aws

用户指南

Amazon Inspector Classic

版本 Latest

Amazon Inspector Classic: 用户指南

Table of Contents

终止支持通知：2026年5月20日， AWS 将终止对Amazon Inspector Classic的支持。2026 年 5 月 20 日之后，您将无法再访问亚马逊 Inspector Classic 控制台或亚马逊 Inspector Classic 资源。Amazon Inspector Classic 不再适用于新账户和在过去 6 个月内未完成评估的账户。对于所有其他账户，访问权限将在 2026 年 5 月 20 日之前有效，之后您将无法再访问亚马逊 Inspector Classic 控制台或 Amazon Inspector Classic 资源。有关更多信息，请参阅 Amazon Inspector Classic 终止支持。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。

Amazon Inspector Classic 是什么？

> **Note**
>
> 全新 Amazon Inspector 是完全重新架构和重新设计的 Amazon Inspector Classic 版本，现已在 AWS 区域上市。新的 Amazon Inspector 扩大了覆盖范围，除了实例外，还增加了对驻留在亚马逊弹性容器注册表 (Amazon ECR) Container Registry 中的容器镜像的支持。 EC2 全新 Amazon Inspector 通过集成和基于常见漏洞和风险的持续软件漏洞和网络可访问性扫描（ ）来提供多账户支持。 AWS Organizations CVEs我们鼓励探索和使用这些功能以及其他新的和改进的功能，并从显著增强的安全价值中受益。要了解全新 Amazon Inspector 的功能和定价，请参阅 Amazon Inspector。要了解如何移到新的 Amazon Inspector，请参阅Amazon Inspector Classic。

Amazon Inspector Classic 会测试您的亚马逊 EC2 实例的网络可访问性以及在这些实例上运行的应用程序的安全状态。Amazon Inspector Classic 会自动评估应用程序的暴露、漏洞以及偏离最佳实践的情况。执行评估后，Amazon Inspector Classic 将生成按严重级别组织的安全结果的详细列表。

借助 Amazon Inspector Classic，您可以在整个开发和部署管道或静态生产系统中实现安全漏洞评估的自动化。这使您能够将安全测试作为开发和 IT 操作的常规部分。

Amazon Inspector Classic 还提供名为代理的预定义软件，您可以选择将其安装在要评估的 EC2 实例的操作系统中。代理监控 EC2 实例的行为，包括网络、文件系统和进程活动。它还收集各种行为和配置数据（遥测）。

> **Important**
>
> AWS 并不能保证遵循所提供的建议可以解决所有潜在的安全问题。Amazon Inspector Classic 生成的调查结果取决于您选择的每个评估模板中包含的规则包、系统中是否存在非AWS 组件以及其他因素。您应对在 AWS 服务上运行的应用程序、流程和工具的安全性负责。有关更多信息，请参阅用于保证安全的AWS 责任共担模型。

> **Note**
>
> AWS 负责保护运行 AWS 云端提供的服务的全球基础架构。该基础架构由运行 AWS 服务的硬件、软件、网络和设施组成。 AWS 提供了来自第三方审计师的几份报告，这些审计师已验证我们遵守了各种计算机安全标准和法规。有关更多信息，请参阅AWS 云合规性。

有关 Amazon Inspector Classic 术语的信息，请参阅 Amazon Inspector Classic 术语和概念。

Amazon Inspector Classic 的优势

以下是 Amazon Inspector Classic 的一些主要优势：

- 将自动安全检查集成到您的常规部署和生产流程中 — 评估 AWS 资源的安全性，以进行取证、故障排除或主动审计。在开发过程中运行评估，或在稳定的生产环境中运行评估。
- 查找应用程序安全问题 – 自动实施应用程序安全评估并主动发现漏洞。这使您能够快速开发和迭代新应用程序，并评估对最佳实践和政策的遵从性。
- 更深入地了解您的 AWS 资源 — 通过查看 Amazon Inspector Classic 得出的调查结果，随时了解 AWS 资源的活动和配置数据。

Amazon Inspector Classic 的功能

以下是 Amazon Inspector Classic 的一些主要功能：

- 配置扫描和活动监控引擎 – Amazon Inspector Classic 提供分析流和资源配置的代理。它还监控活动以确定评估目标的情况、行为方式及其依赖组件。此遥测的组合全面展示了目标及其潜在的安全或合规问题。
- 内置内容库 – Amazon Inspector Classic 包含一个内置的规则和报告库。这包括针对最佳实践、常见合规性标准和漏洞进行的检查。检查包括用于解决潜在安全问题的详细建议步骤。
- 通过 API 的自动化 – Amazon Inspector Classic 可通过 API 完全自动执行。这使您能够将安全测试引入到开发和设计过程中，包括选择、执行和报告这些测试的结果。

访问 Amazon Inspector Classic

您可以通过以下任何方式使用 Amazon Inspector Classic 服务：

Amazon Inspector Classic 控制台

登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。

该控制台是一个基于浏览器的接口，可让您访问和使用 Amazon Inspector Classic 服务。

AWS SDKs

AWS 提供软件开发套件 (SDKs)，其中包括适用于各种编程语言和平台的库和示例代码。这包括 Java、Python、Ruby、.NET、iOS、Android 等。它们 SDKs 提供了一种便捷的方式来创建对 Amazon Inspector Classic 服务的编程访问权限。有关信息 AWS SDKs，包括如何下载和安装它们，请参阅适用于 Amazon Web Services 的工具。

Amazon Inspector Classic HTTPS API

你可以使用 Amazon Inspector Classic HTTPS API AWS 以编程方式访问亚马逊 Inspector Classic，它允许你直接向服务发出 HTTPS 请求。有关更多信息，请参阅Amazon Inspector Classic API 参考。

AWS 命令行工具

您可以使用 AWS 命令行工具在系统的命令行上运行命令以执行 Amazon Inspector Classic 任务。如果要生成执行 AWS 任务的脚本，命令行工具也很有用。有关更多信息，请参阅 Amazon Inspector 经典 AWS 命令行界面。

Amazon Inspector Classic 术语和概念

当您开始使用 Amazon Inspector Classic 时，了解其关键概念会很有用。

Amazon Inspector Classic 代理

可以在评估目标中包含的 EC2 实例上安装的软件代理。此代理收集各种配置数据（遥测）。有关更多信息，请参阅 Amazon Inspector Classic 代理。

评估运行

通过针对指定规则包分析评估目标的配置来发现潜在安全问题的过程。在评估运行期间，Amazon Inspector 将监控、收集和分析指定目标内各项资源的配置数据（遥测）。接下来，Amazon Inspector 将分析这些数据并将其与评估运行期间使用的评估模板中指定的一组安全规则包进行比较。已完成的评估运行将生成一个结果列表，这些结果是各种严重性的潜在安全问题。有关更多信息，请参阅 Amazon Inspector Classic 评估模板和评估运行。

评估目标

在 Amazon Inspector Classic 环境中，以单元形式运行来帮助您完成业务目标的 AWS 资源的集合。Amazon Inspector Classic 将评估构成评估目标的响应的安全状况。

> **Important**
>
> 目前，您的 Amazon Inspector Classic 评估目标只能由 EC2实例组成。有关更多信息，请参阅 Amazon Inspector Classic 服务限制。

要创建 Amazon Inspector Classic 评估目标，您必须首先使用您选择的键值对来标记您的 EC2 实例。接下来，您可以创建这些带有常用键或常用值的已标记 EC2 实例的视图。有关更多信息，请参阅 Amazon Inspector Classic 评估目标。

评估模板

评估运行期间使用的配置。模板包含以下内容：

- Amazon Inspector Classic 用来评估您的评估目标的规则包
- 您希望 Amazon Inspector Classic 将有关评估运行状态和结果的通知发送到的 Amazon SNS 主题
- 标签（键值对），您可将其分配给评估运行所生成的结果
- 评估运行的持续时间

调查发现

指定目标的评估运行期间 Amazon Inspector Classic 发现的潜在安全问题。结果将显示在 Amazon Inspector Classic 控制台中或通过 API 进行检索。它们包含安全问题的详细描述和有关如何解决该问题的建议。有关更多信息，请参阅 Amazon Inspector Classic 能取得的结果。

规则

在 Amazon Inspector Classic 环境中，在评估运行期间执行的安全检查。当规则检测到潜在安全问题时，Amazon Inspector Classic 将生成一个描述该问题的结果。

规则包

在 Amazon Inspector Classic 的背景下，这是规则集合。规则包对应于您可能具有的安全目标。您可在创建 Amazon Inspector Classic 评估模板时选择适用的规则包来指定安全目标。有关更多信息，请参阅 Amazon Inspector Classic 规则包和规则。

遥测

EC2 实例的已安装软件包信息和软件配置。Amazon Inspector Classic 在评估运行期间收集数据。

Amazon Inspector Classic 服务限制

下表显示 AWS 账户的 Amazon Inspector Classic 限制。

> **Important**
>
> 目前，您的评估目标只能包含实 EC2 例。

下面是每个 AWS 账户在每个区域的 Amazon Inspector Classic 限制：

资源	默认限制	评论
正在运行的评估中的实例数	500	每个区域每个账户在所有正在运行的评估中可以包含的最大 EC2 实例数。
评估运行数	50000	可为每个区域的每个账户创建的评估运行的最大数量。只要用于这些运行的评估目标不包含重叠的 EC2 实例，您就可以同时进行多个评估。
评估模板	500	您在任何给定时间可在每个区域的每个账户中拥有的评估模板的最大数量。
评估目标	50	每个区域的每个账户在任何给定时间可拥

资源	默认限制	评论
		有的评估目标的最大数量。

除非另有说明，否则可联系 AWS 支持 中心根据请求提高这些限制。

Amazon Inspector Classic 定价

Amazon Inspector Classic 的定价基于每次评估中包含的 EC2 实例数量以及这些评估中使用的规则包。

网络可到达性规则包的定价

使用网络可到达性规则包的 Amazon Inspector Classic 评估按每月每个实例的每次评估（实例评估）定价。例如，如果您对 1 个实例运行 1 次评估，那就是 1 个实例评估。如果您对 10 个实例运行 1 次评估，那就是 10 个实例评估。每月每实例评估的起价为 0.15 美元，算上批量折扣，每月每实例评估可低至 0.04 美元。

免费试用详情

前 90 天使用 Amazon Inspector Classic	每实例评估价格
前 250 次实例评估	0.00

定价详细信息

在给定月份	每实例评估价格
前 250 次实例评估	0.15 美元
接下来的 750 次实例评估	0.13 美元
接下来的 4,000 次实例评估	0.10 美元
接下来的 45,000 次实例评估	0.07 美元

在给定月份	每实例评估价格
所有其他实例评估	0.04 美元

主机评估规则包定价

对于评估中包含的常见漏洞和暴露 (CVE)、互联网安全中心 (CIS) 基准、安全最佳实践和运行时行为分析的任意组合

Amazon Inspector Classic 的主机评估规则包使用部署在运行您要评估的应用程序的亚马逊 EC2 实例上的代理。使用主机规则包的评估按每月每个代理每次评估（代理评估）定价。例如，如果您对 1 个代理进行 1 次评估，那就是 1 个代理评估。如果您对 10 个代理进行 1 次评估，那就是 10 个代理评估。每月每个代理评估的起价为 0.30 美元，算上批量折扣，每月每个代理评估可低至 0.05 美元。

免费试用详情

前 90 天使用 Amazon Inspector Classic	每代理评估价格
前 250 次代理评估	0.00

定价详细信息

在给定月份	每代理评估价格
前 250 次代理评估	0.30 美元
接下来的 750 次代理评估	0.25 美元
接下来的 4,000 次代理评估	0.15 美元
接下来的 45,000 份代理评估	0.10 美元
所有其他代理评估	0.05 美元

Amazon Inspector Classic 支持的操作系统和区域

本章提供有关 Amazon Inspector Classic 支持的操作系统和 AWS 区域的信息。

> **Important**
>
> 目前，Amazon Inspector Classic 评估目标只能包含 EC2 实例。无论操作系统如何，您都可以使用网络可到达性规则包在任何 EC2 实例上运行无代理评估。

有关能够跨支持的操作系统使用的 Amazon Inspector Classic 规则包的信息，请参阅支持的操作系统的 Amazon Inspector Classic 规则包。

主题

- Amazon Inspector Classic 代理支持的基于 Linux 的操作系统
- Amazon Inspector Classic 代理支持的基于 Windows 的操作系统
- 支持的 AWS 区域

Amazon Inspector Classic 代理支持的基于 Linux 的操作系统

您可在 64 位 x86 和 Arm EC2 实例上使用 Amazon Inspector Classic 代理。代理与以下版本的基于 Linux 的操作系统兼容：

- 64 位 x86 实例
  - Amazon Linux 2
  - Amazon Linux (2018.03、2017.09、2017.03、2016.09、2016.03、2015.09、2015.03、2014.09、2014.03、2013.09、
  - Ubuntu (20.04 LTS、18.04 LTS、16.04 LTS、14.04 LTS)
  - Debian (10.x、9.0 - 9.5、8.0 - 8.7)
  - 红帽企业 Linux (8.x、7.2、6.2-6.9)
  - CentOS (7.2 - 7.x、6.2 - 6.9)
- Arm 实例
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS、16.04 LTS)

