a Amazon S3: error de acceso

Cuando exporta GuardDuty los resultados a un bucket de Amazon S3 (destino de publicación), si no puede acceder a este destino de publicación, GuardDuty es posible que se produzca un error de acceso.

Tras configurar los ajustes para exportar los resultados, si no GuardDuty es posible exportarlos, se mostrará un mensaje de error en la página de configuración de la GuardDuty consola. Esto puede suceder potencialmente cuando ya no GuardDuty pueda acceder al recurso de destino. Por ejemplo, si el bucket de Amazon S3 se ha eliminado o se ha modificado el permiso de acceso al bucket. Esto también puede ocurrir cuando ya no GuardDuty pueda acceder a la AWS KMS clave que se utilizó para cifrar los datos de su bucket de Amazon S3. Cuando GuardDuty no puede exportar, envía una notificación al correo electrónico asociado a la cuenta para proporcionar información sobre este problema.

### ¿Cómo se resuelve el error de acceso?

Para resolver el problema, asegúrate de que existan los recursos correspondientes y de GuardDuty que tengas los permisos para acceder a los recursos necesarios.

Para obtener más información, consulte [Exportar los resultados generados a Amazon S3](#).

### ¿Qué ocurre si no se resuelve este error?

Si no resuelve el problema antes de que finalice el período de retención de hallazgos de 90 días GuardDuty, sus hallazgos no se exportarán. GuardDuty impedirá encontrar la configuración de exportación de esta cuenta en la región específica.

Para volver a exportar resultados, actualice los parámetros de configuración de la región en cuestión.

## Problemas de la protección contra malware para EC2

En esta sección se describen los errores que podría experimentar al configurar o utilizar la protección contra malware para EC2.

### Falta el permiso AWS Organizations de administración necesario al habilitar el análisis de GuardDuty-initiated malware

Si desea administrar varias cuentas mediante el uso AWS Organizations y aparece este error `The request failed because you do not have required AWS Organization master permission.`, significa que le falta el permiso para habilitar el análisis de GuardDuty-initiated malware en varias cuentas de su organización.

Para obtener información sobre la concesión de permisos a la cuenta de administración, consulte [Establecer un acceso confiable para permitir la detección de GuardDuty-initiated malware](#).

Estoy iniciando un análisis de On-demand software malicioso, pero se produce un error de falta de permisos necesarios.

Si recibe un error que indica que no tiene los permisos necesarios para iniciar un análisis de On-demand malware en una instancia de Amazon EC2, compruebe que ha adjuntado la [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) política a su función de IAM.

Si es miembro de una AWS organización y sigue apareciendo el mismo error, conéctese con su cuenta de administración. Para obtener más información, consulte [AWS Organizations SCP: acceso denegado](#).

Recibo un error **iam:GetRole** al trabajar con la protección contra malware para EC2.

Si recibes este error `Unable to get role:`

`AWSServiceRoleForAmazonGuardDutyMalwareProtection`, significa que te falta el permiso para activar GuardDuty-initiated o utilizar el análisis de On-demand malware. Compruebe que ha adjuntado la política [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) a su rol de IAM.

Soy un GuardDuty administrador de cuentas que necesito habilitar el escaneo de GuardDuty-initiated malware, pero no uso una política AWS administrada: AmazonGuardDutyFullAccess administrar GuardDuty.

- Configura la función de IAM que utilizas GuardDuty para disponer de los permisos necesarios para activar el análisis de GuardDuty-initiated malware. Para obtener más información sobre los permisos necesarios, consulte [Crear un rol vinculado al servicio para la protección contra malware para EC2](#).
- Adjunte [AWS política gestionada: AmazonGuardDutyFullAccess\\_v2 \(recomendada\)](#) al rol de IAM. Esto te ayudará a habilitar la detección de GuardDuty-initiated malware en las cuentas de los miembros.

## Problemas de supervisión en tiempo de ejecución

En esta sección se describen los errores que se pueden producir al configurar o utilizar la Supervisión en tiempo de ejecución.

## Problemas de cobertura en tiempo de ejecución

Cuando la cobertura del tiempo de ejecución de los recursos protegidos deja de estar dañada, la GuardDuty consola proporciona el tipo de problema exacto. Una vez que conozca el tipo de problema, utilice los siguientes documentos para conocer los pasos de solución de problemas correspondientes a cada tipo de recurso admitido:

- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EC2](#)
- [Solución de problemas de cobertura en ECS-Fargate tiempo de ejecución de Amazon](#)
- [Resolución de problemas de cobertura en tiempo de ejecución de Amazon EKS](#)

## Solución de problemas de error de memoria insuficiente en la Supervisión en tiempo de ejecución (solo compatible con Amazon EC2)

En esta sección se describen los pasos de solución de problemas cuando se produce un error de memoria insuficiente debido [Límite de CPU y memoria](#) a la implementación manual del agente de GuardDuty seguridad.

Si systemd cancela el GuardDuty agente debido a out-of-memory un problema y considera que es razonable proporcionarle más memoria, puede actualizar el límite. GuardDuty

1. Con el permiso de raíz, abra `/lib/systemd/system/amazon-guardduty-agent.service`.
2. Busque `MemoryLimit` y `MemoryMax`, y actualice ambos valores.

```
MemoryLimit=256M
MemoryMax=256M
```

3. Tras actualizar los valores, reinicie el GuardDuty agente mediante el siguiente comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Ejecute el siguiente comando para ver el estado:

```
sudo systemctl status amazon-guardduty-agent
```

La salida esperada mostrará el nuevo límite de memoria:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

## Mi AWS Step Functions flujo de trabajo está fallando inesperadamente

Si el GuardDuty contenedor contribuyó al error del flujo de trabajo, consulte [Solución de problemas de cobertura en ECS-Fargate tiempo de ejecución de Amazon](#). Si el problema persiste, para evitar que el flujo de trabajo falle a causa del GuardDuty contenedor, lleve a cabo uno de los siguientes pasos:

- Agregue la etiqueta `GuardDutyManaged:false` al clúster de Amazon ECS asociado.
- Deshabilite la configuración automática del agente AWS Fargate (solo para ECS) a nivel de cuenta. Añada la etiqueta de inclusión `GuardDutyManaged: true` al clúster de Amazon ECS asociado que desee seguir supervisando con el agente GuardDuty automatizado.

## Otras cuestiones de solución de problemas

Si no encuentra un escenario adecuado para su problema, consulte las siguientes opciones de solución de problemas:

- Para obtener información sobre problemas generales de IAM al acceder al <https://console.aws.amazon.com/guardduty/>, consulte [Solución de problemas de GuardDuty identidad y acceso a Amazon](#).
- Para obtener información sobre problemas de autenticación y autorización al acceder AWS AWS Console Home, consulte [Solución de problemas de IAM](#).



# GuardDuty Regiones y puntos de conexión de Amazon

Para ver Regiones de AWS dónde GuardDuty está disponible Amazon, consulta los [GuardDuty puntos de enlace de Amazon](#) en. Referencia general de Amazon Web Services

Le recomendamos que habilite todas GuardDuty las opciones compatibles Regiones de AWS. Esto permite GuardDuty generar información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utiliza activamente. Esto también permite GuardDuty monitorear AWS CloudTrail los eventos para las personas con soporte Regiones de AWS, y reduce su capacidad para detectar actividades que involucren servicios globales.

## Region-specific disponibilidad de funciones

Una lista de las diferencias regionales para especificar la disponibilidad de las GuardDuty funciones.

Campos filtrables ampliados para y CreateFilter UpdateFilter

Los [campos filtrables adicionales](#) para las reglas y filtros de supresión solo están disponibles en la AWS partición (). aws En otras particiones, puede seguir utilizando los campos compatibles con la consola.

ListFindings y las API GetFindingsStatistics

Las API [GetFindingsStatistics](#) y [ListFindings](#) tienen una marca consoleOnly temporal. Cuando se utiliza una de estas API o ambas, la marca consoleOnly significa que la API puede obtener resultados hasta un límite máximo de 1000.

Malware Protection for EC2

GuardDuty admite la [Malware Protection for EC2](#) función en las [Zonas Locales AWS Dedicadas](#).

Protección de RDS

La protección de RDS no se admite en la región Asia Pacífico (Taipéi) (ap-east-2).

La protección RDS no se admite en las Zonas Locales AWS Dedicadas.

Tipo de búsqueda de IAM: [CredentialAccess:IAMUser/CompromisedCredentials](#)

El tipo de CredentialAccess:IAMUser/CompromisedCredentials búsqueda no se admite en las siguientes regiones.

| Región de AWS          | Código de región |
|------------------------|------------------|
| AWS GovCloud (US-West) | us-gov-west-1    |
| AWS GovCloud (US-East) | us-gov-east-1    |
| China (Pekín)          | cn-north-1       |
| China (Ningxia)        | cn-northwest-1   |

Tipo de búsqueda de IAM: [DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)

El tipo de DefenseEvasion:IAMUser/BedrockLoggingDisabled hallazgo no se admite en la región Asia Pacífico (Hong Kongap-east-1) ().

Compatibilidad general de la API

Las siguientes API de la Amazon GuardDuty API Reference pueden tener diferencias regionales debido a la falta de disponibilidad de algunas de las fuentes de datos o características especificadas Regiones de AWS anteriormente:

- [CreateDetector](#)
- [UpdateDetector](#)
- [UpdateMemberDetectors](#)
- [UpdateOrganizationConfiguration](#)
- [GetDetector](#)
- [GetMemberDetectors](#)
- [DescribeOrganizationConfiguration](#)

Tipos de resultados de Amazon EC2: [DefenseEvasion:EC2/UnusualDoHActivity](#) y [DefenseEvasion:EC2/UnusualDoTActivity](#)

En la siguiente tabla se muestra Regiones de AWS dónde GuardDuty está disponible, pero estos dos tipos de búsqueda de Amazon EC2 aún no son compatibles.

| Región de AWS        | Código de región |
|----------------------|------------------|
| Asia-Pacífico (Seúl) | ap-northeast-2   |

| Región de AWS           | Código de región |
|-------------------------|------------------|
| Asia-Pacífico (Osaka)   | ap-northeast-3   |
| Asia-Pacífico (Yakarta) | ap-southeast-3   |

### AWS GovCloud (US) Regiones

Para obtener la información más reciente, consulta [Amazon GuardDuty](#) en la Guía AWS GovCloud (US) del usuario.

### Regiones de China

Para obtener información más actualizada, consulte [Feature availability and implementation differences](#).

# GuardDuty acciones y parámetros heredados

Amazon GuardDuty ha dejado en desuso algunas de las acciones y parámetros de la API, pero aún los admite. La práctica recomendada consiste en utilizar las acciones y los parámetros nuevos de la API que sustituyen a las opciones heredadas. En la tabla siguiente se comparan las acciones y los parámetros heredados y los nuevos.

| Legado actions/parameters                                                                                                   | Nuevo actions/parameters                             | Comparación                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">DisassociateFromMasterAccount</a>                                                                               | <a href="#">DisassociateFromAdministratorAccount</a> | Con la misma implementación en ambas acciones, GuardDuty utiliza el término Administrator en DisassociateFromAdministratorAccount.                                                                                                                                                                                                                                                                                                                                |
| autoEnable parámetro en <a href="#">DescribeOrganizationConfiguration</a> y <a href="#">UpdateOrganizationConfiguration</a> | <a href="#">autoEnableOrganizationMembers</a>        | Con autoEnableOrganizationMembers, la cuenta de GuardDuty administrador puede auditar y aplicar cualquiera de los valores GuardDuty para todas las cuentas de los miembros. Con la API, la actualización de la configuración de todas las cuentas de miembros puede tardar hasta 24 horas en efectuarse. Para obtener más información sobre los valores posibles del autoEnableOrganizationMembers campo, consulte <a href="#">auto EnableOrganizationMembers</a> |
| Parámetro dataSource en las API que figuran                                                                                 | <a href="#">features</a>                             | A partir de marzo de 2023, podrá configurar <a href="#">GuardDuty Protección contra malware para EC2</a> y utilizar los nuevos planes de GuardDuty protección features. Los planes de                                                                                                                                                                                                                                                                             |

| Legado actions/parameters                                        | Nuevo actions/parameters | Comparación                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">en GuardDuty Cambios en la API en marzo de 2023.</a> |                          | protección lanzados antes de marzo de 2023, incluida la protección contra malware para EC2, aún admiten la configuración mediante <code>dataSources</code> . Si utiliza las API para configurar un plan de protección, cada solicitud a la API puede incluir <code>dataSources</code> o <code>features</code> , pero no ambas opciones. |

# Historial de documentos de Amazon GuardDuty

En la siguiente tabla se describen los cambios importantes en la documentación desde la última versión de la Guía del GuardDuty usuario de Amazon. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

| Cambio                                                                       | Descripción                                                                                                                                                                                                                | Fecha              |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">Funcionalidad actualizada: búsqueda de criterios de filtrado</a> | Se han eliminado los campos no admitidos de la lista de criterios de filtrado de búsqueda. Para obtener más información, consulte <a href="#">Filtrar los resultados en GuardDuty</a> .                                    | 29 de mayo de 2026 |
| <a href="#">Se retiraron dos tipos de hallazgos</a>                          | Los tipos de <a href="#">Persisten</a><br><a href="#">ce:Kubernetes/ContainerWithSensitiveMount</a> búsqueda <a href="#">PrivilegeEscalation:Kubernetes/PrivilegedContainer</a> y búsqueda se han retirado.                | 29 de mayo de 2026 |
| <a href="#">Funcionalidad actualizada: Runtime Monitoring</a>                | GuardDuty Supervisión del tiempo de ejecución Se agregó soporte para la versión 1.36 de Kubernetes. Para obtener más información, consulte <a href="#">Requisitos previos</a> para la supervisión del tiempo de ejecución. | 28 de mayo de 2026 |
| <a href="#">Funcionalidad actualizada: Runtime Monitoring</a>                | GuardDuty Runtime Monitorin g lanza la nueva versión 1.15.0 del agente de seguridad para los recursos de Amazon ECS.AWS Fargate Para obtener más informaci                                                                 | 28 de mayo de 2026 |

ón sobre la nueva versión del agente y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

Funcionalidad actualizada:  
Detección Extendida de  
Amenazas

GuardDuty La detección extendida de amenazas añade cinco nuevos tipos de indicadores a los detalles de búsqueda de la secuencia de ataques: MALICIOUS\_PACKAGE, MISCONFIGURATION, REACHABILITY, SENSITIVE\_DATA y VULNERABILITY. [Para obtener más información, consulte Detalles de búsqueda de secuencias de ataques.](#)

20 de mayo de 2026

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.15.0 del agente de seguridad para los recursos de Amazon EKS y Amazon EC2. Para obtener más información sobre la nueva versión del agente y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de lanzamiento del [agente GuardDuty de seguridad](#).