Amazon Inspector Classic 代理支持的基于 Windows 的操作系统

您只能在运行以下基于 Windows 的操作系统的 64 位版本的 EC2 实例上使用 Amazon Inspector Classic 代理：

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

支持的 AWS 区域

以下 AWS 区域支持 Amazon Inspector Classic：

- 美国东部（俄亥俄）us-east-2
- 美国东部（弗吉尼亚州北部）us-east-1
- 美国西部（加利福尼亚北部）us-west-1
- 美国西部（俄勒冈）us-west-2
- 亚太地区（孟买）ap-south-1
- 亚太地区（首尔）ap-northeast-2
- 亚太地区（悉尼）ap-southeast-2
- 亚太地区（东京）ap-northeast-1
- 欧洲（法兰克福）eu-central-1
- 欧洲（爱尔兰）eu-west-1
- 欧洲地区（伦敦） eu-west-2
- 欧洲地区（斯德哥尔摩）eu-north-1
- AWS GovCloud （美国东部） gov-us-east-1
- AWS GovCloud （美国西部） gov-us-west-1

> **Note**
>
> 网络可访问性规则包不在 AWS GovCloud （美国）地区提供。

Amazon Inspector Classic

经过深思熟虑，我们决定自2026年5月20日起终止对Amazon Inspector Classic的支持。从 2025 年 5 月 20 日起，亚马逊 Inspector Classic 将不再接受新客户。作为账户在 2025 年 5 月 20 日之前注册该服务的现有客户，您可以继续使用 Amazon Inspector Classic 功能。2026 年 5 月 20 日之后，您将无法再使用亚马逊 Inspector Classic。

全新 Amazon Inspector 现已在全球 AWS 区域上市。全新 Amazon Inspector 是现有 Amazon Inspector（现名为 Amazon Inspector Classic）的完全重新架构和重新设计的版本。以下功能是 Amazon Inspector 的主要增强功能：

- 专为扩展而构建 – 全新 Amazon Inspector 专为扩展和动态云环境而打造。账户中可扫描的实例或图像数量没有限制。
- 支持容器映像 – 全新 Amazon Inspector 还会扫描位于 Amazon Elastic Container Registry (Amazon ECR)中的容器映像，以查找软件漏洞。
- 支持多账户管理 – 全新 Amazon Inspector 已与 Organizations 集成。这允许您为组织的 Amazon Inspector 委托管理员账户。委托管理员账户是集中式账户，整合了所有检查结果，可配置所有成员账户。
- 使用 AWS Systems Manager 代理（SSM 代理）— 有了新的 Amazon Inspector，您不再需要在所有 EC2 实例上安装和维护独立的 Amazon Inspector 代理。全新 Amazon Inspector 利用了广泛部署的 SSM 代理。
- 自动和持续扫描 – 通过 Amazon Inspector Classic，可手动设置评估目标、评估模板并配置评估频率。但是，新版本的 Amazon Inspector 会自动检测所有新启动的 EC2 实例和推送到 Amazon ECR 的符合条件的容器镜像，并立即扫描它们是否存在软件漏洞和意外网络泄露。资源会根据多个触发因素自动重新扫描，包括正在启动的新 EC2 实例、推送到 Amazon ECR 的容器映像、在 EC2 实例中安装新软件包、安装补丁或发布影响资源的新常见漏洞和暴露 (CVE)。
- Amazon Inspector 风险评分 – 全新 Amazon Inspector 计算 Amazon Inspector 风险评分，以帮助确定检查结果的优先顺序。风险评分是通过将 up-to-date CVE信息与时间和环境因素（例如网络可访问性和可利用性信息）关联来计算的。
- 更多集成 — 所有发现都汇总到新设计的 Amazon Inspector 控制台中，并推送到 AWS Security Hub CSPM 和亚马逊， EventBridge 以实现工单等工作流程的自动化。与容器映像相关的结果也会推送到 Amazon ECR。

要了解全新 Amazon Inspector 的所有功能和定价，请参阅《Amazon Inspector 用户指南》。

虽然我们会在一段时间内继续支持 Amazon Inspector Classic，并且客户可以在同一个账户中同时使用全新 Amazon Inspector 和 Amazon Inspector Classic，但我们强烈建议您迁移到新的 Amazon Inspector。以下各节将全程引导您从 Amazon Inspector Classic 迁移到全新 Amazon Inspector。

主题

步骤 1：（可选）导出评估报告和检查结果

要在 Amazon Inspector Classic 中保存评估报告和检查结果，请生成一份评估报告。

要生成评测报告

1. 在 Assessment runs (评估运行) 页面上，找到要为其生成报告的评估运行。确保其状态设置为 分析完成。
2. 在该评估运行的 Reports (报告) 列下，选择报告图标。

   > **Important**
   >
   > 仅为 2017 年 4 月 25 日后已执行的或将执行的评估运行的 Reports (报告) 列中显示报告图标。也就是说，当 Amazon Inspector Classic 中的评估报告变得可用时。

3. 在 评估报告 对话框中，选择要查看的报告的类型（结果报告或完整报告）和报告格式（HTML 或 PDF）。然后选择 Generate report (生成报告)。

步骤 2：删除 Amazon Inspector Classic 中所有计划的评估运行

要禁用 Amazon Inspector Classic，请删除账户中所有活动 AWS 区域中的评估模板。删除评估模板会中止所有计划的未来评估运行。

删除评估模板

- 在 Assessment Templates (评估模板) 页面上，选择要删除的模板，然后选择 Delete (删除)。当系统提示您确认时，选择是。

> **Important**
>
> 当您删除某个评估模板时，与此模板关联的所有评估运行、报告的结果和版本也将被删除。

步骤 3：启用新的 Amazon Inspector

您可以使用 AWS 管理控制台 或新的亚马逊 Inspector 启用新的 Amazon Inspector APIs。要开始使用新的 Amazon Inspector，请参阅《Amazon Inspector 用户指南》中的入门。

Amazon Inspector Classic 入门

本教程介绍如何设置 Amazon Inspector Classic 并通过创建和运行您的第一个评估来开始使用。

注册获取 AWS 账户

要开始使用 AWS，你需要一个 AWS 账户。有关创建的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》 AWS 账户中的入门指南。

One-click 设置

以下过程向您展示了如何使用预先构建的模板和预定义的计划参数（每周一次或仅限一次）在当前和的所有可用亚马逊弹性计算云 (Amazon EC2) 实例上创建和运行自动评估。 AWS 账户 AWS 区域

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在 Welcome (欢迎) 页面上，选择要运行的评估的类型。网络评估会分析您 AWS 环境的网络配置是否存在漏洞，并且不需要 Amazon Inspector Classic 代理。主机评估 分析您的 EC2 实例的主机上软件和配置有无漏洞，并且需要在 EC2 实例上安装代理。

   选择 Run weekly (recommended) (每周运行(建议)) 或 Run once (运行一次)。选择之后，该服务会自动为您创建评估。具体来说，该服务执行以下操作：

   a. 创建服务相关角色。

      > **Note**
      >
      > Amazon Inspector Classic 需要枚举您的 EC2 实例和标签来识别评估目标中指定的 EC2 实例。Amazon Inspector Classic 通过名为 `AWSServiceRoleForAmazonInspector` 的服务相关角色访问 AWS 账户 资源。有关服务相关角色的更多信息，请参阅对 Amazon Inspector Classic 使用服务相关角色和使用 Service-Linked 角色。

   b. 如果适用，请在您 AWS 账户 和地区的所有可用的 EC2 实例上安装 Amazon Inspector Classic 代理。

> **Note**
>
> 该服务仅在那些允许 AWS Systems Manager 运行命令的 EC2 实例上安装 Amazon Inspector Classic 代理。要使用此选项，请确保您的所有 EC2 实例都处于当前状态，并且已安装 SSM 代理， AWS 账户 并且 AWS 区域 具有允许 Run Command 的 IAM 角色。有关更多信息，请参阅 使用 Systems Manager Run Command 在多个 EC2 实例上安装代理。

c. 将这些实例添加至评估目标。

d. 通过一组标准化的规则包将该目标包含在评估模板中。

e. 根据您选择的是 Run weekly (recommended) (每周运行(建议)) 还是 Run once (运行一次)，每周运行一次评估或只运行一次评估。

3. 在确认对话框中，选择确定。Amazon Inspector Classic 会自动运行评估。

高级设置

以下过程说明如何选择要在评估目标和模板中包含的特定 Amazon EC2 实例、规则包和计划参数。

1. 在 Welcome (欢迎) 页面上，选择 Advanced setup (高级设置)。
2. 在 Define an assessment target (定义评估目标) 页面上，输入评估目标的名称。
3. 对于所有实例，您可以将复选框保持选中状态，将您 AWS 账户 和地区的所有 EC2 实例都包括在评估目标中。如果您想选择要包含的 EC2 实例，请清除所有实例复选框，然后输入与目标 EC2 实例关联的密钥和值标签。有关标记 EC2 实例的更多信息，请参阅标记 Amazon EC2 资源。
4. 对于 安装代理，如果实例允许 System Manager Run Command，则可保留该复选框的默认选中状态。该服务在评估目标中允许的所有 EC2 实例上安装 Amazon Inspector Classic 代理 AWS Systems Manager。要使用此选项，请确保您的所有 EC2 实例都处于当前状态，并且已安装 SSM 代理， AWS 账户 并且 AWS 区域 具有允许 Run Command 的 IAM 角色。有关更多信息，请参阅使用 Systems Manager Run Command 在多个 EC2 实例上安装代理。如果要手动安装该代理，请参阅安装 Amazon Inspector 代理。
5. 选择下一步。
6. 在 Define an assessment template (定义评估模板) 页面上，输入评估模板的名称。
7. 对于 Rules packages (规则包)，选择要在评估模板中包含的规则包。有关规则包的更多信息，请参阅 Amazon Inspector 规则包和规则。
8. 对于 Duration (持续时间)，请选择评估运行的持续时间。

9. 对于 评估计划，可以设置周期性评估运行的计划。
10. 选择下一步。
11. 在 Review (审核) 页面上，查看您针对评估目标和模板所做的选择。如果对配置满意，请选择 创建。如果为评估模板设置了评估计划，评估将在您选择 Create (创建) 后立即自动运行。

> **Note**
>
> Amazon Inspector Classic 需要枚举您的 EC2 实例和标签来识别评估目标中指定的 EC2 实例。Amazon Inspector Classic AWS 账户 可以通过名`AWSServiceRoleForAmazonInspector`为的服务相关角色访问您的这些资源。有关使用 Amazon Inspector Classic 服务相关角色的更多信息，请参阅 对 Amazon Inspector Classic 使用服务相关角色。有关服务相关角色的详细信息，请参阅《AWS Identity and Access Management 用户指南》中的使用服务相关角色。

12. 如果未设置评估计划，请通过控制台导航到评估模板，然后选择 Run (运行)。
13. 要跟踪评估运行的进度，请在控制台的导航窗格中选择 Assessment runs (评估运行)，然后选择 Findings (结果)。有关结果的更多信息，请参阅 Amazon Inspector Classic 能取得的结果。

Amazon Inspector Classic 教程

以下教程介绍如何在 Red Hat Enterprise Linux 和 Ubuntu 操作系统执行 Amazon Inspector Classic 评估运行。

教程

- 教程：通过 Red Hat Enterprise Linux 使用 Amazon Inspector Classic
- 教程：通过 Ubuntu Server 使用 Amazon Inspector Classic

Amazon Inspector Classic 教程 - Red Hat Enterprise Linux

在按照本教程中的说明进行操作之前，建议您熟悉一下 Amazon Inspector Classic 术语和概念。

本教程演示如何使用 Amazon Inspector Classic 分析运行 Red Hat Enterprise Linux 7.5 操作系统的 EC2 实例的行为。它提供了 step-by-step有关如何浏览 Amazon Inspector Classic 工作流程的说明。该工作流程包括准备 Amazon EC2 实例、运行评估模板以及执行评估结果中生成的建议安全修复。如果您是首次接触的用户并且要通过一键单击来设置和运行 Amazon Inspector Classic 评估，请参阅创建基本评估。

主题

- 步骤 1：设置 Amazon EC2 实例，与 Amazon Inspector Classic 配合使用
- 步骤 2：修改 Amazon EC2 实例
- 步骤 3：创建评估目标并在 EC2 实例上安装代理
- 步骤 4：创建和运行评估模板
- 步骤 5：找到并分析您的结果
- 步骤 6：将推荐的修复应用于评估目标

步骤 1：设置 Amazon EC2 实例，与 Amazon Inspector Classic 配合使用

在本教程中，将创建一个运行 Red Hat Enterprise Linux 7.5 的 EC2 实例，并使用 Name 密钥和值 **`InspectorEC2InstanceLinux`**为其添加标签。

> **Note**
>
> 有关为 EC2 实例添加标签的更多信息，请参阅资源和标签。

步骤 2：修改 Amazon EC2 实例

在本教程中，您将修改目标 EC2 实例以了解潜在安全问题 CVE-2018-1111。欲了解更多信息，请参阅 https://cve.mitre。 org/cgi-bin/cvename.cgi？ name=cve -2018-1111 和。常见漏洞和风险

连接到实例 **InspectorEC2InstanceLinux** 并运行以下命令：

```
sudo yum install dhclient-12:4.2.5-68.el7
```

关于连接到 EC2 实例方法的说明，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的连接到您的实例。

步骤 3：创建评估目标并在 EC2 实例上安装代理

Amazon Inspector Classic 使用评估目标指定要评估的 AWS 资源。

创建评估目标并在 EC2 实例上安装代理

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择 Assessment targets (评估目标)，然后选择 Create (创建)。

   执行以下操作：

   a. 对于 Name (名称)，输入评估目标的名称。

      在本教程中，请输入 **MyTargetLinux**。

   b. 对于使用标签，在密钥字段和值字段中输入值，以选择要包含在此评估目标中的 EC2 实例。

      在本教程中，通过在密钥字段中输入 **Name** 并在 值字段中输入 **InspectorEC2InstanceLinux**，选择上一步创建的 EC2 实例。

      要在评估目标中包含您的 AWS 账户和区域中的所有 EC2 实例，请选中 所有实例 复选框。

   c. 选择保存。

d. 在标记的 EC2 实例上安装 Amazon Inspector Classic 代理。要在评估目标中包含的所有 EC2 实例上安装代理，请选中 Install Agents (安装代理) 复选框。

> **Note**
>
> 您还可使用 AWS Systems Manager Run Command 来安装 Amazon Inspector Classic 代理。要在评估目标中的所有实例上安装代理，您可以指定您在创建评估目标时使用的相同标签。您也可以在 EC2 实例上手动安装 Amazon Inspector Classic 代理。有关更多信息，请参阅 安装 Amazon Inspector Classic 代理。

e. 选择 Save。

> **Note**
>
> 此时，Amazon Inspector Classic 将创建名为 `AWSServiceRoleForAmazonInspector`的服务相关角色。此角色向 Amazon Inspector Classic 授予对您的资源的必需访问权限。有关更多信息，请参阅 为 Amazon Inspector Classic 创建服务相关角色。

步骤 4：创建和运行评估模板

创建并运行您的模板

1. 在导航窗格中，选择 Assessment templates (评估模板)，然后选择 Create (创建)。
2. 对于 Name (名称)，输入评估模板的名称。在本教程中，请输入 **`MyFirstTemplateLinux`**。
3. 对于 Target name (目标名称)，请选择上面创建的评估目标 **`MyTargetLinux`**。
4. 对于 Rules packages (规则包)，选择要在此评估模板中使用的规则包。

   在本教程中，选择 Common Vulnerabilities and Exposures-1.1 (常见漏洞和风险-1.1)。
5. 对于持续时间，为评估模板指定持续时间。

   在本教程中，请选择 15 minutes (15 分钟)。
6. 选择创建并运行。

步骤 5：找到并分析您的结果

已完成的评估运行将生成一组结果，或生成 Amazon Inspector Classic 在评估目标中发现的潜在安全问题。您可以查看结果并执行推荐步骤以解决潜在安全问题。

在本教程中，如果完成了上述步骤，评估运行将生成针对常见漏洞 CVE-2018-1111 的结果。

找到并分析您的结果

1. 在导航窗格中，选择 Assessment runs (评估运行)。验证名为的评估模板的运行状态MyFirstTemplateLinux是否设置为收集数据。这表示该评估运行当前正在进行，并且系统正在针对所选规则包收集和分析您的目标的遥测数据。
2. 您无法查看由仍在进行的评估运行生成的结果。让评估运行完成其整个持续时间。但是，在本教程中，您可以在几分钟后停止该运行。

   状态首先MyFirstTemplateLinux更改为 “正在停止”，然后在几分钟后更改为 “分析”，最后变为 “分析完成”。要查看状态的这些变化，请选择 Refresh (刷新) 图标。
3. 在导航窗格中，选择 调查发现。

   你可以看到一个名为 Instance Ins pector 的高严重性新发现EC2InstanceLinux 容易受到 CVE-2018-1111 的攻击。

   > **Note**
   >
   > 如果没有看到该新结果，请选择 Refresh (刷新) 图标。

   要展开视图并查看此结果的详细信息，请选择结果左侧的箭头。结果的详细信息包含以下内容：

   - 结果的 ARN
   - 生成此结果的评估运行的名称
   - 生成此结果的评估目标的名称
   - 生成此结果的评估模板的名称
   - 评估运行开始时间
   - 评估运行结束时间
   - 评估运行状态
   - 包含触发了此结果的规则的规则包的名称

- Amazon Inspector Classic 代理 ID
- 结果的名称
- 结果的严重性
- 结果的描述
- 建议的补救步骤，您可完成这些步骤来修复结果描述的潜在安全问题

步骤 6：将推荐的修复应用于评估目标

在本教程中，您已修改评估目标以了解潜在安全问题 CVE-2018-1111。在此过程中，您可以将推荐的修复应用于此问题。

将修复应用于目标

1. 连接到上一节中创建的实例 **InspectorEC2InstanceLinux**，然后运行以下命令：

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```
2. 在评估模板页面上 MyFirstTemplateLinux，选择，然后选择运行，使用此模板开始新的评估。
3. 按照中的步骤操作步骤 5：找到并分析您的结果，查看后续运行MyFirstTemplateLinux模板后得出的结果。

   由于您已解决 CVE-2018-1111 安全问题，因此，应将不会再看到此问题的结果。

Amazon Inspector Classic 教程 - Ubuntu Server

在按照本教程中的说明进行操作之前，建议您熟悉一下 Amazon Inspector Classic 术语和概念。

本教程演示如何使用 Amazon Inspector Classic 分析运行 Ubuntu Server 16.04 LTS 操作系统的 EC2 实例的行为。它提供了 step-by-step有关如何浏览 Amazon Inspector Classic 工作流程的说明。

如果您是首次接触的用户并且要通过一键单击来设置和运行 Amazon Inspector Classic 评估，请参阅创建基本评估。

主题

- 步骤 1：设置 Amazon EC2 实例，与 Amazon Inspector Classic 配合使用
- 步骤 2：创建评估目标并在 EC2 实例上安装代理
- 步骤 3：创建和运行评估模板

步骤 1：设置 Amazon EC2 实例，与 Amazon Inspector Classic 配合使用

设置 EC2 实例

- 在本教程中，将运行 Ubuntu Server 16.04 LTS 创建一个 EC2 实例，并使用 Name 密钥和值 为其添加标签**InspectorEC2InstanceUbuntu**。

> **Note**
>
> 有关为 EC2 实例添加标签的更多信息，请参阅资源和标签。

步骤 2：创建评估目标并在 EC2 实例上安装代理

Amazon Inspector Classic 使用评估目标指定要评估的 AWS 资源。

创建评估目标并在 EC2 实例上安装代理

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择 Assessment targets (评估目标)，然后选择 Create (创建)。
3. 对于 Name (名称)，输入评估目标的名称。

   在本教程中，请键入 **MyTargetUbuntu**。
4. 对于使用标签，在密钥字段和值字段中输入值，以选择要包含在此评估目标中的 EC2 实例。

   在本教程中，通过在密钥字段中输入 **Name** 并在 值字段中输入 **InspectorEC2InstanceUbuntu**，选择上一步创建的 EC2 实例。

   要在评估目标中包含您的 AWS 账户和区域中的所有 EC2 实例，请选中 All instances (所有实例) 框。
5. 在标记的 EC2 实例上安装 Amazon Inspector Classic 代理。要在评估目标中包含的所有 EC2 实例上安装代理，请选中 Install Agents (安装代理) 框。

> **Note**
>
> 您还可使用 Systems Manager Run Command 来安装 Amazon Inspector 代理。要在评估目标中的所有实例上安装代理，您可以指定用于创建评估目标的相同标签。您也可以在 EC2 实例上手动安装 Amazon Inspector 代理。有关更多信息，请参阅 安装 Amazon Inspector Classic 代理。

6. 选择 Save。

> **Note**
>
> 此时，将创建一个名为 `AWSServiceRoleForAmazonInspector` 的服务相关角色来授予 Amazon Inspector Classic 访问您的资源的权限。有关更多信息，请参阅 为 Amazon Inspector Classic 创建服务相关角色。

步骤 3：创建和运行评估模板

创建并运行您的模板

1. 如果使用的是 Advanced setup (高级设置)，将定向到 Define an assessment template (定义评估模板) 页面。否则，导航到 Assessment templates (评估模板) 页面，然后选择 Create (创建)。
2. 对于 Name (名称)，输入评估模板的名称。在本教程中，请输入 **`MyFirstTemplateUbuntu`**。
3. 对于 Target name (目标名称)，请选择上面创建的评估目标 **`MyTargetUbuntu`**。
4. 对于 Rules packages (规则包)，使用下拉菜单选择要在此评估模板中使用的规则包。

   在本教程中，选择 Common Vulnerabilities and Exposures-1.1 (常见漏洞和风险-1.1)。
5. 对于持续时间，为评估模板指定持续时间。

   在本教程中，请选择 15 minutes (15 分钟)。
6. 如果使用的是 Advanced setup (高级设置)，请选择 Next (下一步)。在下面的 Review (审核) 页面上，选择 Create (创建)。否则，请选择 Create and run (创建并运行)。

步骤 4：找到并分析生成的结果

已完成的评估运行将生成一组结果，或生成 Amazon Inspector Classic 在评估目标中发现的潜在安全问题。您可以查看结果并执行推荐步骤以解决潜在安全问题。

1. 导航到 Assessment Runs (评估运行) 页面。验证您在上一步中创建的名为MyFirstTemplateUbuntu的评估模板的运行状态是否设置为收集数据。这表示该评估运行当前正在进行，并且系统正在针对所选规则包收集和分析您的目标的遥测数据。
2. 您无法查看由仍在进行的评估运行生成的结果。让评估运行完成其整个持续时间。

   状态首先MyFirstTemplateUbuntu更改为 “正在停止”，然后在几分钟后更改为 “分析”，最后变为 “分析完成”。要查看状态的这些变化，请选择 Refresh (刷新) 图标。
3. 导航到 Findings (结果) 页面。

   要展开视图并查看结果的详细信息，请选择结果左侧的箭头。结果的详细信息包含以下内容：

   - 结果的 ARN
   - 生成此结果的评估运行的名称
   - 生成此结果的评估目标的名称
   - 生成此结果的评估模板的名称
   - 评估运行开始时间
   - 评估运行结束时间
   - 评估运行状态
   - 包含触发了此结果的规则的规则包的名称
   - Amazon Inspector Classic 代理 ID
   - 结果的名称
   - 结果的严重性
   - 结果的描述
   - 建议的补救步骤，您可完成这些步骤来修复结果描述的潜在安全问题

步骤 5：将推荐的修复应用于评估目标

在此过程中，您将应用更新来修复未发现的问题。

1. 连接到您的实例 **InspectorEC2InstanceUbuntu**，然后执行软件包更新。

2. 在 “评估模板” 页面上 MyFirstTemplateUbuntu，选择，然后选择 “运行”，使用此模板开始新的运行。
3. 按照中的步骤操作步骤 4：找到并分析生成的结果，查看后续运行MyFirstTemplateUbuntu模板后得出的结果。

   软件包更新应已解决第一次运行模板时发现的问题。

Amazon Inspector Classic 安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。 Third-party 作为AWS 合规计划合规计划合规计划合的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon Inspector Classic 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon Inspector Classic 时应用责任共担模式。以下主题说明如何配置 Amazon Inspector Classic 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务以帮助您监控和保护 Amazon Inspector Classic 资源。

主题

Amazon Inspector Classic 中的数据保护

分担责任模式 AWS 分适用于 Amazon Inspector Classic 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还

负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题解答AWS条款。 有关欧洲数据保护的信息，请参阅通用数据保护条例（GDPR）中心。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括你使用控制台、API 或软件开发工具包 AWS 服务 使用 Amazon Inspector Classic 或其他 AWS 软件开发工具包的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

主题

静态数据加密

Amazon Inspector Classic 代理在评估运行期间生成的遥测数据的格式将设置为 JSON 文件。这些文件通过 TLS 近乎实时地传输到 Amazon Inspector Classic，在那里使用每次评估运行的临时派生密钥进行加密。 AWS KMS

这些文件安全地存储在专用于 Amazon Inspector Classic 的 S3 存储桶中。Amazon Inspector Classic 的规则引擎执行以下操作：

- 访问 S3 存储桶中的加密的遥测数据
- 在内存中进行解密
- 根据配置的评估规则处理数据以生成结果

传输中数据加密

作为一项托管服务，Amazon Inspector Classic 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Amazon Inspector Classic。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（短暂的）或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。 Diffie-Hellman大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

适用于 Amazon Inspector Classic 的 Identity and Access Management

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用 Amazon Inspector 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Amazon Inspector Classic 如何与 IAM 配合使用
- 示例 2：仅允许用户对 Amazon Inspector 结果执行描述和列出操作
- Amazon Inspector 的策略资源
- Amazon Inspector 的策略条件键
- Amazon Inspector 中的 ACL

- ABAC 与 Amazon Inspector
- 将临时凭证用于 Amazon Inspector
- Cross-service Amazon Inspector 的主要权限
- Amazon Inspector 的服务角色
- Service-linked Amazon Inspector 的角色
- Identity-based Amazon Inspector 经典版的政策示例
- 对 Amazon Inspector Classic 使用服务相关角色
- Amazon Inspector Classic 身份和访问问题排查

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅Amazon Inspector Classic 身份和访问问题排查）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅Amazon Inspector Classic 如何与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Identity-based Amazon Inspector 经典版的政策示例）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