14 de mayo de 2026

### [Actualizado AmazonGuardDutyServiceRolePolicy](#)

Se agregaron `s3:ListBucket` y `ecs:DescribeTaskDefinition` permisos para el rol GuardDuty vinculado al servicio. `ecs:DescribeTasks` Para obtener más información, consulte [GuardDuty las actualizaciones de las políticas AWS administradas.](#)

23 de abril de 2026

### [Funcionalidad actualizada: Runtime Monitoring](#)

GuardDuty Runtime Monitoring lanza la nueva versión 1.12.2 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre la nueva versión del agente y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad.](#)

22 de abril de 2026

### [Funcionalidad actualizada: campos filtrables ampliados](#)

GuardDuty ahora admite el filtrado de cualquier campo de búsqueda al crear o actualizar las reglas de supresión. Los campos de marca de tiempo aceptan valores en formato Unix Epoch de milisegundos. [Para obtener más información, consulte Filtrar los resultados en. GuardDuty](#)

20 de abril de 2026



Funcionalidad actualizada:  
protección contra malware  
para S3

La EventBridge notificación de los resultados del escaneo de objetos de S3 ahora incluye un `statusReasons` campo `scanResultDetails` cuando se omite un escaneo. Este campo proporciona el motivo específico por el que se omitió el escaneo. Para obtener más información, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

10 de abril de 2026

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.9.2 del agente de seguridad para los recursos de Amazon EC2. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

3 de abril de 2026

### [Actualizado AmazonGuardDutyServiceRolePolicy](#)

Se agregó el `cloudtrail:CreateServiceLinkedChannel` permiso para habilitar un mecanismo adicional para consumir AWS CloudTrail eventos. Para obtener más información, consulte [GuardDuty las actualizaciones de las políticas AWS gestionadas](#).

25 de marzo de 2026

### [Funcionalidad actualizada: Runtime Monitoring](#)

GuardDuty Supervisión del tiempo de ejecución Se agregó soporte para la versión 1.35 de Kubernetes. Para obtener más información, consulte [Requisitos previos](#) para la supervisión del tiempo de ejecución.

20 de marzo de 2026

### [La nueva política de acceso total con alcance reducido AmazonGuardDutyFullAccess\\_v2 reemplaza AmazonGuardDutyFullAccess](#)

A partir del 13 de marzo de 2026, la política GuardDuty quedó obsoleta y la sustituyó por una AmazonGuardDutyFullAccess política de ámbito limitado denominada «Política de ámbito limitado». AmazonGuardDutyFullAccess\_v2 Para obtener más información, consulta la política [AWS gestionada: \\_v2](#). AmazonGuardDutyFullAccess

13 de marzo de 2026

Nuevo tipo de resultado:[CredentialAccess:IAMUser/CompromisedCredentials](#)

GuardDuty Introduce un nuevo tipo de búsqueda que detecta cuándo se utiliza una clave de acceso de IAM que se considera potencialmente comprometida para invocar las operaciones de la API. AWS Para obtener más información, consulte [CredentialAccess:IAMUser/CompromisedCredentials](#).

6 de marzo de 2026

Nuevo tipo de resultado:[UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#)

GuardDuty presenta un nuevo tipo de búsqueda que detecta cuando un host externo AWS intenta ejecutar operaciones de AWS API con AWS credenciales temporales que se crearon en un AWS Lambda recurso de su AWS entorno. Para obtener más información, consulte [UnauthorizedAccess:IAMUser/ResourceCredentialExfiltration.OutsideAWS](#).

16 de diciembre de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.9.1 del agente de seguridad para los recursos de Amazon EC2. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

2 de diciembre de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.12.1 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre la nueva versión del agente y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

2 de diciembre de 2025

Funcionalidad actualizada:  
Detección Extendida de  
Amenazas

GuardDuty Extended Threat Detection presenta dos nuevos tipos de búsqueda de secuencias de ataques que ayudan a detectar ataques en varias etapas que involucran instancias de Amazon EC2 y clústeres de Amazon ECS comprometidos. [AttackSequence:EC2/CompromisedInstanceGroupAttackSequence:ECS/CompromisedCluster](#) Habilite la supervisión del tiempo de ejecución para [maximizar la detección de amenazas](#). Para obtener más información, consulte [Tipos de búsqueda de secuencias de ataques](#).

2 de diciembre de 2025

Nueva función: los comodines  
en las reglas de supresión

GuardDuty ha mejorado sus capacidades de supresión con la introducción de partidas y NotMatches condiciones que admiten comodines. Los clientes ahora pueden usar \* (para hacer coincidir cualquier número de caracteres) y ? (para que coincida como máximo con 1 carácter) como comodín al crear reglas de supresión. [Reglas de supresión](#).

2 de diciembre de 2025

[Nueva función: Amazon CloudWatch Usage Metrics Support](#)

GuardDuty introduce la publicación de métricas de uso en Amazon CloudWatch para todos los planes de protección, lo que permite a los clientes supervisar el uso. Para obtener más información, consulte [Supervisión del GuardDuty uso y estimación de los costes](#)

25 de noviembre de 2025

[Nuevo tipo de resultado: DefenseEvasion:IAMUser/BedrockLoggingDisabled](#)

GuardDuty presenta un nuevo tipo de hallazgo que detecta cuando el registro de invocaciones del modelo Amazon Bedrock está deshabilitado, lo que puede indicar intentos de evadir la detección de la actividad de la carga de trabajo de la IA. Para obtener más información, consulte [DefenseEvasion:IAM User/BedrockLoggingDisabled](#)

21 de noviembre de 2025

### [Nueva función: Malware Protection for Backup](#)

GuardDuty Malware Protection for Backup ya está disponible en todas las regiones comerciales en las que GuardDuty esté disponible. Esta función le ayuda a detectar la posible presencia de malware en sus recursos de backup mediante escaneos completos e incrementales de las instantáneas de Amazon EBS, las AMI de EC2 y los puntos de recuperación. Para obtener más información sobre esta función, consulte [Malware Protection for Backup](#).

19 de noviembre de 2025

### [Cambie a AmazonGuardDutyFullAccess y AmazonGuardDutyFullAccess\\_V2](#)

Se agregó un permiso que le permite transferir una función de IAM GuardDuty al habilitar Malware Protection for Backup.

19 de noviembre de 2025

### [Nueva función: protección contra malware para el escaneo bajo demanda de S3.](#)

GuardDuty anuncia Scan on Demand for Malware Protection para S3. Con esta función, puede utilizar la nueva SendObjectMalwareScan API para activar escaneos de cualquier objeto que ya esté almacenado en sus depósitos de S3. Para obtener más información, consulte el análisis de [malware de S3 bajo demanda](#).

17 de noviembre de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.9.0 del agente de seguridad para los AWS Fargate recursos de Amazon ECS. Para obtener información sobre las nuevas versiones de los agentes de seguridad y una lista de recursos adicionales para actualizar su agente de seguridad, consulte [las versiones de lanzamiento del agente de GuardDuty seguridad](#).

28 de octubre de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.9.0 del agente de seguridad para los recursos de Amazon EC2. Para obtener información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

23 de octubre de 2025



[Nuevo tipo de resultado  
s de Runtime Monitoring:  
DefenseEvasion:Runtime/Kern  
elModuleLoaded](#)

GuardDuty Runtime Monitorin  
g presenta un nuevo tipo de  
descubrimiento que ayuda  
a identificar las técnicas de  
evasión de la defensa en las  
que los actores de amenazas  
utilizan los módulos del núcleo  
para eludir los controles  
de seguridad, modificar las  
operaciones del sistema y  
obtener acceso persisten  
te al sistema. Para obtener  
más información, consulte  
[DefenseEvasion:Runtime/Kern  
elModuleLoaded](#).

15 de octubre de 2025

[Funcionalidad actualizada:  
Runtime Monitoring](#)

Se agregó compatibilidad con  
la versión 1.34 de Kuberne  
te para las distribuciones del  
sistema operativo y la versión  
del agente de seguridad  
para los recursos de Role  
GuardDuty SageMaker  
Manager para Amazon EKS.  
Para obtener más información,  
consulte [Validar los requisito  
s de arquitectura de Amazon  
EKS](#).

3 de octubre de 2025

Se agregó una guía de solución de problemas para las bases de datos de Amazon RDS???

Se agregó una guía para resolver los problemas de las bases de datos de RDS que pueden afectar a las capacidades de monitoreo de GuardDuty RDS Protection, incluidos el storage-full estado y los requisitos de réplica de lectura de RDS para PostgreSQL. Para obtener más información, consulte [Solución de problemas del monitoreo de RDS Protection](#).

15 de septiembre de 2025

[Funcionalidad actualizada:](#)  
[Runtime Monitoring](#)

Se agregó la distribución Ubuntu Noble OS compatible con las versiones 6.13 y 6.14 del kernel para GuardDuty Runtime Monitoring para Amazon EC2. Para obtener información sobre la versión del agente de EC2 compatible con esta distribución de sistema operativo, consulte [Validar los requisitos de arquitectura de Amazon EC2](#).

13 de septiembre de 2025

[Funcionalidad actualizada:](#)  
[RDS Protection](#)

Se agregó compatibilidad con PostgreSQL 17 para RDS para bases de datos PostgreSQL supervisadas por RDS Protection. GuardDuty Para más información, consulte la [bases de datos compatibles](#) en Protección de RDS.

13 de septiembre de 2025

Funcionalidad actualizada:  
protección contra malware  
para S3

GuardDuty Malware Protection for S3 aumenta la cuota predeterminada de archivos extraídos de 1000 a 10 000 archivos. Para obtener más información, consulte [Cuotas en la protección contra malware para S3](#).

3 de septiembre de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.11 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre la nueva versión del agente de seguridad y una lista de recursos adicionales para actualizar el agente de seguridad, consulte [las versiones de lanzamiento del agente de GuardDuty seguridad](#).

29 de agosto de 2025

Funcionalidad actualizada:  
trabajar con listas

GuardDuty presenta listas personalizadas de entidades de amenazas y de confianza que admiten direcciones IP y nombres de dominio. GuardDuty sigue admitiendo la lista de direcciones IP y recomienda utilizar la lista de entidades para la detección personalizada de amenazas. Para obtener más información, consulte [Personalización de la detección de amenazas con listas de entidades y listas de direcciones IP](#).

15 de agosto de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.8.0 del agente de seguridad para los recursos de Amazon EC2 y Amazon ECS AWS Fargate -. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

12 de agosto de 2025

### [Compatibilidad con la región Asia-Pacífico \(Taipéi\)](#)

Amazon ya GuardDuty está disponible en la región Asia Pacífico (Taipéi-ap-east-2 ). Para GuardDuty activarlo en esta región, consulta [Cómo empezar](#). Puede recibir notificaciones sobre las actualizaciones de las GuardDuty funciones y las detecciones de amenazas [suscribiéndose a los anuncios de Amazon GuardDuty SNS](#) en esta región.

31 de julio de 2025

### [Funcionalidad actualizada: protección contra malware para S3](#)

La protección contra malware para S3 ahora admite el análisis de objetos de hasta 100 GB, antes era de 5 GB. Esto incluye tanto los objetos individuales como los archivos extraídos. Para obtener más información, consulte [Cuotas de la protección contra malware para S3](#).

23 de julio de 2025

Funcionalidad actualizada: se agregó el propietario esperado del bucket en las listas de amenazas e IP de confianza

GuardDuty se agregó el campo Propietario esperado del bucket para las listas de IP confiables e IP de amenazas. En este campo opcional, puede especificar un Cuenta de AWS ID que GuardDuty se utilizará para verificar la propiedad del bucket de Amazon S3. Para obtener más información, consulte [Trabajo con listas de IP fiables y listas de amenazas](#).

16 de julio de 2025

[Funcionalidad actualizada:](#)  
[Detección Extendida de](#)  
[Amenazas](#)

17 de junio de 2025

GuardDuty La detección extendida de amenazas ahora amplía el soporte para los clústeres de Amazon EKS al correlacionar varias señales de seguridad entre los registros de auditoría de EKS, el comportamiento de los procesos en tiempo de ejecución y la actividad de las AWS API. Active EKS Protection, Runtime Monitoring (con el complemento EKS) o ambas opciones para [maximizar la detección de amenazas](#). Para identificar posibles amenazas, GuardDuty presenta un nuevo tipo de hallazgo: [AttackSequence:EKS/CompromisedCluster](#). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

Funcionalidad actualizada:  
protección contra malware  
para S3

La protección contra malware para S3 no admite el análisis de archivos con una relación de compresión extremadamente alta. Estos archivos se omitirán durante el análisis y se marcarán con un resultado de análisis de UNSUPPORTED. Para obtener más información, consulte [Estado potencial de análisis de objeto de S3 y estado del producto](#).

13 de junio de 2025

Funcionalidad actualizada:  
Malware Protection for EC2

Malware Protection for EC2 ha añadido compatibilidad para escanear la mayoría de las instancias con productCode como marketplace. Esto se aplica tanto a los escaneos de GuardDuty-initiated malware como a los escaneos de On-demand malware. Para obtener más información, consulte [Motivos para omitir un recurso durante el análisis de malware](#).

13 de junio de 2025



## [Nueva política de AmazonGuardDutyFullAccess\\_v2](#)

Se agregó una nueva AmazonGuardDutyFullAccess\_v2 política con permisos para mejorar la seguridad al restringir las acciones administrativas a los directores GuardDuty de servicio. Para obtener información sobre esta política recomendada, consulte la [política administrada de AWS : AmazonGuardDutyFullAccess\\_v2](#)

4 de junio de 2025

## [Compatibilidad regional ampliada para RDS Protection](#)

GuardDuty RDS Protection ya está disponible en las regiones de México (Centro), Asia Pacífico (Tailandia) y Asia Pacífico (Malasia). La protección de rDS ayuda a detectar comportamientos de inicio de sesión potencialmente sospechosos en Aurora MySQL, Aurora PostgreSQL (incluida la base de datos ilimitada) y RDS para PostgreSQL compatibles. En caso de que se detecte una amenaza, GuardDuty genera un resultado de protección de RDS. Para obtener más información sobre las bases de datos compatibles y sobre cómo habilitar este plan de protección en las nuevas regiones compatibles, consulte [Protección de RDS](#).

4 de junio de 2025

[Funcionalidad actualizada:](#)  
[Runtime Monitoring](#)

GuardDuty Runtime Monitoring lanza la nueva versión 1.7.1 del agente de seguridad para los recursos de Amazon EC2. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

3 de junio de 2025

[Compatibilidad con la](#)  
[Detección Extendida de](#)  
[Amenazas](#)

GuardDuty La detección extendida de amenazas ya está disponible en Asia Pacífico (Tailandia) (ap-south-east-7). Sin necesidad de activación, detecta ataques en varias etapas que abarcan fuentes de datos, varios tipos de AWS recursos y tiempo, en un abrir y cerrar de ojos. Cuenta de AWS Cuando se detectan amenazas potenciales, se generan resultados de la secuencia de ataque. Para obtener más información, consulte [Detección Extendida de Amenazas](#).

12 de mayo de 2025

### [Compatibilidad con la región de México \(centro\)](#)

Amazon ya GuardDuty está disponible en la región México (Centromx-central-1 ). Para GuardDuty activarlo en esta región, consulta [Cómo empezar](#). Puede recibir notificaciones sobre las actualizaciones de las GuardDuty funciones y las detecciones de amenazas [suscribiéndose a los anuncios de Amazon GuardDuty SNS](#) en esta región.

7 de mayo de 2025

### [Funcionalidad actualizada: Runtime Monitoring](#)

GuardDuty Runtime Monitoring lanza la nueva versión 1.10.0 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

4 de abril de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.7.0 del agente de seguridad para ECS-Fargate los recursos de Amazon. Para obtener más información sobre las nuevas versiones de los agentes de seguridad y una lista de recursos adicionales para actualizar su agente de seguridad, consulte [las versiones de lanzamiento del agente de GuardDuty seguridad](#).

4 de abril de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.7.0 del agente de seguridad para los recursos de Amazon EC2. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar el agente de seguridad, consulte las versiones de [lanzamiento del agente GuardDuty de seguridad](#).

3 de abril de 2025

### Compatibilidad con la región Asia-Pacífico (Tailandia)

Amazon ya GuardDuty está disponible en la región Asia Pacífico (Tailandia). Para obtener información sobre las funciones compatibles en esta región, consulta la [disponibilidad de las Region-specific funciones](#). Para activarlas GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las GuardDuty funciones y las detecciones de amenazas [suscribiéndose a los anuncios de Amazon GuardDuty SNS](#).

1 de abril de 2025

### Funcionalidad actualizada

El panel de resumen ahora muestra información basada en todos los resultados de seguridad generados, lo que elimina la limitación de 5000 resultados anteriores. [Para obtener información sobre estos datos, consulte GuardDuty el panel de resumen.](#)

17 de marzo de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring lanza la nueva versión 1.9.0 del agente de seguridad para los recursos de Amazon EKS. Para obtener más información sobre las nuevas versiones de los agentes de seguridad y una lista de recursos adicionales para actualizar su agente de seguridad, consulte [las versiones de lanzamiento del agente de GuardDuty seguridad](#).

2 de marzo de 2025

Funcionalidad actualizada:  
Runtime Monitoring

GuardDuty Runtime Monitoring ha agregado un nuevo tipo de problema de cobertura (agente no aprovisionado) para los recursos de Amazon EC2. Para obtener información sobre la solución de este problema, consulte [Solución de problemas de cobertura del tiempo de ejecución de Amazon EC2](#).

21 de febrero de 2025

[Funcionalidad actualizada:](#)  
[Runtime Monitoring](#)

GuardDuty Runtime Monitoring lanza nuevos agentes de seguridad para Amazon EC2 y Amazon ECS-Fargate Resources. Para obtener más información sobre las nuevas versiones de los agentes y una lista de recursos adicionales para actualizar sus agentes de seguridad, consulte [las versiones de lanzamiento de los agentes de GuardDuty seguridad](#).

6 de febrero de 2025

[GuardDuty soporte en la región actual de Asia Pacífico \(Malasia\)](#)

GuardDuty La detección ampliada de amenazas ya está disponible en la región de Asia Pacífico (Malasia). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

28 de enero de 2025



### Compatibilidad con la región Asia-Pacífico (Malasia)

Amazon ya GuardDuty está disponible en la región Asia Pacífico (Malasia). Para obtener información sobre las funciones compatibles en esta región, consulta la [disponibilidad de las Region-specific funciones](#). Para activarlas GuardDuty en esta región, consulte [Primeros pasos](#). Puede recibir notificaciones sobre las actualizaciones de las GuardDuty funciones y las detecciones de amenazas [suscribiéndose a los anuncios de Amazon GuardDuty SNS](#).

16 de enero de 2025

### Funcionalidad actualizada: Runtime Monitoring

GuardDuty Runtime Monitoring ha actualizado la información adicional y los pasos para solucionar los problemas de ECS-Fargate cobertura de Amazon relacionados con el agente no aprovisionado. Para obtener más información sobre el tipo de problema de agente no aprovisionado, consulta [Solución de problemas de cobertura del ECS-Fargate tiempo de ejecución de Amazon](#).

8 de enero de 2025

Nuevo tipo de resultado:  
[Policy:IAMUser/ShortTermRootCredentialUsage](#)

GuardDuty presenta un nuevo tipo de búsqueda que le avisa cuando se utilizan credenciales de usuario restringidas, creadas para los usuarios que aparecen Cuentas de AWS en su entorno, para realizar solicitudes. Servicios de AWS Para obtener más información, consulte [Policy:IAMUser/ShortTermRootCredentialUsage](#).

8 de enero de 2025

Nueva función: detección de amenazas GuardDuty ampliada

GuardDuty anuncia la detección ampliada de amenazas, que detecta secuencias de ataques en varias etapas que abarcan las fuentes de datos y AWS los recursos GuardDuty fundamentales de su país Cuenta de AWS durante un período de tiempo específico. Sin coste adicional, esta función se habilita automáticamente para todas las cuentas que la hayan activado. GuardDuty Esta función anuncia dos nuevos tipos de GuardDuty búsqueda, denominados tipos de [búsqueda de secuencias de ataque](#). Para obtener más información, consulte [Detección Extendida de Amenazas](#).

1 de diciembre de 2024

## [Funcionalidad de multiservicio mejorada: Runtime Monitoring y Malware Protection for EC2](#)

Impacto de las nuevas funciones de Amazon Elastic Kubernetes Service (Amazon EKS) en las funciones de Amazon: GuardDuty

1 de diciembre de 2024

- Modo automático de Amazon EKS: tanto Runtime Monitoring para Amazon EKS como Malware Protection for EC2 lo admiten.
- Nodos híbridos de Amazon EKS: tanto Runtime Monitoring para Amazon EKS como Malware Protection for EC2 los admiten.

Para obtener más información, consulte [Cómo funciona Runtime Monitoring con los clústeres de Amazon EKS y Malware Protection for EC2](#).

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EKS](#)

Runtime Monitoring ha lanzado una nueva versión de agente 1.8.1 (v1.8.1-eks-build.2) para los recursos de Amazon EKS. Con esta nueva versión del agente, GuardDuty amplía la compatibilidad con Runtime Monitoring para los recursos de Amazon EKS que se ejecutan en RedHat Centos y Fedora. Para obtener más información, consulte [Validar los requisitos de arquitectura](#). Para obtener información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad para los recursos de Amazon EKS](#).

23 de noviembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EC2](#)

Runtime Monitoring lanzó una nueva versión 1.5.0 del agente para los recursos de Amazon EC2. Con esta nueva versión del agente, GuardDuty amplía la compatibilidad con Runtime Monitoring para los recursos de Amazon EC2 que se ejecutan en RedHat Centos y Fedora. Para obtener más información, consulte [Validar los requisitos de arquitectura](#). Para obtener información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad para los recursos de Amazon EC2](#).

20 de noviembre de 2024

[Funcionalidad actualizada en Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring lanzó una nueva versión 1.5.0 del agente para ECS-Fargate los recursos de Amazon. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para AWS Fargate \(solo Amazon ECS\)](#).

14 de noviembre de 2024

[Funcionalidad actualizada en Malware Protection for EC2](#)

GuardDuty Malware Protection for EC2 ha agregado tres tipos de hallazgos de Runtime Monitoring a la lista de [hallazgos que invocan el análisis de GuardDuty-initiated malware en instancias](#) de Amazon EC2. Las cuentas que hayan activado la protección contra malware para EC2 detectarán el GuardDuty-initiated malware cuando detecten alguno de GuardDuty los siguientes resultados:

7 de noviembre de 2024

- [Execution:Runtime/MaliciousFileExecuted](#)
- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

## Funcionalidad actualizada en RDS Protection

GuardDuty RDS Protection añade la nueva 16.4-limitless versión del motor de bases de datos [Aurora PostgreSQL Limitless](#) a la lista de bases de datos compatibles. Si Cuentas de AWS ya tiene habilitada la protección RDS, GuardDuty empezará automáticamente a supervisar el comportamiento de inicio de sesión de la base de datos Limitless. Las cuentas que ya hayan utilizado la versión de prueba gratuita de 30 días de RDS Protection incurrirán en los costos de uso asociados a la base de datos ilimitada, junto con otras bases de datos compatibles que estén monitoreadas. Para obtener más información, consulte [Protección de RDS](#).

6 de noviembre de 2024

### [Expansión e integración de la GuardDuty región AWS PrivateLink](#)

GuardDuty ahora amplía el soporte regional para [Amazon GuardDuty y los puntos de enlace de la VPC de interfaz](#) ().AWS PrivateLink Anteriormente, la compatibilidad con regiones estaba disponible para el Este de EE. UU. (Norte de Virginia), Europa (Irlanda) e Israel (Tel Aviv). Este soporte ahora se extiende a todos los Regiones de AWS lugares disponibles GuardDuty . Para obtener más información sobre las diferencias regionales, consulta la [disponibilidad de las Region-specific funciones](#).