Resource-based 策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略（SCP）– 指定 AWS Organizations中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略（RCP）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略（RCP）。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Amazon Inspector Classic 如何与 IAM 配合使用

在使用 IAM 管理对 Amazon Inspector 的访问权限之前，您应该了解哪些 IAM 功能可用于 Amazon Inspector。

可与 Amazon Inspector Classic 结合使用的 IAM 功能

IAM 功能	Amazon Inspector 支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	是
服务角色	否
Service-linked 角色	是

要全面了解 Amazon Inspector 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Identity-based Amazon Inspector 的政策

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Identity-based Amazon Inspector 的政策示例

要查看 Amazon Inspector 基于身份的策略的示例，请参阅Identity-based Amazon Inspector 经典版的政策示例。

Resource-based 亚马逊 Inspector 中的政策

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Amazon Inspector 的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

有关 Amazon Inspector 操作的列表，请参阅《服务授权参考》中的 Amazon Inspector 定义的操作。

Amazon Inspector 中的策略操作在操作前使用以下前缀：

```
inspector
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

以下权限策略向用户授予运行以 Describe 和 List 开头的所有操作的权限。这些操作显示有关 Amazon Inspector 资源（如评估目标或结果）的信息。Resource 元素中的通配符 (*) 表示可对该账户拥有的所有 Amazon Inspector 资源执行操作。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

示例 2：仅允许用户对 Amazon Inspector 结果执行描述和列出操作

以下权限策略向用户授予仅运行 ListFindings 和 DescribeFindings 操作的权限。这些操作显示有关 Amazon Inspector 结果的信息。Resource 元素中的通配符 (*) 表示可对该账户拥有的所有 Amazon Inspector 资源执行操作。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

要查看 Amazon Inspector 基于身份的策略的示例，请参阅Identity-based Amazon Inspector 经典版的政策示例。

Amazon Inspector 的策略资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Amazon Inspector 的资源类型及其 ARN 的列表，请参阅《服务授权参考》中的由 Amazon Inspector Classic 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon Inspector Classic 定义的操作。

要查看 Amazon Inspector 基于身份的策略的示例，请参阅Identity-based Amazon Inspector 经典版的政策示例。

Amazon Inspector 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Amazon Inspector 条件键的列表，请参阅《服务授权参考》中的 Amazon Inspector Classic 的条件键。要了解您可以对哪些操作和资源使用条件键，请参阅 Amazon Inspector Classic 定义的操作。

要查看 Amazon Inspector 基于身份的策略的示例，请参阅Identity-based Amazon Inspector 经典版的政策示例。

Amazon Inspector 中的 ACL

支持 ACL：否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

ABAC 与 Amazon Inspector

支持 ABAC（策略中的标签）：部分支持

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/`*`key-name`*`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证用于 Amazon Inspector

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Cross-service Amazon Inspector 的主要权限

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Amazon Inspector 的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Amazon Inspector 的功能。仅当 Amazon Inspector 提供相关指导时才编辑服务角色。

Service-linked Amazon Inspector 的角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。该服务可以代替您执行操作。 Service-linked 角色出现在您的， AWS 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理 Amazon Inspector 服务相关角色的详细信息，请参阅 对 Amazon Inspector Classic 使用服务相关角色。

Identity-based Amazon Inspector 经典版的政策示例

默认情况下，用户和角色没有创建或修改 Amazon Inspector 资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Amazon Inspector 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 的格式，请参阅《服务授权参考》中的 Amazon Inspector Classic 的操作、资源和条件键。

主题

策略最佳实践

Identity-based 策略决定了是否有人可以在您的账户中创建、访问或删除亚马逊 Inspector 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Amazon Inspector 控制台

要访问 Amazon Inspector Classic 控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您的 AWS 账户中的 Amazon Inspector 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon Inspector 控制台，还需要将亚马逊检查器*ConsoleAccess*或*ReadOnly* AWS 托管策略附加到这些实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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": "*"
        }
    ]
}
```

仅允许用户对 Amazon Inspector 结果执行描述和列出操作

以下权限策略向用户授予仅运行 `ListFindings` 和 `DescribeFindings` 操作的权限。这些操作显示有关 Amazon Inspector 结果的信息。`Resource` 元素中的通配符 (*) 表示可对该账户拥有的所有 Amazon Inspector 资源执行操作。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

对 Amazon Inspector Classic 使用服务相关角色

Amazon Inspector Classic 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 Amazon Inspector Classic。 Service-linked 角色由 Amazon Inspector Classic 预定义，包括该服务 AWS 服务 代表您呼叫他人所需的所有权限。

服务相关角色可让您更轻松地设置 Amazon Inspector Classic，因为您不必手动添加必要的权限。Amazon Inspector Classic 定义其服务相关角色的权限，除非另外定义，否则只有 Amazon Inspector Classic 可以代入该角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这将保护您的 Amazon Inspector Classic 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的AWS 服务，并在Service-linked 角色列中查找标有 “是” 的服务。请选择是与查看该服务的服务关联角色文档的链接。

Service-linked Amazon Inspector 经典版的角色权限

Amazon Inspector Classic 使用名为 AWSServiceRoleForAmazonInspector—ServiceLinkedRoleDescription 的服务相关角色。

AWSServiceRoleForAmazonInspector 服务相关角色信任以下服务来代入该角色：

- `inspector.amazonaws.com`

名为的角色权限策略 AmazonInspectorServiceRolePolicy 允许 Amazon Inspector Classic 对指定资源完成以下操作：

- 操作：`arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector` 上的 `iam:CreateServiceLinkedRole`

必须配置权限，允许 IAM 实体（如 IAM 用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的Service-linked 角色权限。

为 Amazon Inspector Classic 创建服务相关角色

您无需手动创建服务关联角色。当你 CompleteThisCreateActionInThisService 在 AWS 管理控制台、或 AWS API 中时 AWS CLI，Amazon Inspector Classic 会为你创建服务相关角色。

为 Amazon Inspector Classic 编辑服务相关角色

Amazon Inspector Classic 不允许您编辑 AWSServiceRoleForAmazonInspector 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除适用于 Amazon Inspector Classic 的服务相关角色

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时，Amazon Inspector Classic 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 **`AWSServiceRoleForAmazonInspector`** 使用的 Amazon Inspector Classic 资源

- AWS 账户 在你运行 Amazon Inspector Classic 的所有 AWS 区域 地方，删除你的评估目标。有关更多信息，请参阅 Amazon Inspector Classic 评估目标。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAmazonInspector服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

Amazon Inspector Classic 服务相关角色支持的区域

Amazon Inspector Classic 支持在该服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

Amazon Inspector Classic 身份和访问问题排查

您可以使用以下信息，帮助诊断和修复在使用 Amazon Inspector 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Amazon Inspector 中执行操作
- 我无权执行 iam：PassRole

- 我想允许我以外的人进入 AWS 账户 访问我的 Amazon Inspector 资源

我无权在 Amazon Inspector 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 inspector:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 inspector:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，指明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon Inspector。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon Inspector 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人进入 AWS 账户 访问我的 Amazon Inspector 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon Inspector 是否支持这些功能，请参阅Amazon Inspector Classic 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Amazon Inspector Classic 中的日志记录和监控

Amazon Inspector Classic 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Amazon Inspector Classic 中采取的操作的记录。 CloudTrail 将亚马逊 Inspector Classic 的所有 API 调用捕获为事件，包括来自亚马逊 Inspector Classic 控制台的调用和对亚马逊 Inspector Classic API 操作的代码调用

有关在 Amazon Inspector Classic 中使用 CloudTrail 登录功能的信息，请参阅使用记录 Amazon Inspector 经典 API 调用 AWS CloudTrail。

您可以使用亚马逊监控 Amazon Inspector Classic CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。默认情况下，Amazon Inspector Classic 会 CloudWatch 在 5 分钟内向发送指标数据。

有关 CloudWatch 与 Amazon Inspector Classic 配合使用的信息，请参阅使用亚马逊监控亚马逊 Inspector Classic CloudWatch。

Amazon Inspector Classic 中的事件响应

Amazon Inspector Classic 的事件响应是一项 AWS 责任。 AWS 有正式的、记录在案的政策和计划来管理事件响应。

AWS 具有广泛影响的运营问题发布在 S AWS ervice Health Dashboard 上。

操作性问题也通过 AWS Health Dashboard发布到个人账户。有关如何使用的信息 Health Dashboard，请参阅《AWS Health 用户指南》。

Amazon Inspector Classic 的合规性验证

Third-party 作为多个合规计划的一部分，审计师对 Amazon Inspector Classic 的安全和 AWS 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规计划范围内的 AWS 服务列表，请参阅按合规计划划分的 AWS 范围内的服务 AWS 按合规计划。有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅在 AWS Artifact 中下载报告。

您在使用 Amazon Inspector Classic 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全性与合规性快速入门指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS上部署基于安全性和合规性的基准环境的步骤。
- 在 Amazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用来 AWS 创建应用程序。 HIPAA-compliant
- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub CSPM— 此 AWS 服务可全面了解您的安全状态 AWS ，帮助您检查是否符合安全行业标准和最佳实践。

Amazon Inspector Classic 故障恢复能力

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

Amazon Inspector Classic 是高度可用的，并使用计算资源跨多个可用区执行查询。如果无法访问特定可用区，它会自动适当地路由查询。

Amazon Inspector Classic 使用 Amazon S3 作为其底层数据存储，使您的数据具备高可用性和持久性。Amazon S3 提供持久性基础设施来存储重要数据。旨在为对象提供 99.999999999% 的持久性。您的数据以冗余方式存储在多个设施中，以及各个设施内的多个设备上。

Amazon Inspector Classic 基础设施安全性

作为一项托管服务，Amazon Inspector Classic 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Amazon Inspector Classic。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（短暂的）或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。 Diffie-Hellman大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

有关 Amazon Inspector Classic 网络和代理安全的更多信息，请参阅 the section called “网络和 Amazon Inspector Classic 代理安全”。

Amazon Inspector Classic 中的配置和漏洞分析

Amazon Inspector Classic 提供称为代理的预定义软件，您可选择将它安装在要评估的 EC2 实例的操作系统中。代理将收集各种配置数据（称为遥测）。有关 Amazon Inspector Classic 代理的更多信息，请参阅 Amazon Inspector Classic 代理。

Amazon Inspector Classic 安全最佳实践

Amazon Inspector Classic 提供了在您开发和实施自己的安全策略时需要考虑的大量安全特征。这些最佳实践是一般准则，并不代表完整的安全解决方案。这些最佳实操可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。

有关 Amazon Inspector Classic`的安全最佳实践的列表，请参阅 the section called “Amazon Inspector Classic 安全最佳实践”。

Amazon Inspector Classic 代理

Amazon Inspector Classic 代理是收集 Amazon EC2 实例的已安装软件包信息和软件配置的实体。尽管不是在所有情况下都有此要求，但您应在您的每个目标 Amazon EC2 实例上安装 Amazon Inspector Classic 代理，以便完整评估其安全性。

有关如何安装、卸载和重新安装代理，如何验证已安装代理是否正在运行以及如何为代理配置代理支持的更多信息，请参阅在基于 Linux 的操作系统上使用 Amazon Inspector Classic 代理和在基于 Windows 的操作系统上使用 Amazon Inspector Classic 代理。

> **Note**
>
> 无需使用 Amazon Inspector Classic 代理即可运行网络可到达性规则包。

> **Important**
>
> Amazon Inspector Classic 代理依赖 Amazon EC2 实例元数据来正常运行。它使用实例元数据服务（IMDSv1 或 IMDSv2）的版本 1 或版本 2 访问实例元数据。请参阅实例元数据和用户数据，了解有关 EC2 实例元数据和访问方法的更多信息。

主题

Amazon Inspector Classic 代理权限

您必须具有管理权限或根权限才能安装 Amazon Inspector Classic 代理。在受支持的基于 Linux 的操作系统上，代理包含使用根访问权限运行的用户模式可执行文件。在受支持的基于 Windows 的操作系统上，代理包含更新程序服务和代理服务，这两项服务均在用户模式下使用 `LocalSystem` 权限运行。

网络和 Amazon Inspector Classic 代理安全

Amazon Inspector Classic 代理启动与 Amazon Inspector Classic 服务的所有通信。这表示代理必须具有至公共终端节点的出站网络路径，以便可以发送遥测数据。例如，代理可能连接到 `arsenal.<region>.amazonaws.com`，或终端节点可能为 处的 Amazon S3 存储桶。请务必`<region>`替换为您运行 Amazon Inspector Classic 的实际 AWS 区域。有关更多信息，请参阅 AWS IP 地址范围。由于与代理的所有连接都是为出站而建立的，因此无需在您的安全组中打开端口来允许从 Amazon Inspector Classic 到代理的入站通信。

代理通过受 TLS 保护的渠道定期与 Amazon Inspector Classic 通信，该通道使用与 EC2 实例的角色关联的 AWS 身份进行身份验证，或者如果未分配角色，则使用实例的元数据文档进行身份验证。当进行身份验证时，代理会将检测信号消息发送到服务，并接收来自服务的指令作为响应。如果已安排评估，则代理将接收该评估的指令。这些指令是结构化的 JSON 文件，并且它们将告知代理启用或禁用代理中预先配置的特定传感器。每个指令操作都在代理中进行了预定义。无法执行任意指令。