6 de noviembre de 2024

### [Funcionalidad actualizada en Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring ha publicado una nueva versión del agente 1.4.1 para ECS-Fargate los recursos de Amazon. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para AWS Fargate \(solo Amazon ECS\)](#).

24 de octubre de 2024

[Se agregó soporte para las operaciones GuardDuty CloudFormation de etiquetado](#)

GuardDuty ahora admite la actualización de la clave y el valor de la etiqueta, así como de las etiquetas a nivel de pila. Para ello, agregue el permiso `guardduty:tagResource` al rol de IAM. Para obtener más información GuardDuty CloudFormation, consulte la [referencia de tipos de GuardDuty recursos de Amazon](#) en la Guía del AWS CloudFormation usuario.

24 de octubre de 2024

[Funcionalidad actualizada de GuardDuty Malware Protection para S3](#)

Al habilitar la protección contra malware para S3, puede elegir un rol de servicio que tenga los permisos necesarios para realizar acciones de análisis de malware en su nombre. Para obtener más información sobre cómo habilitar la protección contra malware para S3, consulte [Configurar la protección contra malware para S3 para el bucket de S3](#).

22 de octubre de 2024



## Funcionalidad actualizada

GuardDuty mejora el tipo de [UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS](#) búsqueda para detectar el uso de AWS credenciales de instancia de Amazon EC2 desde puntos de enlace de la VPC (AWS PrivateLink) Cuentas de AWS que no están asociadas al rol de instancia de Amazon EC2. Esta nueva GuardDuty capacidad detecta un posible uso indebido de las credenciales de la instancia Amazon EC2 y proporciona un contexto del control remoto Cuenta de AWS mediante las credenciales de sesión de extracción. Para obtener más información sobre los puntos de enlace de AWS servicio compatibles con esta nueva detección, consulte [Registrar los eventos de actividad de la red](#) en la Guía del usuario.AWS CloudTrail

21 de octubre de 2024

Funcionalidad actualizada:  
supervisión del GuardDuty  
tiempo de ejecución

GuardDuty Runtime Monitorin  
g agregó los siguientes tres  
tipos de búsqueda que le  
notifican cuando se ejecutan  
comandos sospechosos en  
una instancia de Amazon EC2  
o en una carga de trabajo de  
contenedor dentro de su AWS  
entorno:

10 de octubre de 2024

- [Discovery:Runtime/  
SuspiciousCommand](#)
- [Persistence:Runtime/Suspici  
ousCommand](#)
- [PrivilegeEscalation:Runtime/  
SuspiciousCommand](#)

Nueva característica:  
compatibilidad agregada con  
puntos de conexión de VPC

GuardDuty ahora está  
integrado con puntos finales  
de VPC AWS PrivateLink  
y es compatible con ellos.  
Para obtener más informaci  
ón sobre la AWS PrivateLink  
integración, consulte [Amazon  
GuardDuty y los puntos de  
enlace de la VPC de interfaz](#)  
([.AWS PrivateLink](#)

17 de septiembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.7.1 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para Amazon EKS](#).

13 de septiembre de 2024

[Funcionalidad actualizada en la protección contra malware para S3](#)

Malware Protection for S3 agregó un nuevo campo, `s3Throttled`, al esquema Amazon EventBridge (EventBridge) del resultado del escaneo de objetos de S3. El campo `s3Throttled` indica si hubo o no un retraso en la carga o recuperación de almacenamiento de los buckets de Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).

13 de septiembre de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: Amazon EC2](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.3.1 para los recursos de Amazon EC2. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para Amazon EC2](#).

12 de septiembre de 2024

[Funcionalidad actualizada en Runtime Monitoring - Amazon ECS-Fargate](#)

Runtime Monitoring lanzó una nueva versión del agente 1.3.1 para ECS-Fargate los recursos de Amazon. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para AWS Fargate \(solo Amazon ECS\)](#).

11 de septiembre de 2024

[Función GuardDuty vinculada a servicios \(SLR\) actualizada](#)

GuardDuty ha actualizado la SLR para incluir el `ec2:DescribeVpcs` permiso en las acciones de Amazon EC2. Para obtener más información, consulte los [permisos de Service-linked rol para](#). GuardDuty

22 de agosto de 2024

### [Importante adición de contenidos](#)

GuardDuty se han añadido importantes actualizaciones de contenido a la función Malware Protection for S3.

20 de agosto de 2024

- Se han añadido nuevos ejemplos de un esquema de notificaciones de ejemplo para configurar EventBridge las reglas de Amazon para recibir notificaciones relacionadas con el estado de los recursos del plan de protección contra malware y el resultado del análisis de objetos de S3. Para obtener más información, consulte [Supervisión de escaneos de objetos de S3 con Amazon EventBridge](#).
- Se ha agregado información sobre la [Solución de problemas de errores de etiquetas posteriores al análisis de objetos de S3](#).

### [Funcionalidad actualizada en GuardDuty Runtime Monitoring - Amazon EC2](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión 1.3.0 del agente para los recursos de Amazon EC2. Para obtener más información sobre las notas de la versión, consulte el [agente de GuardDuty seguridad para Amazon EC2](#).

19 de agosto de 2024

### [Funcionalidad actualizada en GuardDuty Runtime Monitoring - Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.7.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad para los clústeres de Amazon EKS](#).

17 de agosto de 2024

### [Importante adición de contenidos](#)

GuardDuty agregó nueva información sobre la metodología de detección de malware y los motores de escaneo que utiliza para las funciones Malware Protection for S3 y Malware Protection for EC2. Para obtener más información, consulte el [motor de análisis de detección de GuardDuty malware](#).

15 de agosto de 2024

### [Nueva característica: protección de las cargas de trabajo de IA](#)

GuardDuty La detección de amenazas fundamental y la protección Lambda le ayudan a proteger y detectar mejor las amenazas a las cargas de trabajo de IA basadas en ellas. AWS Para obtener más información, consulte [Proteger las cargas de trabajo de IA con GuardDuty](#)

14 de agosto de 2024

[Funcionalidad actualizada en GuardDuty Runtime Monitoring: Fargate \(solo Amazon ECS\)](#)

Runtime Monitoring lanzó una nueva versión 1.3.0 del agente para los recursos AWS Fargate (solo de Amazon ECS). Para obtener más información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad de Fargate-ECS](#).

9 de agosto de 2024

[Funcionalidad actualizada: protección contra malware para S3](#)

GuardDuty Malware Protection for S3 aumenta la cuota máxima de cubos de S3 de 10 a 25 cubos. Esta cuota se aplica a una Cuenta de AWS por cada una. Región de AWS Para obtener más información, consulte [Protección contra malware para S3](#).

8 de agosto de 2024

[Actualizado: nuevos tipos de resultados en la Supervisión en tiempo de ejecución](#)

GuardDuty ha agregado dos nuevos tipos de detección de Runtime Monitoring que le ayudarán a detectar las amenazas que implican la creación de un shell sospechoso en el recurso monitoreado y la escalada de privilegios, cuando un proceso eleva sus privilegios a root de forma sospechosa.

6 de agosto de 2024

- [Execution:Runtime/SuspiciousShellCreated](#)
- [PrivilegeEscalation:Runtime/ElevationToRoot](#)

[Actualizado: se integra con AWS Security Hub CSPM](#)

AWS Security Hub CSPM proporciona una lista de controles de GuardDuty seguridad para evaluar sus recursos y comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad. Para obtener más información, consulte [Uso de GuardDuty controles en Security Hub CSPM](#).

11 de julio de 2024

[Se actualizó el script GuardDuty del comprobador para comprobar los resultados](#)

GuardDuty ahora admite más de 100 hallazgos con diferentes AWS recursos en una cuenta dedicada. Para obtener más información, consulta los [GuardDuty resultados de las pruebas en cuentas específicas](#).

28 de junio de 2024



### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha publicado una nueva versión 1.2.0 del agente de seguridad para el recurso de Amazon EC2. Para obtener información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad para la instancia Amazon EC2](#).

Para obtener información sobre la actualización manual del agente de seguridad a esta versión, consulte [Administrar manualmente el agente de seguridad para una instancia de Amazon EC2](#).

13 de junio de 2024

### [Nueva característica: protección contra malware para la disponibilidad regional de S3](#)

GuardDuty La protección contra malware para S3 ya está disponible en todas las regiones comerciales en las que GuardDuty está disponible. Esta funcionalidad ayuda a analizar los objetos recién cargados en los buckets de Amazon S3 en busca de malware potencial y cargas sospechosas, así como a tomar medidas para aislarlos antes de que se ingieran en los procesos posteriores. Para obtener información sobre cómo activar la protección contra malware para S3, consulte [Protección contra GuardDuty malware para S3](#).

12 de junio de 2024

## Nueva característica: protección contra malware para S3

11 de junio de 2024

GuardDuty anuncia la disponibilidad general de Malware Protection para S3, que le ayuda a escanear los objetos recién cargados a los buckets de Amazon S3 en busca de posibles cargas sospechosas y malware, y a tomar medidas para aislarlos antes de que se introduzcan en los procesos posteriores. Esta función está totalmente gestionada por AWS GuardDuty publica el resultado del escaneo de objetos de S3 en su bus de eventos EventBridge predeterminado. Puede permitir añadir etiquetas GuardDuty a los objetos S3 escaneados. Puede crear flujos de trabajo posteriores, como el aislamiento en un bucket de cuarentena, o definir políticas de bucket mediante etiquetas que impidan a los usuarios o aplicaciones acceder a determinados objetos. Para obtener más información, consulte [GuardDuty Protección contra malware para S3](#). Actualmente está disponible en las siguientes regiones:

- Este de EE. UU. (Norte de Virginia)

- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Oregón)
- Europa (Irlanda)
- Europa (Fráncfort)
- Europa (Estocolmo)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Asia-Pacífico (Singapur)

[Se actualizó la política de AmazonGuardDutyFullAccess](#)

Se agregó un permiso que le permite transferir una función de IAM GuardDuty al habilitar la protección contra malware para S3. Para obtener más información sobre esta actualización de la política, consulte la [política administrada de AWS : AmazonGuardDutyFullAccess](#).

10 de junio de 2024

### [Funcionalidad actualizada en GuardDuty RDS Protection](#)

La protección de RDS amplía la compatibilidad para supervisar la actividad de inicio de sesión en las bases de datos de RDS para PostgreSQL. Como parte de esta expansión, GuardDuty empezará automáticamente a supervisar los datos de inicio de sesión de las bases de datos de RDS para PostgreSQL de las cuentas que ya tienen habilitada la protección de RDS. GuardDuty Para obtener más información, consulte [Protección de RDS](#).

6 de junio de 2024

### [Funcionalidad actualizada en GuardDuty Runtime Monitoring: Fargate \(solo Amazon ECS\)](#)

Runtime Monitoring lanzó una nueva versión 1.2.0 del agente para los recursos AWS Fargate (solo de Amazon ECS). Para obtener más información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad de Fargate-ECS](#).

31 de mayo de 2024

### [Funcionalidad actualizada de GuardDuty Malware Protection para EC2](#)

Para cada volumen de Amazon EBS adjunto a sus instancias de Amazon EC2 y cargas de trabajo de contenedores GuardDuty, Malware Protection for EC2 ha aumentado el tamaño del volumen de EBS que escanea hasta 2048 GB. Para obtener información sobre cómo escanear los volúmenes de Amazon EBS adjuntos a sus instancias, consulte [GuardDuty Malware Protection for EC2](#).

29 de mayo de 2024

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La monitorización en tiempo de ejecución de ECS-Fargate los recursos de Amazon ahora permite detectar posibles amenazas en las tareas lanzadas por AWS Batch y AWS CodePipeline. Para obtener más información, consulte [Cómo funciona la Supervisión en tiempo de ejecución con Fargate \(solo Amazon ECS\)](#).

28 de mayo de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.6.1 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

14 de mayo de 2024

[Compatibilidad regional ampliada para la Supervisión en tiempo de ejecución](#)

GuardDuty amplía el soporte para Runtime Monitoring a la región de Canadá Oeste (Calgary). Para obtener información sobre cómo comenzar a utilizar la Supervisión en tiempo de ejecución, consulte [Habilitar la Supervisión en tiempo de ejecución](#).

7 de mayo de 2024

### [Compatibilidad regional ampliada para RDS Protection](#)

GuardDuty amplía el soporte de RDS Protection a lo siguiente: Regiones de AWS

3 de mayo de 2024

- Oeste de Canadá (Calgary)
- Asia-Pacífico (Hyderabad)
- Europa (España)
- Europa (Zúrich)
- Medio Oriente (EAU)
- Israel (Tel Aviv)
- Asia-Pacífico (Melbourne)

Para obtener información sobre cómo habilitar esta característica, consulte [Protección de RDS](#).

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Runtime Monitoring lanzó una nueva versión del agente 1.1.0 para los recursos AWS Fargate (solo de Amazon ECS). Para obtener más información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad de Fargate-ECS](#).