在评估期间，代理将收集系统中的遥测数据以通过受 TLS 保护的通道将这些数据发送回 Amazon Inspector Classic。代理不会更改其从中收集数据的系统。在代理收集遥测数据后，它会将数据发送回 Amazon Inspector Classic 以供处理。除了它生成的遥测数据外，代理无法收集或传输有关系统或评估目标的任何其他数据。目前，无法截取和检查代理处的遥测数据。

Amazon Inspector Classic 代理更新

在 Amazon Inspector Classic 代理的更新变得可用时，将自动从 Amazon S3 下载并应用这些更新。这也会更新任何必需的依赖项。自动更新功能使您无需跟踪和手动维护已安装在 EC2 实例上的代理的版本控制。所有更新受已审核 Amazon 更改控制流程的约束，以确保符合适用的安全标准。

为了进一步确保代理的安全，代理与自动更新发布站点 (S3) 之间的所有通信都是通过 TLS 连接进行的，并且将对服务器进行身份验证。自动更新过程中涉及的所有二进制文件都将进行数字签名，并且更新程序会在安装前对签名进行验证。自动更新过程仅在非评估期执行。如果检测到任何错误，则更新过程将回滚并重试更新。最后，代理更新过程仅支持升级代理功能。在更新工作流中，不会将代理中的您

的任何特定信息发送到 Amazon Inspector Classic。在更新过程中，传送的唯一信息是基本安装成功或失败遥测（如果适用）以及任何更新失败诊断信息。

遥测数据生命周期

Amazon Inspector Classic 代理在评估运行期间生成的遥测数据的格式将设置为 JSON 文件。这些文件 near-real-time通过 TLS 传输到 Amazon Inspector Classic，在那里使用源自 K per-assessment-run MS 的临时密钥进行加密。这些文件将安全存储在 Amazon Inspector Classic 专用的 Amazon S3 存储桶中。Amazon Inspector Classic 的规则引擎将访问 S3 存储桶中的加密遥测数据，在内存中解密这些数据，并针对配置的评估规则处理数据以生成结果。S3 中存储的遥测数据仅保留以供支持请求之用。Amazon 不会针对任何其他用途使用或收集该数据。30 天后，依据 Amazon Inspector Classic 数据的标准 S3 存储桶生命周期策略，将永久删除遥测数据。目前，Amazon Inspector Classic 不提供针对收集的遥测数据的 API 或 S3 存储桶访问机制。

从 Amazon Inspector Classic 访问 AWS 账户的

作为一项安全服务，Amazon Inspector Classic 只有在需要通过查询标签来查找要评估的 EC2 实例时才会访问您的 AWS 账户和资源。它通过初始设置 Amazon Inspector Classic 服务时创建的角色进行的标准 IAM 访问来实现这一点。在评估期间，与您的环境进行的所有通信都是由 EC2 实例上本地安装的 Amazon Inspector Classic 代理启动的。创建的 Amazon Inspector Classic 服务对象 (例如，评估目标、评估模板和服务生成的结果) 将存储在由 Amazon Inspector Classic 管理且仅可由其访问的数据库中。

Amazon Inspector Classic 代理限制

有关 Amazon Inspector Classic 代理限制的信息，请参阅 Amazon Inspector Classic 服务限制。

安装 Amazon Inspector Classic 代理

可以使用 Systems Manager Run Command 将 Amazon Inspector Classic 代理安装在多个实例 (包括基于 Linux 的实例和基于 Windows 的实例) 上。或者，您可以通过登录每个 EC2 实例来单独安装代理。本章中的过程提供了这两种方法的说明。

另一个选项是，在控制台的定义评估目标页面上选中安装代理复选框，即可在评估目标中包含的所有 Amazon EC2 实例上快速安装代理。

主题

- 使用 Systems Manager Run Command 在多个 EC2 实例上安装代理
- 在基于 Linux 的 EC2 实例上安装代理
- 在基于 Windows 的 EC2 实例上安装代理

> **Note**
>
> 本章中的程序适用于 Amazon Inspector Classic 支持的所有 AWS 区域。

使用 Systems Manager Run Command 在多个 EC2 实例上安装代理

您可以使用 Systems Manager Run Command 在 EC2 实例上安装 Amazon Inspector Classic 代理。这使您可以一次在多个实例 (对基于 Linux 和基于 Windows 的实例采用同样的命令) 上远程安装代理。

> **Important**
>
> Debian 操作系统目前不支持使用 Systems Manager Run Command 的代理安装。

> **Important**
>
> 要使用此选项，请确保您的 EC2 实例已安装了 SSM 代理且其 IAM 角色支持 Run Command。默认情况下，SSM 代理已安装在 Amazon EC2 Windows 实例和 Amazon Linux 实例上。Amazon EC2 Systems Manager 需要 EC2 实例具有处理命令的 IAM 角色，且执行命令的用户具有单独角色。有关更多信息，请参阅安装和配置 SSM 代理和为 SSM 配置安全角色。

使用 Systems Manager Run Command 在多个 EC2 实例上安装 代理

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 在导航窗格中的 “节点工具” 下，选择 “运行命令”。
3. 选择 Run a command（运行一个命令）。
4. 对于命令文档，请选择亚马逊拥有的名为 AmazonInspector-Manag e AWSAgent 的文档。此文档包含在 EC2 实例上安装 Amazon Inspector Classic 代理所用的脚本。

5. 对于 目标，您可以使用不同的方法选择 EC2 实例。要在评估目标的所有实例上安装代理，您可以指定用于创建评估目标的标签。
6. 使用从控制台运行命令中的说明为其他可用选项提供您的选择，然后选择 Run (运行)。

> **Note**
>
> 您还可以在创建评估目标时在多个 EC2 实例（基于 Linux 和基于 Windows 的实例）上安装代理，也可以对现有目标使用 使用 Run Command 安装代理按钮。有关更多信息，请参阅 创建评估目标。

在基于 Linux 的 EC2 实例上安装代理

执行以下过程以在基于 Linux 的 EC2 实例上安装 Amazon Inspector Classic 代理。

在基于 Linux 的 EC2 实例上安装 代理

1. 登录到一个运行基于 Linux 的操作系统 (您要在其中安装 Amazon Inspector Classic 代理) 的 EC2 实例。

   > **Note**
   >
   > 有关 Amazon Inspector Classic 支持的操作系统的信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

2. 通过运行下列命令之一来下载代理安装脚本：

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. （可选）确认代理安装脚本未更改或损坏。有关更多信息，请参阅 (可选) 在基于 Linux 的操作系统上验证 Amazon Inspector Classic 代理安装脚本的签名。
4. 要安装代理，请运行 sudo bash install。

   > **Note**
   >
   > 如果您在 SELinux 环境中安装代理，Amazon Inspector Classic 可能会被检测为不受限制的守护程序。您可以通过将代理进程的域从默认值 `initrc_t` 更改为 `bin_t` 来避免这种

情况。在安装代理之前，使用以下命令将bin_t上下文分配给 Amazon Inspector Classic 运行脚本 SELinux：
sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> 在 代理的更新变得可用时，将自动从 Amazon S3 下载并应用这些更新。有关更多信息，请参阅 Amazon Inspector Classic 代理更新。
> 如果您要跳过此自动更新过程，请在安装代理时运行以下命令：
> sudo bash install -u false

> **Note**
>
> （可选）要删除代理安装脚本，请运行 rm install。

5. 验证代理成功安装并正常运行所需的以下文件已安装：

   - libcurl4（在 Ubuntu 18.04 上安装代理时需要）
   - libcurl3
   - libgcc1
   - libc6
   - libstdc++6
   - libssl1.0.1
   - libssl1.0.2（在 Debian 9 上安装代理时需要）
   - libssl1.1（在 Ubuntu 20.04 LTS 上安装代理时需要）
   - libpcap0.8

在基于 Windows 的 EC2 实例上安装代理

执行以下过程以在基于 Windows 的 EC2 实例上安装 Amazon Inspector Classic 代理。

在基于 Windows 的 EC2 实例上安装 代理

1. 登录运行基于 Windows 的操作系统且您想要安装 代理的 EC2 实例。

> **Note**
>
> 有关 Amazon Inspector Classic 支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

2. 下载以下 .exe 文件：

```
https://inspector-agent.amazonaws.com/windows/installer/latest/
AWSAgentInstall.exe
```

3. 打开命令提示符窗口（使用管理权限），导航到已下载 `AWSAgentInstall.exe` 的保存位置，然后运行 .exe 文件以安装代理。

> **Note**
>
> 在 代理的更新变得可用时，将自动从 Amazon S3 下载并应用这些更新。有关更多信息，请参阅 Amazon Inspector Classic 代理更新。
> 如果您要跳过此自动更新过程，请在安装代理时运行以下命令：
> AWSAgentInstall.exe AUTOUPDATE=No

在基于 Linux 的操作系统上使用 Amazon Inspector Classic 代理

您可以安装、删除、验证和修改 Amazon Inspector Classic 代理的行为。登录到运行基于 Linux 的操作系统的 Amazon EC2 实例，然后运行以下任一过程。有关 Amazon Inspector Classic 支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

> **Important**
>
> Amazon Inspector Classic 代理依赖 Amazon EC2 实例元数据来正常运行。它使用实例元数据服务（IMDSv1 或 IMDSv2）的版本 1 或版本 2 访问实例元数据。请参阅实例元数据和用户数据，了解有关 EC2 实例元数据和访问方法的更多信息。

> **Note**
>
> 本节中的命令适用于 Amazon Inspector Classic 支持的所有 AWS 区域。

主题

验证 Amazon Inspector Classic 代理是否正在运行

- 要验证代理是否已安装且正在运行，请登录您的 EC2 实例，然后运行以下命令：

  sudo /opt/aws/awsagent/bin/awsagent status

  此命令将返回当前运行的代理的状态，或返回一个指示无法联系代理的错误。

停止 Amazon Inspector Classic 代理

- 要停止代理，请运行以下命令：

  sudo /etc/init.d/awsagent stop

启动 Amazon Inspector Classic 代理

- 要启动代理，请运行以下命令：

  sudo /etc/init.d/awsagent start

修改 Amazon Inspector Classic 代理设置

在您的 EC2 实例上安装并运行 Amazon Inspector Classic 代理后，您可以修改 agent.cfg文件中的设置来更改代理的行为。在基于 Linux 的操作系统上，agent.cfg 文件位于 /opt/aws/awsagent/etc 目录中。在修改并保存 agent.cfg 文件后，您必须停止并启动代理以使更改生效。

> **Important**
>
> 强烈建议您仅在 Amazon Web Services Support 的指导下修改 agent.cfg 文件。

配置 Amazon Inspector Classic 代理的代理支持

要实现对基于 Linux 的操作系统上的代理的代理服务器支持，请使用带特定环境变量的代理特定配置文件。欲了解更多信息，请参阅 https://wiki.archlinux。 org/index.php/proxy_设置。

完成下列过程之一：

在使用代理服务器的 EC2 实例上安装代理

1. 创建一个名为 awsagent.env 的文件并将该文件保存在 /etc/init.d/ 目录中。
2. 编辑 awsagent.env 以包含以下格式的环境变量：

   - export https_proxy=hostname:port
   - export http_proxy=hostname:port
   - export no_proxy=169.254.169.254

   > **Note**
   >
   > 将上述示例中的值仅替换为有效的主机名和端口号组合。为 no_proxy 变量指定实例元数据终端节点的 IP 地址 (169.254.169.254)。

3. 完成在基于 Linux 的 EC2 实例上安装代理过程中的步骤来安装 Amazon Inspector Classic 代理。

在具有运行中的代理的 EC2 实例上配置代理支持

1. 要配置代理支持，您的 EC2 实例上运行的代理的版本必须是 1.0.800.1 或更高版本。如果您为代理启用了自动更新过程，则可使用验证 Amazon Inspector Classic 代理是否正在运行过程来验证

您的代理的版本是否为 1.0.800.1 或更高版本。如果您未为代理启用自动更新过程，则必须遵循 在基于 Linux 的 EC2 实例上安装代理 过程再次在该 EC2 实例上安装代理。

2. 创建一个名为 awsagent.env 的文件并将该文件保存在 /etc/init.d/ 目录中。
3. 编辑 awsagent.env 以包含以下格式的环境变量：

   - export https_proxy=hostname:port
   - export http_proxy=hostname:port
   - export no_proxy=169.254.169.254

   > **Note**
   >
   > 将上述示例中的值仅替换为有效的主机名和端口号组合。为 no_proxy 变量指定实例元数据终端节点的 IP 地址 (169.254.169.254)。

4. 先使用以下命令停止代理，以重新启动该代理：

   ```
   sudo /etc/init.d/awsagent restart
   ```

   代理设置由代理和自动更新过程选取和使用。

卸载 Amazon Inspector Classic 代理

卸载代理

1. 登录运行基于 Linux 的操作系统且您想要卸载代理的 EC2 实例。

   > **Note**
   >
   > 有关 Amazon Inspector Classic 支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

2. 要卸载代理，请使用下列命令之一：

   - 在 Amazon Linux、CentOS 和 Red Hat 上，运行以下命令：

     sudo yum remove 'AwsAgent*'

   - 在 Ubuntu Server 上，运行以下命令：

```
sudo apt-get purge 'awsagent*'
```

在基于 Windows 的操作系统上使用 Amazon Inspector Classic 代理

您可以启动、停止和修改 Amazon Inspector Classic 代理的行为。登录到运行基于 Windows 的操作系统的 EC2 实例，然后执行本章中任一过程。有关 Amazon Inspector Classic 支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

> **Important**
>
> Amazon Inspector Classic 代理依赖 Amazon EC2 实例元数据来正常运行。它使用实例元数据服务 (IMDSv1or IMDSv2) 的版本 1 或版本 2 访问实例元数据。请参阅实例元数据和用户数据，了解有关 EC2 实例元数据和访问方法的更多信息。

> **Note**
>
> 本章中的命令适用于 Amazon Inspector Classic 支持的所有 AWS 区域。

主题

启动或停止 Amazon Inspector Classic 代理或验证该代理是否正在运行

启动、停止或验证代理

1. 在您的 EC2 实例 上，选择开始、运行，然后输入 **`services.msc`**。
2. 如果代理已成功运行，服务窗口中将列出状态设置为 Started 或 Running 的两项服务：AWS Agent Service 和 AWS Agent Updater Service。
3. 要启动代理，请右键单击 AWS Agent Service，然后选择启动。如果此服务成功启动，则状态更新为已启动或正在运行。

4. 要停止代理，请右键单击 AWS Agent Service，然后选择停止。如果此服务成功停止，则将清空状态（显示为空白）。建议您不要停止 AWS Agent Updater Service，因为这会禁止安装该代理的所有将来的增强功能和修补程序。
5. 要验证代理是否已安装且正在运行，请登录您的 EC2 实例，然后使用管理权限打开命令提示符。导航到 `C:\Program Files\Amazon Web Services\AWS Agent`，然后运行以下命令：

   AWSAgentStatus.exe

   此命令将返回当前运行的代理的状态，或返回一个指示无法联系代理的错误。

修改 Amazon Inspector Classic 代理设置

在您的 EC2 实例上安装并运行 Amazon Inspector Classic 代理后，您可以修改 `agent.cfg`文件中的设置来更改代理的行为。在基于 Windows 的操作系统上，该文件位于 `C:\ProgramData\Amazon Web Services\AWS Agent` 目录中。在修改并保存 `agent.cfg` 文件后，您必须停止并启动代理以使更改生效。

> **Important**
>
> 强烈建议您仅在 Amazon Web Services Support 的指导下修改 `agent.cfg` 文件。

配置 Amazon Inspector Classic 代理的代理支持

要在基于 Windows 的操作系统上获取对代理的代理支持，请使用 `WinHTTP` 代理。要使用 `netsh` 实用程序设置 `WinHTTP` 代理，请参阅用于 Windows 超文本传输协议 (WINHTTP) 的 Netsh 命令。

> **Important**
>
> 基于 Windows 的实例仅支持 HTTPS 代理。

完成下列过程之一：

在使用代理服务器的 EC2 实例上安装代理

1. 下载以下 .exe 文件：`https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`

2. 打开命令提示符窗口或 PowerShell 窗口（使用管理权限）。导航到您将下载的 `AWSAgentInstall.exe` 保存到的位置，然后运行以下命令：

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

在具有运行中的代理的 EC2 实例上配置代理支持

1. 要配置代理支持，您的 EC2 实例上运行的 Amazon Inspector Classic 代理的版本必须是 1.0.0.59 或更高版本。如果您为代理启用了自动更新过程，则可使用启动或停止 Amazon Inspector Classic 代理或验证该代理是否正在运行过程来验证您的代理的版本是否为 1.0.0.59 或更高版本。如果您未为代理启用自动更新过程，则必须遵循 在基于 Windows 的 EC2 实例上安装代理 过程再次在该 EC2 实例上安装代理。
2. 打开注册表编辑器 (`regedit.exe`)。
3. 导航到以下注册表项：`"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`。
4. 在此注册表项内，创建一个名为 `"UseProxy"` 的注册表 `DWORD(32bit)` 值。
5. 双击此值并将此值设置为 1。
6. 键入**`services.msc`**，在服务窗口中找到 AWS Agent Service 和 AWS Agent Updater Service，然后重新启动每个进程。在这两个进程成功重新启动后，运行 `AWSAgentStatus.exe` 文件（请参阅启动或停止 Amazon Inspector Classic 代理或验证该代理是否正在运行中的步骤 5）。查看您的代理的状态并确认它使用的是已配置的代理。

卸载 Amazon Inspector Classic 代理

卸载代理

1. 登录到一个运行基于 Windows 的操作系统 (您要在其中卸载 Amazon Inspector Classic 代理) 的 EC2 实例。

   > **Note**
   >
   > 有关 Amazon Inspector Classic 支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

2. 在您的 EC2 实例上，依次导航到 Control Panel 和 Add/Remove Programs。
3. 在已安装程序的列表中，选择 AWS 代理，然后选择 卸载。

(可选) 在基于 Linux 的操作系统上验证 Amazon Inspector Classic 代理安装脚本的签名

本主题描述验证基于 Linux 的操作系统的 Amazon Inspector Classic 代理安装脚本是否有效的建议的过程。

无论何时从 Internet 下载应用程序，我们都建议您验证软件发布者的身份，并检查应用程序从发行以来是否已遭更改或损坏。这会保护您免于安装含有病毒或其他恶意代码的应用程序版本。

如果您在执行本主题中的步骤后，确定适用于 Amazon Inspector Classic 代理的软件已遭更改或损坏，请不要运行安装文件。请联系 Amazon Web Services Support。

适用于基于 Linux 的操作系统的 Amazon Inspector Classic 代理文件是使用 GnuPG（安全数字签名的 Pretty Good Privacy 的开源式执行 (OpenPGP) 标准）进行签名的。GnuPG（也称为 GPG）通过数字签名提供身份验证和完整性检查。Amazon EC2 发布了您可用于验证下载的 Amazon EC2 CLI 工具的公有密钥和签名。有关 PGP 和 GnuPG (GPG) 的更多信息，请参阅 http://www.gnupg.org。

第一步是与软件发行商建立信任。下载软件发布者的公有密钥，检查公有密钥的所有人是否真为其人，然后将该公有密钥添加到您的密钥环。密钥环是已知公有密钥的集合。验证公有密钥的真实性后，您可以使用它来验证应用程序的签名。

主题

安装 GPG 工具

如果您的操作系统是 Linux 或 Unix，GPG 工具很可能已经安装。要测试系统上是否已安装这些工具，请在命令提示符处键入 gpg。如果已安装 GPG 工具，您会看到 GPG 命令提示。如果没有安装 GPG 工具，您会看到错误信息，告诉您无法找到命令。您可以从存储库安装 GnuPG 包。

在基于 Debian 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：apt-get install gnupg。

在基于 Red Hat 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：yum install gnupg。

验证并导入公有密钥

本流程的下一步是验证 Amazon Inspector Classic 公有密钥，并在 GPG 密钥环中将其添加为可信任密钥。

验证并导入 Amazon Inspector Classic 公有密钥

1. 通过执行下列操作之一获取公共 GPG 生成密钥的副本：

   - 从 https://d1wk0tztpsntt1.cloudfront 下载。 net/linux/latest/inspector.gpg。
   - 将以下文本中的密钥复制并粘贴到名为 `inspector.gpg` 的文件中。确保包含下列所有项：

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
```

```
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. 在保存 inspector.gpg 的目录中的命令提示符处，使用以下命令将 Amazon Inspector Classic 公有密钥导入密钥环：

```
gpg --import inspector.gpg
```

该命令返回的结果类似于下方内容：

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

请记下该键值，因为下一步需要用到。在上一示例中，键值为 58360418。

3. 通过运行以下命令，将 key-value 替换为上一步中的值来验证指纹：

```
gpg --fingerprint key-value
```

该命令返回的结果类似于下方内容：

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

此外，指纹字符串应与上述示例中所示的 DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418 相同。将返回的密钥指纹与此页上发布的指纹进行比较。它们应该相互匹配。如果它们不匹配，请不要安装 Amazon Inspector Classic 代理安装脚本，并联系 Amazon Web Services Support。

验证软件包的签名

在安装 GPG工具、验证并导入 Amazon Inspector Classic 公有密钥以及确认公有密钥可信后，便可以验证安装脚本的签名。

验证安装脚本签名

1. 在命令提示符处，运行以下命令以下载安装脚本的签名文件：

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. 通过在保存 `install.sig` 和 Amazon Inspector Classic 安装文件的目录中的命令提示符处运行以下命令来验证签名。这两个文件都必须存在。

```
gpg --verify ./install.sig
```

输出应与以下内容类似：

```
gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
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: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
```

如果输出包含短语 `Good signature from "Amazon Inspector <inspector@amazon.com>"`，则意味着已成功验证签名，您可以继续运行 Amazon Inspector Classic 安装脚本。

如果输出包含短语 `BAD signature`，则检查是否正确执行了此过程。如果您持续获得此响应，请不要运行之前下载的安装文件，而是联系 Amazon Web Services Support。

下面是有关您可能看到的警告的详细信息：

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. 这表示您坚信自己拥有 Amazon Inspector Classic的可信公有密钥的个人信任级别。理想情况下，您将前往 AWS 办公室并亲自接收此密钥。但更常见的情况是，从网站下载此密钥。在此示例中，该网站为 AWS 网站。
- gpg: no ultimately trusted keys found. 这意味着您 (或您信任的其他人) 对特定密钥不是“绝对信任”。

有关更多信息，请参阅 http://www.gnupg.org。

(可选) 在基于 Windows 的操作系统上验证 Amazon Inspector Classic 代理安装脚本的签名

本主题描述验证基于 Windows 的操作系统的 Amazon Inspector Classic 代理安装脚本是否有效的建议的过程。

无论何时从 Internet 下载应用程序，我们都建议您验证软件发布者的身份，并检查应用程序从发行以来是否已遭更改或损坏。这会保护您免于安装含有病毒或其他恶意代码的应用程序版本。

如果您在执行本主题中的步骤后，确定适用于 Amazon Inspector Classic 代理的软件已遭更改或损坏，请不要运行安装文件。请联系 Amazon Web Services Support。

要验证基于 Windows 的操作系统上的已下载代理安装脚本是否有效，必须确保其 Amazon Services LLC 签署人证书的指纹等于此值：

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

要验证此值，请执行以下过程：

1. 右键单击下载的 `AWSAgentInstall.exe`，然后打开 Properties (属性) 窗口。
2. 选择数字签名选项卡。
3. 在签名列表中，选择 Amazon Web Services, Inc.，然后选择详细信息。
4. 选择常规选项卡 (如果尚未选择)，然后选择查看证书。
5. 选择详细信息选项卡，然后选择显示下拉列表中的全部 (如果尚未选择)。
6. 向下滚动直至您看到指纹字段，然后选择指纹。这将在下部窗口中显示整个指纹值。

   - 如果下部窗口中的指纹值等于以下值：

     E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

     则您的已下载代理安装脚本是可信的，并且可以安全安装。
   - 如果下部详细信息窗口中的指纹值不等于上述值，请不要运行 `AWSAgentInstall.exe`。

Amazon Inspector Classic 评估目标

您可以使用 Amazon Inspector Classic 来 AWS 评估您的评估目标（您的 AWS 资源集合）是否存在您应该解决的潜在安全问题。

> **Important**
>
> 目前，您的评估目标只能由在受支持的操作系统上运行的 EC2 实例组成。有关受支持的操作系统和受支持的 AWS 区域的信息，请参阅 the section called “支持的操作系统和区域”。

> **Note**
>
> 有关启动 EC2 实例的信息，请参阅 Amazon Elastic Compute Cloud 文档。

主题

为资源添加标签以创建评估目标

要创建评估目标以便 Amazon Inspector Classic 进行评估，请先为要包含在目标中的 EC2 实例添加标签。标签是用作元数据的单词或短语，用于识别和组织您的实例和其他 AWS 资源。Amazon Inspector Classic 使用您创建的标签来标识属于您的目标的实例。

每个 AWS 标签都由您选择的密钥和值对组成。例如，您可以选择将密钥命名为 “名称”，将值命名为 “MyFirstInstance”。为实例添加标签后，可使用 Amazon Inspector Classic 控制台将实例添加到评估目标。任何实例都不必与多个标签键值对匹配。

当您为 EC2 实例添加标签以构建评估目标时，您可以创建自己的自定义标签密钥或使用同一 AWS 账户中其他人创建的标签密钥。您也可以使用 AWS 自动创建的标签密钥。例如， AWS 自动为您启动的 EC2 实例创建名称标签密钥。

您可以在创建标签时将标签添加到 EC2 实例，也可以在每个 EC2 实例的控制台页面上一次添加、更改或删除一个标签。您还可使用标签编辑器一次性将标签添加到多个 EC2 实例。

有关更多信息，请参阅标签编辑器。有关为 EC2 实例添加标签的更多信息，请参阅资源和标签。

Amazon Inspector Classic 评估目标限制

每个 AWS 账户最多可以创建 50 个评估目标。有关更多信息，请参阅 Amazon Inspector Classic 服务限制。

创建评估目标

您可使用 Amazon Inspector Classic 控制台创建评估目标。

创建评估目标

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择 Assessment Targets (评估目标)，然后选择 Create (创建)。
3. 对于 Name (名称)，输入评估目标的名称。
4. 请执行以下操作之一：
   - 要将此 AWS 账户和区域中的所有 EC2 实例包含在此评估目标中，请选中 “所有实例” 复选框。