1 de mayo de 2024

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.6.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

29 de abril de 2024

### [Compatibilidad con IPAddress v6](#)

GuardDuty ha añadido compatibilidad con IPAddress V6 para los detalles de IP locales y remotos. Puede utilizar los [atributos de filtro asociados para filtrar los](#) GuardDuty resultados o [crear](#) reglas de supresión.

18 de abril de 2024

### [Experiencia de consola actualizada para configurar la exportación de resultados](#)

GuardDuty ha actualizado la experiencia de la consola para exportar las conclusiones generadas en su Cuentas de AWS cuenta a un bucket de Amazon S3. Para obtener más información, consulte [Exportación de GuardDuty los resultados](#).

1 de abril de 2024



### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha publicado una nueva versión 1.1.0 del agente de seguridad para el recurso de Amazon EC2. Esta versión admite la configuración GuardDuty automática de agentes en Runtime Monitoring para instancias de Amazon EC2. Para obtener información sobre las notas de la versión, consulte el [agente GuardDuty de seguridad para la instancia Amazon EC2](#).

28 de marzo de 2024

## [Disponibilidad general de la Supervisión en tiempo de ejecución para las instancias de Amazon EC2](#)

28 de marzo de 2024

GuardDuty anuncia la disponibilidad general (GA) de Runtime Monitoring para instancias de Amazon EC2. Ahora, tiene la opción de [habilitar la configuración automática del agente](#) que le permite GuardDuty instalar y administrar el agente de seguridad para sus instancias de Amazon EC2 en su nombre. Con el agente GuardDuty automatizado, también puede usar etiquetas de inclusión o exclusión como información GuardDuty para instalar y administrar el agente de seguridad solo en instancias seleccionadas de Amazon EC2. Para obtener más información, consulte [Cómo funciona el Monitoreo de tiempo de ejecución con las instancias de Amazon EC2](#).

Lista de nuevos tipos de resultados publicados con esta disponibilidad general

- [Execution:Runtime/SuspiciousTool](#)
- [Execution:Runtime/SuspiciousCommand](#)
- [DefenseEvasion:Runtime/SuspiciousCommand](#)

- [DefenseEvasion:Runtime/PtraceAntiDebugging](#)
- [Execution:Runtime/MaliciousFileExecuted](#)

## [Amazon GuardDuty ha actualizado el Service-linked rol \(SLR\)](#)

Utilice AWS Systems Manager acciones para gestionar las asociaciones de SSM en las instancias de Amazon EC2 al GuardDuty habilitar Runtime Monitoring con un agente automatizado para Amazon EC2. Cuando la configuración GuardDuty automática de agentes está deshabilitada, solo GuardDuty tiene en cuenta las instancias EC2 que tienen una etiqueta de inclusión (:). GuardDuty Managed true

- En la siguiente lista aparecen los nuevos permisos:

```
"ssm:DescribeAssociation",
"ssm:DeleteAssociation",
"ssm:UpdateAssociation",
"ssm:CreateAssociation",
"ssm:StartAssociationsOnce",
"ssm:AddTagsToResource",
"ssm:CreateAssociation",
"ssm:UpdateAssociation",
"ssm:SendCommand",
"ssm:GetCommandInvocation"
```

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Con la última versión del agente de GuardDuty seguridad (complemento) v1.5.0 para Amazon EKS, Runtime Monitoring ahora admite la configuración de parámetros específicos del agente de GuardDuty seguridad, como la configuración de la CPU y la memoria, la configuración y la `PriorityClass` configuración de la política de DNS. Para obtener más información, consulte [Configuración de los parámetros del agente GuardDuty de seguridad \(complemento EKS\)](#).

7 de marzo de 2024

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.5.0 para los recursos de Amazon EKS. Para obtener más información sobre las notas de la versión, consulte el [Historial de versiones del agente del complemento EKS](#).

7 de marzo de 2024

### [Compatibilidad para Oeste de Canadá \(Calgary\)](#)

Amazon ya GuardDuty está disponible en la región Canadá Oeste (Calgary). GuardDuty Es posible que algunos de los planes de protección incluidos no estén disponibles en esta región. Para obtener la información más reciente, consulte [Regiones y puntos de conexión](#).

6 de marzo de 2024

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

Las versiones 1.0.0 y 1.1.0 del agente de GuardDuty seguridad para los clústeres de Amazon EKS dejarán de ser compatibles a partir del 14 de mayo de 2024. Para obtener información sobre los pasos que puede tomar antes de que finalice el soporte estándar, consulte el [agente de GuardDuty seguridad para los clústeres de Amazon EKS](#).

16 de febrero de 2024

### [Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución es compatible con la [versión más reciente de Kubernetes 1.29](#) con la versión 1.4.1 del agente de seguridad existente. La compatibilidad ha estado disponible desde el lanzamiento de esta versión de Kubernetes. Para obtener información sobre las versiones de Kubernetes compatibles, consulte [Versiones de Kubernetes](#) compatibles con el agente de seguridad. GuardDuty

16 de febrero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: disponibilidad regional](#)

GuardDuty La monitorización del tiempo de ejecución ahora admite Amazon VPC compartida dentro de la misma. AWS Organizations GuardDuty El [rol vinculado a un servicio \(SLR\)](#) tiene un nuevo permiso `organizations:DescribeOrganization` que ayuda a recuperar el ID de la organización de la cuenta de Amazon VPC compartida para establecer la política de puntos finales. Para obtener información sobre los requisitos previos para utilizar un punto de conexión de Amazon VPC compartida en la Supervisión en tiempo de ejecución, consulte [Compatibilidad con Amazon VPC compartida](#). Esta función está disponible en todas las regiones en las que se admite la monitorización del tiempo de ejecución. GuardDuty

12 de febrero de 2024



[Funcionalidad actualizada en la Supervisión en tiempo de ejecución: disponibilidad regional](#)

GuardDuty La monitorización del tiempo de ejecución ahora admite Amazon VPC compartida dentro de la misma. AWS Organizations GuardDuty El [rol vinculado a un servicio \(SLR\)](#) tiene un nuevo permiso `organizations:DescribeOrganization` que ayuda a recuperar el ID de la organización de la cuenta de Amazon VPC compartida para establecer la política de puntos finales. Para obtener información sobre los requisitos previos para utilizar un punto de conexión de Amazon VPC compartida en la Supervisión en tiempo de ejecución, consulte [Compatibilidad con Amazon VPC compartida](#). Actualmente, esta capacidad está disponible en algunas de las Regiones de AWS. Para obtener más información, consulte [Puntos de conexión y Regiones de](#).

9 de febrero de 2024

[Funcionalidad actualizada con soporte para la nueva versión: Malware Protection for EC2 Regiones de AWS](#)

La protección contra malware para EC2 ahora permite escanear los volúmenes de EBS cifrados Claves administradas por AWS en la región EE.UU. Oeste (Oregón).

6 de febrero de 2024

[Funcionalidad actualizada con soporte para la nueva versión Regiones de AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 ahora permite escanear los volúmenes de EBS cifrados con Claves administradas por AWS lo siguiente: Regiones de AWS](#)

5 de febrero de 2024

- Asia-Pacífico (Singapur) (ap-southeast-1 )
- Europa (Fráncfort) (eu-central-1 )
- Asia-Pacífico (Osaka) (ap-northeast-3 )
- Este de EE. UU. (Ohio) (us-east-2 )
- Europa (Milán) (eu-south-1 )
- Asia-Pacífico (Tokio) (ap-northeast-1 )
- Asia-Pacífico (Seúl) (ap-northeast-2 )
- Canadá (centro) (ca-central-1 )
- Europa (Irlanda) (eu-west-1 )
- Este de EE. UU. (Norte de Virginia) (us-east-1 )

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

GuardDuty Runtime Monitoring ha publicado una nueva versión del agente de GuardDuty seguridad (v1.0.2) para las instancias de Amazon EC2. Esta versión del agente incluye compatibilidad con las AMI de Amazon ECS más recientes. Para obtener más información sobre el historial de versiones de los agentes, consulte [GuardDuty Security Agent for Amazon EC2 instances](#).

2 de febrero de 2024

[Funcionalidad actualizada con soporte para la nueva versión Regiones de AWS : Malware Protection for EC2](#)

[Malware Protection for EC2 ahora admite el escaneo de los volúmenes de Amazon EBS Claves administradas por AWS cifrados con lo siguiente: Regiones de AWS](#)

31 de enero de 2024

- Europa (Londres) (eu-west-2 )
- Europa (Estocolmo) (eu-north-1 )
- Asia Pacífico (Hong Kong) (ap-east-1 )
- África (Ciudad del Cabo) (af-south-1 )
- Medio Oriente (Baréin) (me-south-1 )
- Asia-Pacífico (Hyderabad) (ap-south-2 )
- Europa (España) (eu-south-2 )
- Asia-Pacífico (Melbourne) (ap-southeast-4 )
- Asia-Pacífico (Sídney) (ap-southeast-2 )
- Israel (Tel Aviv) (il-central-1 )

[Se actualizó la administración de cuentas con AWS Organizations](#)

Se reorganizó el contenido en [Administrar cuentas con AWS Organizations](#) , agregó pasos para cambiar la cuenta de GuardDuty administrador delegado y actualizó [Entendiendo la relación entre la cuenta de GuardDuty administrador y las cuentas de los miembros](#).

30 de enero de 2024

[Funcionalidad actualizada con soporte para nuevas Regiones de AWS](#)

[Malware Protection for EC2](#) ahora permite escanear los volúmenes de EBS cifrados con lo Claves administradas por AWS siguiente: [Regiones de AWS](#)

29 de enero de 2024

- Asia-Pacífico (Yakarta) (ap-southeast-3 )
- Oeste de EE. UU. (Norte de California) (us-west-1 )
- Medio Oriente (EAU) (me-central-1 )
- Europa (Zúrich) (eu-central-2 )
- Asia-Pacífico (Mumbai) (ap-south-1 )
- América del Sur (São Paulo) (sa-east-1 )

## [Funcionalidad actualizada en Malware Protection for EC2](#)

### Malware Protection for EC2

25 de enero de 2024

ahora admite el análisis de los volúmenes de EBS cifrados mediante Claves administradas por AWS.

#### [El rol vinculado al servicio \(SLR\) de Malware Protection for EC2](#)

cuenta con dos nuevos permisos: `GetSnapshotBlock` y `ListSnapshotBlocks`. Estos permisos le ayudarán a GuardDuty recuperar la instantánea de un volumen de EBS (cifrado mediante Clave administrada de AWS) Cuenta de AWS y a copiarla a la [cuenta de GuardDuty servicio antes de iniciar el análisis](#) de software malicioso. Actualmente, esta funcionalidad solo se encuentra disponible en Europa (París) (eu-west-3). Para obtener más información, consulte [Volúmenes admitidos para el análisis de malware](#).

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

GuardDuty Runtime Monitoring ha publicado una nueva versión del agente de GuardDuty seguridad (v1.0.1) con mejoras y ajustes generales del rendimiento. Para obtener más información sobre el historial de versiones de los agentes, consulte [GuardDuty Security Agent for Amazon EC2 instances](#).

23 de enero de 2024

[Funcionalidad actualizada en la Supervisión en tiempo de ejecución](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.4.1 para los recursos de Amazon EKS. Para más información, consulte [EKS add-on agent release history](#).

16 de enero de 2024

[La Supervisión en tiempo de ejecución ha lanzado un nuevo agente v1.4.0 para los recursos de Amazon EKS](#)

La Supervisión en tiempo de ejecución ha lanzado una nueva versión de agente 1.4.0 para los recursos de Amazon EKS. Para más información, consulte [EKS add-on agent release history](#).

21 de diciembre de 2023

[Se agregaron tipos de hallazgos basados en S3 y aprendizaje automático \(ML\) en Europa \(Zúrich\), Europa \(España\), Asia Pacífico \(Hyderabad\), Asia Pacífico \(Melbourne\) e Israel \(Tel Aviv\)](#)

El siguiente S3 y CloudTrail los hallazgos que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático (ML) de detección de anomalías ya están disponibles en las regiones de Europa (Zúrich), Europa (España), Asia Pacífico (Hyderabad), Asia Pacífico (Melbourne) e Israel (Tel Aviv):

21 de diciembre de 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)



- [Persistence:IAMUser/AnomalousBehavior](#)
- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty admite 50 000 cuentas de miembros a través de AWS Organizations](#)

Un GuardDuty administrador delegado ahora puede gestionar un máximo de 50 000 cuentas de miembros mediante AWS Organizations. Esto también incluye un máximo de 5000 cuentas de miembros asociadas a la cuenta de GuardDuty administrador mediante invitación.

20 de diciembre de 2023

[GuardDuty El soporte de monitorización del tiempo de ejecución se amplió a 19 Regiones de AWS](#)

La Supervisión en tiempo de ejecución ya se encuentra disponible en Asia-Pacífico (Yakarta), Europa (París), Asia-Pacífico (Osaka), Asia-Pacífico (Seúl), Medio Oriente (Baréin), Europa (España), Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Israel (Tel Aviv), Oeste de EE. UU. (Norte de California), Europa (Londres), Asia-Pacífico (Hong Kong), Europa (Milán), Medio Oriente (EAU), América del Sur (São Paulo), Asia-Pacífico (Mumbai), Canadá (centro), África (Ciudad del Cabo), Europa (Zúrich).

6 de diciembre de 2023

[GuardDuty amplía la capacidad de monitorización del tiempo de ejecución](#)

Además de detectar amenazas en sus clústeres de Amazon EKS, GuardDuty anuncia la disponibilidad general de Runtime Monitoring para detectar amenazas en sus cargas de trabajo de Amazon ECS y una versión preliminar para detectar amenazas en sus instancias de Amazon EC2. Para obtener más información sobre qué Regiones de AWS admiten actualmente la Supervisión en tiempo de ejecución, consulte [Regiones y puntos de conexión](#).

26 de noviembre de 2023

### [Amazon GuardDuty ha actualizado el Service-linked rol \(SLR\)](#)

26 de noviembre de 2023

GuardDuty ha añadido nuevos permisos para utilizar las acciones de Amazon ECS a fin de gestionar y recuperar información sobre los clústeres de Amazon ECS y gestionar la configuración de la cuenta de Amazon ECS con `guardduty:Activate`. Las acciones relacionadas con Amazon ECS también recuperan la información sobre las etiquetas asociadas a ellas GuardDuty.

- Se han agregado los siguientes permisos como parte de la GuardDuty expansión de la capacidad de [monitoreo del tiempo de ejecución](#):

```
"ecs:ListClusters",  
"ecs:DescribeClusters",  
"ecs:PutAccountSettingDefault"
```

### [Se actualizaron las políticas AWS administradas](#)

16 de noviembre de 2023

GuardDuty agregó un nuevo permiso `organizations:ListAccounts` a la [política AWS administrada: AmazonGuardDutyFullAccess](#) y [AmazonGuardDutyReadOnlyAccess](#).

[GuardDuty publicó nuevos tipos de hallazgos que utilizan EKS Audit Log Monitoring.](#)

11 de noviembre de 2023

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados en Asia-Pacífico (Melbourne) (ap-southeast-4 ).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[GuardDuty publicó nuevos tipos de hallazgos que utilizan EKS Audit Log Monitoring.](#)

10 de noviembre de 2023

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados en las regiones de Asia Pacífico (Hyderabad) (ap-south-2 ), Europa (Zúrich) (eu-central-2 ) y Europa (España) (eu-south-2 ).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

- Discovery:Kubernetes/  
AnomalousBehavior.Permis  
sionChecked

[GuardDuty publicó nuevos tipos de hallazgos que utilizan EKS Audit Log Monitoring.](#)

8 de noviembre de 2023

La Supervisión de registros de auditoría de EKS ahora admite los siguientes tipos de resultados. Estos tipos de resultados aún no están disponibles en las regiones Asia-Pacífico (Hyderabad) (ap-south-2 ), Europa (Zúrich) (eu-central-2 ), Europa (España) (eu-south-2 ) y Asia-Pacífico (Melbourne) (ap-southeast-4 ).

- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed



- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

[La supervisión en tiempo de ejecución de EKS ha lanzado el nuevo agente v1.3.1](#)

La Supervisión en tiempo de ejecución de EKS ha lanzado una nueva versión 1.3.1 del agente que incluye importantes revisiones y actualizaciones de seguridad.

23 de octubre de 2023

[Nuevo atributo de filtro para resultados](#)

GuardDuty ha agregado un nuevo criterio para filtrar los hallazgos generados. El sufijo del dominio de solicitud de DNS proporciona el dominio de segundo y nivel superior implicado en la actividad que provocó GuardDuty la generación del hallazgo.

17 de octubre de 2023

[La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.3.0 compatible con la versión 1.28 de Kubernetes](#)

La Supervisión en tiempo de ejecución de EKS lanzó una nueva versión de agente 1.3.0 que admite la versión 1.28 de Kubernetes. Se ha agregado compatibilidad con Ubuntu. Para más información, consulte [EKS add-on agent release history](#).

5 de octubre de 2023

[Se agregaron los tipos de hallazgos basados en el S3 y el aprendizaje AWS CloudTrail automático \(ML\) a las regiones de Asia Pacífico \(Yakarta\) y Medio Oriente \(Emiratos Árabes Unidos\)](#)

El siguiente S3 y CloudTrail los hallazgos que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático (ML) de detección de anomalías ya están disponibles en las regiones de Asia Pacífico (Yakarta) y Oriente Medio (Emiratos Árabes Unidos):

20 de septiembre de 2023

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)
- [Exfiltration:IAMUser/AnomalousBehavior](#)
- [Impact:IAMUser/AnomalousBehavior](#)
- [CredentialAccess:IAMUser/AnomalousBehavior](#)
- [DefenseEvasion:IAMUser/AnomalousBehavior](#)
- [InitialAccess:IAMUser/AnomalousBehavior](#)
- [Persistence:IAMUser/AnomalousBehavior](#)

- [PrivilegeEscalation:IAMUser/AnomalousBehavior](#)
- [Discovery:IAMUser/AnomalousBehavior](#)

[GuardDuty EKS Runtime Monitoring introduce la administración de los agentes GuardDuty de seguridad a nivel de clúster](#)

EKS Runtime Monitoring añade soporte para administrar el agente de GuardDuty seguridad de los clústeres de EKS individuales a fin de monitorear los eventos de tiempo de ejecución solo desde estos clústeres selectivos. La supervisión en tiempo de ejecución de EKS amplía esta capacidad con la compatibilidad con etiquetas.

13 de septiembre de 2023

[GuardDuty Malware Protection para EC2 amplía el soporte a más Regiones de AWS](#)

Malware Protection for EC2 ya está disponible en las regiones Asia-Pacífico (Hyderabad), Asia-Pacífico (Melbourne), Europa (Zúrich) y Europa (España).

11 de septiembre de 2023

### [GuardDuty ahora está disponible en la región Israel \(Tel Aviv\)](#)

Se agregó la región de Israel (Tel Aviv) a la lista de Regiones de AWS lugares donde ahora GuardDuty está disponible. Los siguientes planes de protección ya están disponibles en la región Israel (Tel Aviv):

24 de agosto de 2023

- [EKS Protection](#) incluye la supervisión de registros de auditoría de EKS y la supervisión en tiempo de ejecución de EKS.
- [Protección de Lambda](#).
- [Malware Protection for EC2](#).
- [S3 Protection](#).

Para obtener más información sobre la disponibilidad de planes de protección en la región Israel (Tel Aviv), consulte [Regiones y puntos de conexión](#).

### [GuardDuty se agregó una configuración de activación automática para su organización a nivel de plan de protección](#)

Actualice la configuración organizativa de los planes de protección de su región. Las posibles opciones de configuración son activar para todas las cuentas, habilitar automáticamente para las cuentas nuevas o no habilitar automáticamente para ninguna cuenta de su organización.

16 de agosto de 2023

[Los tipos de detección S3 que identifican comportamientos anómalos mediante GuardDuty el modelo de aprendizaje automático \(ML\) con detección de anomalías ya están disponibles en Asia Pacífico \(Osaka\)](#)

Los siguientes tipos de resultados ya están disponibles en la región Asia-Pacífico (Osaka):

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

10 de agosto de 2023

[La supervisión en tiempo de ejecución de EKS ya está disponible en la región Asia-Pacífico \(Melbourne\)](#)

El monitoreo de tiempo de ejecución de GuardDuty EKS dentro de EKS Protection proporciona detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en AWS el entorno. Ya es compatible con la región Asia-Pacífico (Melbourne).

8 de agosto de 2023

[Se actualizó la lista de GuardDuty hallazgos que invocan el análisis de GuardDuty-initiated malware](#)

Algunos tipos de búsqueda de EKS Runtime Monitoring ahora pueden invocar el análisis de GuardDuty-initiated malware en su ordenador. Cuenta de AWS

19 de julio de 2023

[GuardDuty admite 10.000 cuentas de miembros a través de AWS Organizations](#)

Una cuenta de GuardDuty administrador ahora puede gestionar un máximo de 10 000 cuentas de miembros mediante AWS Organizations. Esto también incluye un máximo de 5000 cuentas de miembros asociadas a la cuenta de GuardDuty administrador mediante invitación.

29 de junio de 2023

[La supervisión en tiempo de ejecución de EKS anuncia tres nuevos tipos de resultados.](#)

La supervisión en tiempo de ejecución de EKS admite tres nuevos tipos de resultados que se basan en la técnica de inyección de procesos. Los nuevos tipos de búsqueda son DefenseEvasion:Runtime/ProcessInjection.Proc DefenseEvasion:Runtime/ProcessInjection.Ptrace, y DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite.

22 de junio de 2023

[La supervisión en tiempo de ejecución de EKS ha lanzado un nuevo agente de la versión 1.2.0 compatible con la versión 1.27 de Kubernetes](#)

EKS Runtime Monitoring lanzó una nueva versión del agente, la 1.2.0, que también es compatible con ARM64-based instancias. Se ha agregado compatibilidad con Bottlerocket. Para más información, consulte [EKS add-on agent release history](#).

16 de junio de 2023

[GuardDuty La consola proporciona una vista resumida de sus hallazgos.](#)

El panel de resumen de la GuardDuty consola proporciona una vista agregada de los GuardDuty hallazgos. Actualmente, el panel muestra los datos a través de varios widgets de las últimas 10 000 conclusiones generadas para tu cuenta (o cuentas de miembros si eres GuardDuty administrador) de la región actual.

12 de junio de 2023

[La supervisión de registros de auditoría de EKS ya está disponible en las regiones Asia-Pacífico \(Hyderabad\), Asia-Pacífico \(Melbourne\), Europa \(Zúrich\) y Europa \(España\)](#)

Habilite la supervisión de registros de auditoría de EKS (en la protección de EKS) para las cuentas para supervisar los registros de auditoría de EKS de los clústeres de Amazon EKS y analizarlos para detectar posibles actividades maliciosas o sospechosas.

1 de junio de 2023

[La supervisión de registros de auditoría de EKS ya está disponible en Medio Oriente \(EAU\)](#)

La Supervisión de registros de auditoría de EKS ya está disponible en Medio Oriente (EAU). Habilite la Supervisión de registros de auditoría de EKS para las cuentas para supervisar los registros de auditoría de EKS de los clústeres de Amazon EKS y analizarlos en busca de actividades potencialmente maliciosas y sospechosas.

3 de mayo de 2023

## [GuardDuty Malware Protection for EC2 anuncia un análisis de On-demand malware](#)

27 de abril de 2023

Malware Protection for EC2 ayuda a detectar la posible presencia de malware en los volúmenes de Amazon EBS asociados a las instancias y cargas de trabajo de contenedores de Amazon EC2. Ahora ofrece dos tipos de escaneos: GuardDuty iniciados y bajo demanda. GuardDuty-initiated el análisis de malware inicia automáticamente un análisis sin agente en los volúmenes de Amazon EBS solo cuando GuardDuty genera uno de los [hallazgos que](#) invoca el análisis de malware. GuardDuty-initiated Puede iniciar un análisis de On-demand malware para detectar instancias de Amazon EC2 en su cuenta proporcionando el nombre de recurso de Amazon (ARN) asociado a esa instancia de Amazon EC2. Para obtener más información sobre las diferencias entre ambos tipos de análisis, consulte [Malware Protection for EC2](#).

- [GuardDuty-initiated análisis de malware](#)
- [On-demand análisis de malware](#)



### [GuardDuty anuncia Lambda Protection](#)

La protección de Lambda le ayuda a identificar posibles amenazas de seguridad en sus funciones de AWS Lambda .

20 de abril de 2023

- [Tipos de resultados de la protección de Lambda](#)
- [Corregir una función de Lambda potencialmente comprometida](#)

### [GuardDuty ya está disponible en la región de Asia Pacífico \(Melbourne\)](#)

Se agregó Asia Pacífico (Melbourne) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener información sobre las características disponibles en esta región, consulte [Regiones y puntos de conexión](#).

19 de abril de 2023

### [GuardDuty se agregaron 3 nuevos tipos de hallazgos de EC2](#)

GuardDuty presenta nuevos tipos de hallazgos para detectar el uso de solucionadores de DNS externos y tecnologías de DNS cifrado. Para obtener información sobre los Regiones de AWS lugares en los que se admiten estos tipos de búsqueda, consulte [Regiones y puntos finales](#).