     > **Note**
     >
     > 当您使用此选项时，可在评估运行中包含的最大代理数限制适用。有关更多信息，请参阅 Amazon Inspector Classic 服务限制。

   - 要选择要在此评估目标中包含的 EC2 实例，对于使用标签，输入标签键名称和键值对。
5. （可选）在创建目标时，您可以选中 安装代理复选框以在此目标中的所有 EC2 实例上安装代理。要使用此选项，您的 EC2 实例必须装有 SSM 代理且其 IAM 角色支持 Run Command。默认情况下，SSM 代理已安装在 Amazon EC2 Windows 实例和 Amazon Linux 实例上。Amazon EC2 Systems Manager 需要 EC2 实例具有处理命令的 IAM 角色，且执行命令的用户具有单独角色。有关更多信息，请参阅 安装和配置 SSM 代理和为 System Manager 配置安全角色。

> **Important**
>
> 如果 EC2 实例已在其上运行代理，则使用此选项会将当前在该实例上运行的代理替换为最新代理版本。

> **Note**
>
> 对于您的现有评估目标，您可以选择 使用 Run Command 安装代理 按钮以在此目标的所有 EC2 实例上安装代理。

> **Note**
>
> 您还可以使用 Systems Manager Run Command 以远程方式在多个 EC2 实例（对基于 Linux 和基于 Windows 的实例采用同样的命令）上安装代理。有关更多信息，请参阅使用 Systems Manager Run Command 在多个 EC2 实例上安装 Amazon Inspector 代理。

6. 选择保存。

> **Note**
>
> 您可以使用评估目标 页面上的 预览目标 按钮检查评估目标中包含的所有 EC2 实例。对于每个 EC2 实例，您可以查看主机名、实例 ID、IP 地址以及代理的状态（如果适用）。代理状态可具有以下值：正常、不正常和未知。当 Amazon Inspector Classic 无法确定 EC2 实例上是否有代理正在运行时，它会显示未知状态。

删除评估目标

要删除评估目标，请执行以下过程。

删除评估目标

- 在 Assessment targets (评估目标) 页面上，选择要删除的目标，然后选择 Delete (删除)。当系统提示您确认时，选择是。

> **Important**
>
> 当您删除某个评估目标时，与该目标关联的所有评估模板、评估运行、报告的结果和版本也将被删除。

您也可以使用 `DeleteAssessmentTarget` API 删除评估目标。

Amazon Inspector Classic 规则包和规则

您可以使用 Amazon Inspector Classic 评估您的评估目标 (AWS 资源的集合) 中是否存在潜在的安全问题和漏洞。Amazon Inspector Classic 会将评估目标的行为和安全配置与所选安全规则包进行比较。在 Amazon Inspector Classic环境中，规则是 Amazon Inspector Classic 在评估运行期间执行的安全检查。

在 Amazon Inspector Classic 中，规则按类别、严重性或定价分组到不同的规则包中。这使您可以选择可执行的分析的类型。例如，Amazon Inspector Classic 提供了大量可用于评估应用程序的规则。但您可能希望包含其中一部分可用规则来将目标锁定在相关的特定区域或发现特定安全问题。拥有大型 IT 部门的公司可能希望确定其应用程序是否面临任何安全威胁。其他公司可能希望仅关注高严重性的问题。

Amazon Inspector Classic 中规则的严重性级别

每条 Amazon Inspector Classic 规则都有指定的严重性级别。这降低了在分析中为各个规则设定优先顺序的需求。它还可在规则突出显示潜在问题时帮助您确定您的响应。

高、中和低级别全都指示存在可能导致评估目标中的信息机密性、完整性和可用性受损的安全问题。这些级别的区别在于问题导致危害的可能性有多大以及解决问题的紧迫性。

信息级别突出显示评估目标的安全配置详细信息。

以下是根据问题的严重程度应对问题的推荐方法：

- 高 - 高严重性问题极为紧急。Amazon Inspector Classic 建议您将此安全问题视为紧急情况并实立即执行补救措施。
- 中 - 中等严重性问题有些紧急。Amazon Inspector Classic 建议您抓住下一次可能的机会修复此问题，例如，在下一次服务更新期间。
- 低 - 低严重性问题不太紧急。Amazon Inspector Classic 建议您将此问题作为将来的其中一项服务更新的一部分进行修复。
- 信息 - 这些问题仅供参考。根据您的业务和组织目标，您可以记下此信息或使用它提高评估目标的安全性。

Amazon Inspector Classic 中的规则包

Amazon Inspector 评估可使用以下规则包的任意组合：

网络评估：

- 网络可到达性

主机评估：

- 常见漏洞和风险
- Center for Internet Security (CIS) 基准
- Amazon Inspector Classic 安全最佳实践

网络可到达性

网络可到达性包中的规则分析您的网络配置以查找您的 EC2 实例的安全漏洞。Amazon Inspector 生成的结果还提供有关限制不安全访问的指导。

网络可访问性规则包使用 AWS 可证明安全计划中的最新技术。

这些规则生成的结果表明是否可从 Internet（通过 Internet 网关，包括 Application Load Balancer 或经典负载均衡器 后的实例）、VPC 对等连接或 VPN（通过虚拟网关）到达您的端口。这些发现还突出显示了允许潜在恶意访问的网络配置，例如管理不善的安全组 ACLs IGWs、、等。

这些规则有助于自动监控您的 AWS 网络，并确定对您的 EC2 实例的网络访问可能配置错误的位置。通过将此软件包包含在评估运行中，您可以实施详细的网络安全检查，而无需安装扫描仪和发送数据包，这些数据包既复杂又昂贵，尤其是在跨VPC对等连接和 VPNs。

> **Important**
>
> 利用此规则包，无需 Amazon Inspector Classic 代理即可评估您的 EC2 实例。但是，安装的代理可以提供有关侦听端口的任何进程的存在性的信息。请勿在 Amazon Inspector Classic 不支持的操作系统上安装代理。如果运行不受支持的操作系统的实例上存在代理，则网络可到达性规则包将不适用于该实例。

有关更多信息，请参阅 支持的操作系统的 Amazon Inspector Classic 规则包。

分析的配置

网络可到达性规则分析以下实体的配置是否存在漏洞：

- Amazon EC2 实例
- 应用程序负载均衡器
- Direct Connect
- Elastic Load Balancer
- 弹性网络接口
- 互联网网关 (IGWs)
- 网络访问控制列表 (ACLs)
- 路由表
- 安全组 (SGs)
- 子网
- 虚拟私有云 (VPCs)
- 虚拟专用网关 (VGWs)
- VPC 对等连接

可到达性路由

网络可到达性规则将检查以下可到达性路由，这些路由对应于从 VPC 外部访问端口的方式：

- **`Internet`** - Internet 网关（包括 Application Load Balancer 和经典负载均衡器）
- **`PeeredVPC`** - VPC 对等连接
- **`VGW`** - 虚拟专用网关

结果类型

包括网络可到达性规则包的评估可以为每个可到达性路由返回以下类型的结果：

- `RecognizedPort`
- `UnrecognizedPortWithListener`
- `NetworkExposure`

RecognizedPort

通常用于已知服务的端口是可访问的。如果代理位于目标 EC2 实例上，则生成的结果还将指示端口上是否存在活动的侦听进程。根据已知服务的安全影响为此类型的结果给出严重级别：

- **RecognizedPortWithListener** – 可通过特定的网络组件从公共 Internet 外部访问已识别的端口，并且进程正在监听该端口。
- **RecognizedPortNoListener** – 可通过特定网络组件从公共 Internet 外部访问端口，并且没有侦听此端口的进程。
- **RecognizedPortNoAgent** – 可通过特定的网络组件从公共 Internet 外部访问端口。如果不在目标实例上安装代理，则无法确定是否存在侦听端口的进程。

下表显示已识别端口的列表：

服务	TCP 端口	UDP 端口
SMB	445	445
NetBIOS	137、139	137、138
LDAP	389	389
LDAP over TLS	636	
全局目录 LDAP	3268	
全局目录 LDAP over TLS	3269	
NFS	111、2049、4045、1110	111、2049、4045、1110
Kerberos	88、464、54 3、544、749、751	88、464、749、750、751、752
RPC	111、135、530	111、135、530
WINS	1512、42	1512、42
DHCP	67、68、546、547	67、68、546、547
Syslog	601	514

服务	TCP 端口	UDP 端口
打印服务	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017、27018、27019、28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521、1630	
Elasticsearch	9300、9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

上表中未列出的端口是可访问的，并且该端口上具有活动的侦听进程。由于此类型的结果显示有关侦听进程的信息，因此仅当目标 EC2 实例上安装了 Amazon Inspector 代理时可生成它们。将为此类型的结果给定低严重级别。

`NetworkExposure`

此类型的结果显示有关您的 EC2 实例上可访问的端口的聚合信息。对于 EC2 实例上弹性网络接口和安全组的每个组合，这些结果显示可访问的 TCP 和 UDP 端口范围组。此类型的结果具有严重级别信息。

常见漏洞和风险

此程序包中的规则有助于验证您的评估目标中的 EC2 实例是否面临常见漏洞和暴露（CVEs）。攻击可利用未修补的漏洞来损害服务或数据的机密性、完整性或可用性。CVE 系统提供了针对公共已知的信息安全漏洞和曝光的参考方法。有关更多信息，请参阅 https://cve.mitre.org/。

如果 Amazon Inspector Classic 评估生成的结果中出现特定的 CVE，您可在 https://cve.mitre.org/ 中搜索 CVE ID (例如，**CVE-2009-0021**)。搜索结果可提供有关此 CVE、其严重性和缓解方式的详细信息。

对于常见漏洞和暴露 (CVE) 规则包，Amazon Inspector 映射了提供的 CVSS 基本评分和 ALAS 严重性级别：

Amazon Inspector 严重性	CVSS 基础分数	ALAS 严重性（若 CVSS 未评分）
高	>= 5	关键或重要
中	< 5 and >= 2.1	中
低	< 2.1 and >= 0.8	低
信息性	< 0.8	不适用

此软件包中包含的规则可帮助您评估您的 EC2 实例是否暴露 CVEs 在以下区域列表中：

- 美国东部（弗吉尼亚北部）
- 美国东部（俄亥俄）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈）
- 欧洲（爱尔兰）
- 欧洲（法兰克福）
- 欧洲 (伦敦)
- 欧洲（斯德哥尔摩）
- 亚太地区（东京）
- 亚太地区（首尔）

- 亚太地区（孟买）
- 亚太地区（悉尼）
- AWS W GovCloud est（美国）
- AWS GovCloud 东部（美国）

CVE 规则包会定期更新；此列表包括在检索此列表的同时进行的评估运行中包含的规则。 CVEs

有关更多信息，请参阅 支持的操作系统的 Amazon Inspector Classic 规则包。

Center for Internet Security (CIS) 基准

CIS安全基准计划提供了定义明确、公正、基于共识的行业最佳实践，以帮助组织评估和提高其安全性。 AWS 是 CIS 安全基准成员公司。有关 Amazon Inspector Classic 认证的列表，请参阅 CIS 网站上的 Amazon Web Services 页面。

Amazon Inspector Classic 当前提供下列 CIS 认证规则包来帮助建立适用于下列操作系统的安全配置状况：

Amazon Linux

- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation

- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation

- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)

- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

如果 Amazon Inspector Classic 评估运行生成的结果中出现特定的 CIS 基准，您可从 https://benchmarks.cisecurity.org/下载此基准的 PDF 格式的详细描述（需要免费注册）。此基准文档提供了有关此 CIS 基准、其严重性以及如何缓解它的详细信息。

有关更多信息，请参阅 支持的操作系统的 Amazon Inspector Classic 规则包。

Amazon Inspector Classic 安全最佳实践

使用 Amazon Inspector Classic 规则帮助确定您的系统的配置是否安全。

> **Important**
>
> 当前，您可将运行基于 Linux 的操作系统或基于 Windows 的操作系统的 EC2 实例包含在评估目标中。
>
> 在评估运行期间，本节中描述的规则将仅生成运行基于 Linux 的操作系统的 EC2 实例的结果。规则不会生成运行基于 Windows 的操作系统的 EC2 实例的结果。
>
> 有关更多信息，请参阅 支持的操作系统的 Amazon Inspector Classic 规则包。

主题

- 配置密码复杂度
- 启用 ASLR
- 启用 DEP
- 配置系统目录的权限

禁止使用根凭证通过 SSH 进行登录

此规则将帮助确定 SSH 守护程序是否已配置为允许使用根凭证登录您的 EC2 实例。

严重性

中等

调查发现

评估目标中的 EC2 实例已配置为允许用户使用根凭证通过 SSH 进行登录。这会增大暴力攻击的成功率。

解决方法

建议您将 EC2 实例配置为阻止根账户通过 SSH 进行登录。而在必要时，以非根用户身份登录并使用 sudo 提升权限。要禁用 SSH 根账户登录，请将 PermitRootLogin 设置为 no（在 /etc/ssh/sshd_config 文件中），然后重启 sshd。

仅支持 SSH 版本 2

此规则将帮助确定您的 EC2 实例是否已配置为支持 SSH 协议版本 1。

严重性

中等

调查发现

评估目标中的 EC2 实例将配置为支持 SSH 1，后者自带的设计缺陷大大降低了其安全性。

解决方法

建议您将评估目标中的 EC2 实例配置为仅支持 SSH-2 及更高版本。对于 OpenSSH，您可以通过在 /etc/ssh/sshd_config 文件中设置 Protocol 2 来实现这一点。有关更多信息，请参阅 man sshd_config。