- [DefenseEvasion:EC2/UnusualDNSResolver](#)
- [DefenseEvasion:EC2/UnusualDoHActivity](#)
- [DefenseEvasion:EC2/UnusualDoTActivity](#)

5 de abril de 2023

## [GuardDuty anuncia la monitorización del tiempo de ejecución de EKS en EKS Protection](#)

30 de marzo de 2023

El monitoreo de tiempo de ejecución de EKS dentro de EKS Protection proporciona la detección de amenazas en tiempo de ejecución para los clústeres de Amazon EKS en AWS el entorno. Utiliza un agente complementario (aws-guardduty-agent ) de Amazon EKS que recopila los [eventos de tiempo de ejecución](#) de sus cargas de trabajo de EKS. Tras GuardDuty recibir estos eventos de tiempo de ejecución, los supervisa y analiza para identificar posibles amenazas de seguridad sospechosas. Para más información, consulte [Detalles de los resultados](#) y [Tipos de resultados de la Supervisión en tiempo de ejecución de EKS](#).

## [GuardDuty añade una nueva funcionalidad: autoEnableOrganizationMembers](#)

23 de marzo de 2023

Amazon GuardDuty añade una nueva opción de configuración de la organización que ayuda a los GuardDuty administradores a auditar y hacer cumplir (si GuardDuty es necesario) lo que está habilitado para ALL los miembros de su organización. La práctica recomendada ahora es utilizar `autoEnableOrganizationMembers` en lugar de `autoEnable`. `autoEnable` está en desuso, pero sigue siendo compatible. Esta nueva funcionalidad afecta a las siguientes API:

- [DescribeOrganizationConfiguration](#)
- [UpdateOrganizationConfiguration](#)
- [DisassociateMembers](#)
- [DeleteMembers](#)
- [DisassociateFromAdministratorAccount](#)
- [StopMonitoringMembers](#)

[La función de protección RDS de Amazon ya GuardDuty está disponible de forma general.](#)

GuardDuty RDS Protection supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de la base de datos de Amazon Aurora. Para más información sobre las Regiones de AWS que admiten RDS Protection, consulte [Regiones y puntos de conexión.](#)

16 de marzo de 2023

[GuardDuty anuncia la activación de funciones](#)

Anteriormente, la GuardDuty API permitía configurar tanto las funciones como las fuentes de datos, pero ahora todos los nuevos tipos de GuardDuty protección se configurarán como funciones y no como fuentes de datos. GuardDuty seguirá admitiendo las fuentes de datos a través de la API, pero no añadirá una nueva API. La activación de las funciones afecta al comportamiento de las API utilizadas para habilitarlas GuardDuty o al tipo de protección que contienen GuardDuty. Si administras tus GuardDuty cuentas mediante una plantilla de API, SDK o CFN, consulta [los cambios en la GuardDuty API en marzo de 2023.](#)

16 de marzo de 2023

[GuardDuty La protección contra malware para EC2 ya está disponible en la región de Oriente Medio \(EAU\)](#)

La función Protección contra malware para EC2 GuardDuty está disponible en la región de Oriente Medio (EAU). Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

13 de marzo de 2023

[Amazon GuardDuty ha actualizado el Service-linked rol \(SLR\)](#)

GuardDuty agregó los siguientes permisos nuevos para admitir la próxima función de monitoreo de tiempo de ejecución de GuardDuty EKS.

8 de marzo de 2023

- Utilice las acciones de Amazon EKS para administrar y recuperar información sobre los clústeres de EKS y administrar los complementos de EKS en los clústeres de EKS. Las acciones de EKS también recuperan la información sobre las etiquetas asociadas a ellas GuardDuty.

```
"eks:ListClusters",  
"eks:DescribeCluster",  
"ec2:DescribeVpcEndpointServices",  
"ec2:DescribeSecurityGroups"
```

[Amazon GuardDuty ha actualizado el Service-linked rol \(SLR\)](#)

La GuardDuty SLR se ha actualizado para permitir la creación de la protección contra malware para las SLR de EC2 una vez habilitada la protección contra malware para EC2.

21 de febrero de 2023

[GuardDuty requiere TLS v1.2 o posterior](#)

Para comunicarse con AWS los recursos, GuardDuty requiere y es compatible con TLS v1.2 o una versión posterior. Para más información, consulte [Protección de los datos](#) y [Seguridad de la infraestructura](#).

14 de febrero de 2023

[GuardDuty ya está disponible en la región de Asia Pacífico \(Hyderabad\)](#)

Se agregó la región Asia-Pacífico (Hyderabad) a la lista de Regiones de AWS lugares donde está disponible. GuardDuty Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

14 de febrero de 2023

[La guía GuardDuty del usuario de Amazon está alineada con las mejores prácticas de IAM](#)

Se ha actualizado la guía para implementar las prácticas recomendadas de IAM. Para obtener más información, consulta [prácticas recomendadas de seguridad en IAM](#).

10 de febrero de 2023

[GuardDuty ya está disponible en la región Europa \(España\)](#)

Se agregó Europa (España) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

8 de febrero de 2023

[GuardDuty ya está disponible en la región de Europa \(Zúrich\)](#)

Se agregó Europa (Zúrich) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

12 de diciembre de 2022

[Versión preliminar de una nueva función: GuardDuty RDS Protection](#)

GuardDuty RDS Protection supervisa y perfila la actividad de inicio de sesión de RDS para identificar comportamientos de inicio de sesión sospechosos en las instancias de la base de datos de Amazon Aurora. Actualmente, estará disponible para una versión preliminar en cinco Regiones de AWS. Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

30 de noviembre de 2022

[GuardDuty ya está disponible en la región de Oriente Medio \(Emiratos Árabes Unidos\)](#)

Se agregó Oriente Medio (Emiratos Árabes Unidos) a la lista de Regiones de AWS lugares donde GuardDuty está disponible. Para obtener más información, consulte [Puntos de conexión y Regiones de](#) .

6 de octubre de 2022



[Se agregó contenido para una nueva función: la protección contra GuardDuty malware para EC2](#)

26 de julio de 2022

GuardDuty La protección contra malware para EC2 es una mejora opcional de Amazon GuardDuty. Si bien GuardDuty identifica los recursos en riesgo, Malware Protection for EC2 detecta el malware que puede ser la fuente del peligro. Con la protección contra malware para EC2 habilitada, cada vez que GuardDuty detecta un comportamiento sospechoso en una instancia de Amazon EC2 o una carga de trabajo de contenedor indicativa de malware GuardDuty, Malware Protection for EC2 inicia un análisis sin agente de los volúmenes de EBS conectados a las cargas de trabajo de la instancia o contenedor de EC2 afectadas para detectar la presencia de malware.

[Para obtener información sobre cómo funciona Malware Protection for EC2 y cómo configurar esta función, consulte Malware Protection for EC2. GuardDuty](#)

- Para obtener información sobre los resultados de Malware Protection for EC2, consulte [Detalles del resultado](#).

- Para obtener información sobre cómo corregir la instancia de EC2 comprometida y un contenedor independiente, consulte [Solucionar los problemas](#) de seguridad descubiertos por GuardDuty.
- Para obtener información sobre la auditoría de CloudWatch los registros de análisis de malware y los motivos por los que se omite un recurso durante el análisis de software malicioso, consulte [Descripción CloudWatch](#) de los registros y los motivos de omisión.
- Para obtener información sobre las detecciones de amenazas por falsos positivos, consulte [Notificación de falsos positivos en GuardDuty Malware Protection](#) for EC2.

[Se ha retirado un tipo de resultado](#)

Se ha retirado [Exfiltration:S3/ObjectRead.Unusual](#).

5 de julio de 2022

[Se agregaron nuevos tipos de detección de S3 que identifican el comportamiento anómalo mediante el modelo GuardDuty de aprendizaje automático \(ML\) de detección de anomalías.](#)

Se han agregado los siguientes tipos de resultados de S3 nuevos. Estos tipos de resultados identifican si una solicitud de API ha invocado una entidad de IAM de forma anómala. El modelo de ML evalúa todas las solicitudes de API de su cuenta e identifica los eventos anómalos asociados a las técnicas utilizadas por los adversarios. Para obtener más información sobre cada uno de estos nuevos resultados, consulte [Tipos de resultados de S3.](#)

5 de julio de 2022

- [Discovery:S3/AnomalousBehavior](#)
- [Impact:S3/AnomalousBehavior.Write](#)
- [Impact:S3/AnomalousBehavior.Delete](#)
- [Impact:S3/AnomalousBehavior.Permission](#)
- [Exfiltration:S3/AnomalousBehavior](#)

[Se agregó contenido de protección GuardDuty EKS para GuardDuty](#)

GuardDuty ahora puede generar resultados para sus recursos de Amazon EKS mediante la supervisión de los registros de auditoría de EKS. Para obtener información sobre cómo configurar esta función, consulte [Protección EKS en Amazon GuardDuty](#). Para ver una lista de las conclusiones que GuardDuty se pueden generar para los recursos de Amazon EKS, consulte las conclusiones de [Kubernetes](#). Se ha agregado una nueva guía de corrección para respaldar la corrección de estos resultados en la [Guía de corrección de resultados de Kubernetes](#).

25 de enero de 2022

[Se ha agregado 1 resultado nuevo](#)

Se ha agregado un nuevo resultado UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS. Este hallazgo le informa cuando una AWS cuenta ajena a su entorno accede a las credenciales de su instancia. AWS

20 de enero de 2022

[Se han actualizado los tipos de resultados para ayudar a identificar los problemas relacionados con log4j](#)

Amazon GuardDuty ha actualizado los siguientes tipos de hallazgos para ayudar a identificar y priorizar los problemas relacionados con CVE-2021-44228 y CVE-2021-45046: Backend:EC2/C&CActivity.B;Backend:EC2/C&CActivity.B!DNS;Behavior:EC2/NetworkPortUnusual.

22 de diciembre de 2021

[Cambios en los resultados](#)

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration se ha cambiado por UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Esta versión mejorada del resultado descubre las ubicaciones habituales en las que se utilizan sus credenciales para reducir los resultados del tráfico que se direcciona a través de las redes locales.  
[UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS](#)

7 de septiembre de 2021

[Actualización a GuardDuty SLR](#)

La GuardDuty SLR se ha actualizado con nuevas acciones para mejorar la precisión de la localización.

3 de agosto de 2021

[Se ha agregado información sobre el origen de datos de cada tipo de resultado.](#)

Las descripciones de los hallazgos ahora contienen información sobre las fuentes de datos que se GuardDuty utilizan para generar ese hallazgo.

10 de mayo de 2021

[Se han retirado 13 tipos de resultados.](#)

Se han retirado 13 hallazgos para reemplazarlos por nuevos AnomalousBehaviour hallazgos. [Persisten](#)  
[ce:IAMUser/NetworkPermissions](#), [Persistence:IAMUser/ResourcePermissions](#), [Persistence:IAMUser/UserPermissions](#), [Privilege Escalation:IAMUser/AdministrativePermissions](#), [Recon:IAMUser/NetworkPermissions](#), [Recon:IAMUser/ResourcePermissions](#), [Recon:IAMUser/UserPermissions](#), [ResourceConsumption:IAMUser/ComputeResources](#), [Stealth:IAMUser/LoggingConfiguration](#) [Modified](#), [Discovery:S3/BucketEnumeration.Unusual](#), [Impact:S3/ObjectDelete.Unusual](#), [Impact:S3/PermissionsModification.Unusual](#), y [UnauthorizedAccess:IAMUser/ConsoleLogin](#).

12 de marzo de 2021

[Se han agregado 8 nuevos tipos de resultados para detectar comportamientos anómalos.](#)

Se han agregado 8 nuevos tipos de resultados de IAMUser en función del comportamiento anómalo de las entidades principales de IAM. [CredentialAccess:IAMUser/AnomalousBehavior](#), [DefenseEvasion:IAMUser/AnomalousBehavior](#), [Discovery:IAMUser/AnomalousBehavior](#), [Exfiltration:IAMUser/AnomalousBehavior](#), [Impact:IAMUser/AnomalousBehavior](#), [InitialAccess:IAMUser/AnomalousBehavior](#), [Persistence:IAMUser/AnomalousBehavior](#), [PrivilegeEscalation:IAMUser/AnomalousBehavior](#).

12 de marzo de 2021

[Se han agregado los resultados de EC2 en función de la reputación del dominio.](#)

Se han agregado 4 nuevos tipos de resultados de impacto en función de la reputación del dominio. [Impact:EC2/AbusedDomainRequest.Reputation](#), [Impact:EC2/BitcoinDomainRequest.Reputation](#), [Impact:EC2/MaliciousDomainRequest.Reputation](#). También se ha agregado un nuevo resultado de EC2 para C&CActivity. [Impact:EC2/SuspiciousDomainRequest.Reputation](#)

27 de enero de 2021

|                                                                                                               |                                                                                                                                                                                                                                                                                                                                       |                          |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">Se han agregado 4 nuevos tipos de resultados.</a>                                                 | Se han agregado 3 nuevos resultados de Malicious IPCaller de S3. <a href="#">Discovery:S3/MaliciousIPCaller</a> , <a href="#">Exfiltration:S3/MaliciousIPCaller</a> , <a href="#">Impact:S3/MaliciousIPCaller</a> . También se ha agregado un nuevo resultado de EC2 para C&CActivity. <a href="#">Backdoor:EC2/C&amp;CActivity.B</a> | 21 de diciembre de 2020  |
| <a href="#">Se ha retirado el tipo de resultado UnauthorizedAccess:EC2/TorIPCaller.</a>                       | El tipo de UnauthorizedAccess:EC2/TorIPCaller hallazgo ahora está retirado de GuardDuty. <a href="#">Más información.</a>                                                                                                                                                                                                             | 1 de octubre de 2020     |
| <a href="#">Se ha agregado el tipo de resultado Impact:EC2/WinRmBruteForce.</a>                               | Se ha agregado un nuevo resultado de impacto, Impact:EC2/WinRmBruteForce. <a href="#">Más información.</a>                                                                                                                                                                                                                            | 17 de septiembre de 2020 |
| <a href="#">Se ha agregado el tipo de resultado Impact:EC2/PortSweep.</a>                                     | Se ha agregado un nuevo resultado de impacto, Impact:EC2/PortSweep. <a href="#">Más información.</a>                                                                                                                                                                                                                                  | 17 de septiembre de 2020 |
| <a href="#">GuardDuty ahora está disponible en las regiones de África (Ciudad del Cabo) y Europa (Milán).</a> | Se han añadido África (Ciudad del Cabo) y Europa (Milán) a la lista de AWS regiones en las que GuardDuty está disponible. <a href="#">Más información</a>                                                                                                                                                                             | 31 de julio de 2020      |



[Se agregaron nuevos detalles de uso para monitorear GuardDuty los costos.](#)

Ahora puedes usar nuevas métricas para consultar los datos de los costos de GuardDuty uso de tu cuenta y de las cuentas que administras. Encontrarás un nuevo resumen de los costes de uso en la consola, en <https://console.aws.amazon.com/guardduty/>. Se puede acceder a información más detallada a través de la API.

31 de julio de 2020

[Se agregó contenido sobre la protección de S3 mediante la supervisión de eventos de datos de S3 en GuardDuty.](#)

GuardDuty La protección de S3 ahora está disponible mediante la supervisión de los eventos del plano de datos de S3 como nueva fuente de datos. Las cuentas nuevas tendrán esta característica habilitada automáticamente. Si ya la está utilizando, GuardDuty puede habilitar la nueva fuente de datos para usted o para sus cuentas de miembros.

31 de julio de 2020

[Se han agregado 14 resultados de S3 nuevos.](#)

Se han agregado 14 nuevos tipos de resultados de S3 para los orígenes del plano de control y del plano de datos de S3.

31 de julio de 2020

[Se ha agregado compatibilidad adicional para los resultados de S3 y se han cambiado 2 nombres de tipos de resultados existentes.](#)

GuardDuty los resultados ahora incluyen más detalles sobre los hallazgos relacionados con los buckets de S3. Se ha cambiado el nombre de los tipos de resultados existentes que estaban relacionados con la actividad de S3: Policy:IAMUser/S3BlockPublicAccessDisabled se ha cambiado a Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled se ha cambiado a Stealth:S3/ServerAccessLoggingDisabled.

28 de mayo de 2020

[Se agregó contenido para la AWS Organizations integración.](#)

GuardDuty ahora se integra con los administradores AWS Organizations delegados para permitirle administrar GuardDuty las cuentas de su organización. Al configurar un administrador delegado como su cuenta de GuardDuty administrador, puede habilitar automáticamente la administración GuardDuty de cualquier miembro de la organización mediante la cuenta de administrador delegado. También puede habilitar automáticamente las cuentas de GuardDuty los nuevos AWS Organizations miembros. [Más información.](#)

20 de abril de 2020

[Se ha agregado contenido para la característica Exportar los resultados.](#)

Se agregó contenido que describe la función Export Findings de GuardDuty.

14 de noviembre de 2019

[Se ha agregado el tipo de resultado UnauthorizedAccess:EC2/MetadataDNSRebind.](#)

Se ha agregado un nuevo resultado no autorizado, UnauthorizedAccess:EC2/MetadataDNSRebind. [Más información.](#)

10 de octubre de 2019

[Se ha agregado el tipo de resultado Stealth:IAMUser/S3ServerAccessLoggingDisabled:](#)

Se ha agregado un nuevo resultado invisible, Stealth:IAMUser/S3ServerAccessLoggingDisabled. [Más información.](#)

10 de octubre de 2019

|                                                                                                   |                                                                                                                                                                               |                       |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Se ha agregado el tipo de resultado Policy:IAMUser/S3BlockPublicAccessDisabled.</a>   | Se ha agregado un nuevo resultado de política, Policy:IAMUser/S3BlockPublicAccessDisabled. <a href="#">Más información.</a>                                                   | 10 de octubre de 2019 |
| <a href="#">Se ha retirado el tipo de resultado Backdoor:EC2/XORDDOS.</a>                         | El tipo de Backdoor:EC2/XORDDOS hallazgo ahora está retirado de GuardDuty. <a href="#">Obtenga más información</a>                                                            | 12 de junio de 2019   |
| <a href="#">Se ha agregado el tipo de resultado PrivilegeEscalation.</a>                          | El tipo de resultado Privilege Escalation detecta cuando los usuarios intentan asignar privilegios escalados y más permisos a sus cuentas. <a href="#">Más información</a>    | 14 de mayo de 2019    |
| <a href="#">GuardDuty ya está disponible en la región de Europa (Estocolmo).</a>                  | Se ha añadido Europa (Estocolmo) a la lista de AWS regiones en las que GuardDuty está disponible. <a href="#">Más información</a>                                             | 9 de mayo de 2019     |
| <a href="#">Se ha agregado un nuevo tipo de resultado, Recon:EC2/PortProbeEMRUnprotectedPort.</a> | Este hallazgo le informa de que un puerto EMR-related confidencial de una instancia EC2 no está bloqueado y se está investigando activamente. <a href="#">Más información</a> | 8 de mayo de 2019     |

[Se han agregado 5 tipos de resultados nuevos que detectan si las instancias de EC2 se están utilizando posiblemente para llevar a cabo ataques de denegación de servicio \(DoS\).](#)

Estos resultados le informan de las instancias EC2 de su entorno cuyo comportamiento puede indicar que se están utilizando para llevar a cabo ataques de denegación de servicio (DoS). [Más información](#)

8 de marzo de 2019

[Se ha agregado un nuevo tipo de resultado: Policy:IAMUser/RootCredentialUsage](#)

Policy:IAMUser/RootCredentialUsageEl tipo de búsqueda le informa de que sus credenciales de inicio de sesión de usuario raíz Cuenta de AWS se utilizan para realizar solicitudes programáticas a los servicios. AWS [Más información](#)

24 de enero de 2019

[Se ha retirado el tipo de resultado UnauthorizedAccess:IAMUser/UnusualASNCaller](#)

Se ha retirado el tipo de resultado UnauthorizedAccess:IAMUser/UnusualASNCaller. Ahora recibirá notificaciones sobre la actividad invocada desde redes inusuales a través de otros tipos de búsquedas activas GuardDuty . El tipo de resultado generado dependerá de la categoría de la API que se invocó desde una red inusual. [Más información](#)

21 de diciembre de 2018

[Se han agregado dos nuevos tipos de resultados: PenTest:IAMUser/ParrotLinux y PenTest:IAMUser/PentooLinux](#)

El tipo de resultado PenTest:IAMUser/ParrotLinux le informa de que un equipo que ejecuta Parrot Security Linux está haciendo llamadas a la API con las credenciales que pertenecen a su cuenta de AWS . El tipo de resultado PenTest:IAMUser/PentooLinux le informa de que una máquina que ejecuta Pentoo Linux está haciendo llamadas a la API con las credenciales que pertenecen a su cuenta de AWS . [Más información](#)

21 de diciembre de 2018

[Se agregó soporte para el tema SNS de GuardDuty anuncios de Amazon](#)

Ahora puede suscribirse al tema SNS de GuardDuty anuncios para recibir notificaciones sobre los tipos de búsqueda publicados recientemente, las actualizaciones de los tipos de búsqueda existentes y otros cambios en las funciones. Las notificaciones están disponibles en todos los formatos que admite Amazon SNS. [Más información](#)

21 de noviembre de 2018

[Se han agregado dos nuevos tipos de resultados: UnauthorizedAccess:EC2/TorClient y UnauthorizedAccess:EC2/TorRelay](#)

UnauthorizedAccess:EC2/TorClient Al buscar el tipo, se indica que una instancia de EC2 de su AWS entorno se está conectando a un nodo de Tor Guard o de Authority . UnauthorizedAccess:EC2/TorRelay buscar el tipo le informa de que una instancia EC2 de su AWS entorno está realizando conexiones a una red Tor, lo que sugiere que actúa como un repetidor de Tor. [Más información](#)

16 de noviembre de 2018

[Se ha agregado un nuevo tipo de resultado: CryptoCurrency:EC2/BitcoinTool.B](#)

Este hallazgo te indica que una instancia de EC2 de tu AWS entorno está consultando un nombre de dominio asociado a Bitcoin u otra actividad relacionada con las criptomonedas. [Más información](#)

9 de noviembre de 2018

[Se agregó soporte para actualizar la frecuencia de las notificaciones enviadas a Events CloudWatch](#)

Ahora puede actualizar la frecuencia de las notificaciones que se envían a CloudWatch Events para que se repitan posteriormente los hallazgos existentes. Los valores posibles son 15 minutos, una hora o seis horas, que es el valor predeterminado. [Más información](#)

9 de octubre de 2018

|                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                    |                     |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Se han agregado regiones compatibles</a>                                                                    | Se agregó soporte regional para AWS GovCloud (US-West) <a href="#">Más información</a>                                                                                                                                                                                                                                                                                                                             | 25 de julio de 2018 |
| <a href="#">Se agregó soporte para CloudFormation StackSets en GuardDuty</a>                                            | Puedes usar la GuardDuty plantilla Enable Amazon para habilitar GuardDuty simultáneamente en varias cuentas. <a href="#">Más información</a>                                                                                                                                                                                                                                                                       | 25 de junio de 2018 |
| <a href="#">Se agregó soporte para reglas de GuardDuty archivado automático</a>                                         | Los clientes ya pueden crear reglas de archivado automático o detalladas para la supresión de resultados. En el caso de los hallazgos que coincidan con una regla de archivado automático, los marca GuardDuty automáticamente como archivados. Esto permite a los clientes ajustar aún más GuardDuty para mantener solo los hallazgos relevantes en la tabla de hallazgos actual. <a href="#">Más información</a> | 4 de mayo de 2018   |
| <a href="#">GuardDuty está disponible en la región de Europa (París)</a>                                                | GuardDuty ya está disponible en Europa (París), lo que le permite ampliar la supervisión continua de la seguridad y la detección de amenazas en esta región. <a href="#">Más información</a>                                                                                                                                                                                                                       | 29 de marzo de 2018 |
| <a href="#">Ahora CloudFormation es posible crear cuentas de administrador y cuentas de miembros a través de ellas.</a> | Para obtener más información, consulte <a href="#">AWS::GuardDuty::master</a> y <a href="#">AWS::GuardDuty::member</a> .                                                                                                                                                                                                                                                                                           | 6 de marzo de 2018  |



|                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Se han añadido nueve nuevas detecciones de CloudTrail-based anomalías.</a>                                                                                                                        | Estos nuevos tipos de búsqueda se activan automáticamente GuardDuty en todas las regiones compatibles. <a href="#">Más información</a>                                                                                                                                                                                                                                                                                                              | 28 de febrero de 2018 |
| <a href="#">Se agregaron tres nuevas detecciones de inteligencia de amenazas (tipos de búsqueda) :</a>                                                                                                        | Estos nuevos tipos de búsqueda se activan automáticamente GuardDuty en todas las regiones compatibles. <a href="#">Más información</a>                                                                                                                                                                                                                                                                                                              | 5 de febrero de 2018  |
| <a href="#">Aumento del límite para las cuentas GuardDuty de los miembros.</a>                                                                                                                                | Con esta versión, puede añadir hasta 1000 cuentas de GuardDuty miembros por AWS cuenta (cuenta de GuardDuty administrador). <a href="#">Más información</a>                                                                                                                                                                                                                                                                                         | 25 de enero de 2018   |
| <a href="#">Cambios en la carga y posterior administración de las listas de direcciones IP confiables y las listas de amenazas para las cuentas de GuardDuty administrador y las cuentas de los miembros.</a> | Con esta versión, los usuarios de GuardDuty cuentas de administrador pueden cargar y gestionar listas de IP fiables y listas de amenazas. Los usuarios de GuardDuty las cuentas de los miembros no pueden cargar ni gestionar listas. Las listas de direcciones IP fiables y las listas de amenazas que carga la cuenta de administrador están sujetas a la GuardDuty funcionalidad de las cuentas de los miembros. <a href="#">Más información</a> | 25 de enero de 2018   |

## Actualizaciones anteriores

| Cambio              | Descripción                                                     | Fecha                   |
|---------------------|-----------------------------------------------------------------|-------------------------|
| Publicación inicial | Publicación inicial de la Guía del GuardDuty usuario de Amazon. | 28 de noviembre de 2017 |

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.