禁止通过 SSH 进行密码身份验证

此规则将帮助确定您的 EC2 实例是否已配置为支持通过 SSH 协议进行密码身份验证。

严重性

中等

调查发现

评估目标中的 EC2 实例将配置为支持通过 SSH 进行密码身份验证。密码身份验证易受暴力攻击，如有可能，应将其禁用以支持基于密钥的身份验证。

解决方法

建议您对 EC2 实例禁用通过 SSH 的密码身份验证，并启用对基于密钥的身份验证的支持。这将大大减小暴力攻击的成功率。有关更多信息，请参阅 https://aws.amazon.com/articles/1233/。如果支持密码身份验证，请务必仅允许通过可信 IP 地址对 SSH 服务器进行的访问。

配置密码最长使用期

此规则将帮助确定是否在您的 EC2 实例上配置密码的最长使用期。

严重性

中等

调查发现

未为评估目标中的 EC2 实例配置密码最长使用期。

解决方法

如果您使用的是密码，建议在评估目标中的所有 EC2 实例上配置密码的最长使用期。这需要用户定期更改其密码，减小密码猜测攻击的成功率。要为现有用户解决此问题，请使用 chage 命令。要为所有将来用户配置密码的最长使用期，请编辑 `/etc/login.defs` 文件中的 `PASS_MAX_DAYS` 字段。

配置密码最小长度

此规则将帮助确定是否在您的 EC2 实例上配置密码的最小长度。

严重性

中等

调查发现

未为评估目标中的 EC2 实例配置密码的最小长度。

解决方法

如果您使用的是密码，建议您在评估目标中的所有 EC2 实例上配置密码的最小长度。强制执行最小密码长度将减小密码猜测攻击的成功率。您可以通过使用 pwquality.conf 文件中的以下选项执行该操作：minlen欲了解更多信息，请参阅 https://linux.die。 net/man/5/pwquality.conf。

如果 pwquality.conf 在您的实例上不可用，您可以使用 pam_cracklib.so 模块设置 minlen选项。有关更多信息，请参阅 man pam_cracklib。

minlen 选项应设置为 14 或更大。

配置密码复杂度

此规则将帮助确定是否在您的 EC2 实例上配置密码复杂度机制。

严重性

中等

调查发现

未在评估目标中的 EC2 实例上配置密码复杂度机制或限制。这将允许用户设置简单密码，从而增加未经授权的用户获得访问权和误用账户的几率。

解决方法

如果您使用的是密码，建议您将评估目标中的所有 EC2 实例配置为需要一定的密码复杂度。您可以通过使用 pwquality.conf 文件中的以下选项执行该操作：lcredit、ucredit、dcredit 和 ocredit。欲了解更多信息，请参阅 https://linux.die。 net/man/5/pwquality.conf。

如果 pwquality.conf 在您的实例上不可用，您可以使用 pam_cracklib.so 模块设置 lcredit、ucredit、dcredit 和 ocredit 选项。有关更多信息，请参阅 man pam_cracklib。

每个选项的预期值都小于或等于 -1，如下所示：

`lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1`

此外，该 `remember` 选项必须设置为 12 或更大的值。有关更多信息，请参阅 `man pam_unix`。

启用 ASLR

此规则将帮助确定是否在评估目标中的 EC2 实例的操作系统上启用地址空间布局随机化 (ASLR)。

严重性

中等

调查发现

评估目标中的 EC2 实例未启用 ASLR。

解决方法

要增强评估目标的安全性，建议您通过运行 echo 2 | sudo tee /proc/sys/kernel/randomize_va_space在目标的所有 EC2 实例的操作系统上启用 ASLR。

启用 DEP

此规则将帮助确定是否在评估目标中的 EC2 实例的操作系统上启用数据执行保护 (DEP)。

> **Note**
>
> 配有 ARM 处理器的 EC2 实例不支持此规则。

严重性

中等

调查发现

评估目标中的 EC2 实例未启用 DEP。

解决方法

建议您在评估目标中的所有 EC2 实例的操作系统上启用 DEP。启用 DEP 将使用缓冲区溢出技术来确保您的实例免受安全损害。

配置系统目录的权限

此规则检查包含二进制文件和系统配置信息的系统目录的权限。它检查是否仅根用户（使用根账户凭证登录的用户）具有这些目录的写入权限。

严重性

高

调查发现

评估目标中的 EC2 实例包含非根用户可写入的系统目录。

解决方法

要增强评估目标的安全性并防止恶意本地用户提升权限，请将目标中的所有 EC2 实例上的所有系统目录配置为只能由使用根账户凭证登录的用户写入。

Amazon Inspector Classic 评估模板和评估运行

Amazon Inspector Classic 通过使用安全规则分析您的 AWS 资源来帮助您发现潜在的安全问题。Amazon Inspector Classic 监控和收集个人资源相关的行为数据（遥测）。这些数据包括有关安全通道使用情况、正在运行的进程之间的网络流量以及与 AWS 服务通信的详细信息的信息。接下来，Amazon Inspector Classic 针对一组安全规则包分析和比较这些数据。最后，Amazon Inspector Classic 将生成一个确定各种严重性的潜在安全问题的结果 的列表。

要开始操作，请创建一个评估目标（您希望 Amazon Inspector Classic 分析的 AWS 资源的集合）。接下来，创建一个评估模板（您用于配置评估的蓝图）。使用该模板启动评估运行，这是一个将生成一组结果的监控和分析过程。

主题

Amazon Inspector Classic 评估模板

利用评估模板，您可以指定评估运行的配置，其中包括：

- Amazon Inspector Classic 用来评估您的评估目标的规则包
- 评估运行的持续时间 – 您可以将评估运行的持续时间设置为 3 分钟到 24 小时。我们建议将评估运行的持续时间设置为 1 小时。
- Amazon Inspector Classic 将有关您的评估运行状态和结果的通知发送到的 Amazon SNS 主题
- Amazon Inspector Classic 属性（键值对），您可将其分配给使用此评估模板的评估运行所生成的结果

在 Amazon Inspector Classic 创建评估模板后，您可为其添加标签，就像为任何其他 AWS 资源添加标签一样。有关更多信息，请参阅标签编辑器。通过为评估模板添加标签，您可以整理这些模板并更好地监督您的安全策略。例如，Amazon Inspector Classic 提供了您在评估您的评估目标时可参考的大量规则。您可能希望在评估模板中包含不同的可用规则子集，以确立特定的关注方面或发现特定的安全问题。通过为评估模板添加标签，您可根据安全策略和目标随时快速查找和运行这些模板。

> **Important**
>
> 评估模板一经创建，便无法修改。

Amazon Inspector Classic 评估模板限制

每个 AWS 账户最多可以创建 500 个评估模板。

有关更多信息，请参阅 Amazon Inspector Classic 服务限制。

创建评估模板

创建评估模板

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择 Assessment Templates (评估模板)，然后选择 Create (创建)。
3. 对于 Name (名称)，输入评估模板名称。
4. 对于目标名称，选择要分析的评估目标。

   > **Note**
   >
   > 当创建评估模板时，您还可以使用评估模板页面上的预览目标按钮查看包含在评估目标中的所有 EC2 实例。对于每个 EC2 实例，您可以查看主机名、实例 ID、IP 地址以及代理的状态（如果适用）。代理状态可具有以下值：正常、不正常和未知。当 Amazon Inspector Classic 无法确定 EC2 实例上是否有代理正在运行时，它会显示未知状态。
   > 您还可以使用评估模板页面上的预览目标按钮查看构成包含在您之前创建的模板中的评估目标的 EC2 实例。

5. 对于规则包，选择要包含在评估模板中的一个或多个规则包。

6. 对于持续时间，为评估模板指定持续时间。
7. （可选）对于 SNS 主题，指定您希望 Amazon Inspector Classic 将有关评估运行状态和结果的通知发送到的 SNS 主题。Amazon Inspector Classic 可发送有关下列事件的 SNS 通知：

   - 评估运行已开始
   - 评估运行已结束
   - 评估运行的状态已更改
   - 已生成结果

   有关设置 SNS 主题的更多信息，请参阅设置 Amazon Inspector Classic 通知的 SNS 主题。
8. （可选）对于 Tag (标签)，输入 Key (键) 和 Value (值) 的值。您可向评估模板添加多个标签。
9. (可选) 对于添加到结果的属性，输入密钥和值的值。Amazon Inspector Classic 将向评估模板生成的所有结果应用属性。您可向评估模板添加多个属性。有关结果以及为结果添加标签的更多信息，请参阅 Amazon Inspector Classic 能取得的结果。
10. （可选）要使用此模板为评估运行设置一个计划，请选中 Set up recurring assessment runs once every <number_of_days>, starting now (从现在开始，每隔 <number_of_days> 天设置一次周期性评估运行) 复选框，并使用向上和向下箭头指定循环模式（天数）。

    > **Note**
    >
    > 当您使用此复选框时，Amazon Inspector Classic 会自动为您正在设置的评估运行计划创建亚马逊 CloudWatch 事件规则。然后，Amazon Inspector Classic 还会自动创建一个名为 `AWS_InspectorEvents_Invoke_Assessment_Template` 的 IAM。此角色允许 Ev CloudWatch ents 对 Amazon Inspector Classic 资源进行 API 调用。有关更多信息，请参阅什么是 Amazon CloudWatch 活动？ 以及对 CloudWatch 事件使用基于资源的策略。

    > **Note**
    >
    > 您还可以通过 AWS Lambda 函数设置自动评估运行。有关更多信息，请参阅 通过 Lambda 函数设置自动评估运行。
11. 选择创建并运行或创建。

删除评估模板

要删除评估模板，请执行以下过程。

删除评估模板

- 在 Assessment Templates (评估模板) 页面上，选择要删除的模板，然后选择 Delete (删除)。当系统提示您确认时，选择是。

> **Important**
>
> 当您删除某个评估模板时，与此模板关联的所有评估运行、报告的结果和版本也将被删除。

您也可以使用 `DeleteAssessmentTemplate` API 删除评估模板。

评估运行数

在您创建评估模板后，可使用它来启动评估运行。只要保持在每个 AWS 账户的运行限制之内，就可以使用同一个模板开始多次运行。有关更多信息，请参阅 Amazon Inspector Classic 评估运行限制。

如果您使用 Amazon Inspector Classic 控制台，则必须先从 评估模板 页启动新评估模板的首次运行。在启动运行后，您可使用评估运行页来监控运行的进度。使用 Run、Cancel 和 Delete 按钮分别可启动、取消或删除运行。您还可以查看运行的详细信息，包括运行的 ARN、为运行选择的规则包、您应用于运行的标签和属性等。

对于评估模板的后续运行，您可使用 Assessment templates 页或 Assessment runs 页上的 Run、Cancel 和 Delete 按钮。

删除评估运行

要删除评估运行，请执行以下过程。

删除运行

- 在 Assessment runs (评估运行) 页面上，选择要删除的运行，然后选择 Delete (删除)。当系统提示您确认时，选择是。

> **Important**
>
> 当您删除某个运行时，该运行中的所有结果和所有版本的报告也将被删除。

您还可使用 `DeleteAssessmentRun` API 删除运行。

Amazon Inspector Classic 评估运行限制

您最多可以为每个 AWS 账户创建 50,000 次评估。

您可同时启动多个运行，前提是用于这些运行的目标不包含重叠的 EC2 实例。

有关更多信息，请参阅 Amazon Inspector Classic 服务限制。

通过 Lambda 函数设置自动评估运行

如果您要为评估设置定期计划，可使用 AWS Lambda 控制台创建 Lambda 函数来将评估模板配置为自动运行。有关更多信息，请参阅 Lambda 函数。

要使用 AWS Lambda 控制台设置自动评估运行，请执行以下步骤。

通过 Lambda 函数设置自动运行

1. 登录并 AWS 管理控制台打开AWS Lambda 控制台。
2. 在导航窗格中，选择 控制面板 或 函数，然后选择 创建 Lambda 函数。
3. 在 Create function (创建函数) 页面上，选择 Browse serverless app repository (浏览无服务器应用程序存储库)，然后在搜索字段中输入 **`inspector`**。
4. 选择 inspector-scheduled-run 蓝图。
5. 在 “查看、配置和部署” 页面上，通过指定触发函数 CloudWatch 的事件，为自动运行设置定期计划。为此，请输入规则名称和描述，然后选择计划表达式。计划表达式确定运行发生的频率，例如，每 15 分钟或每天发生一次。有关 CloudWatch 事件和概念的更多信息，请参阅什么是 Amazon CloudWatch 活动？

   如果您选中 Enable trigger (启用触发器) 复选框，则运行将在您创建完函数后立即开始。后续自动运行遵循您在 Schedule expression (计划表达式) 字段中指定的定期模式。如果您在创建函数时未选中启用触发器复选框，则可稍后编辑函数来启用此触发器。

6. 在配置函数页上，指定以下内容：

   - 对于 Name (名称)，输入您的函数的名称。
   - （可选）对于 Description (描述)，输入稍后将帮助您识别函数的描述。
   - 对于运行时间，请保留默认值**Node.js 8.10**。 AWS Lambda 仅支持**Node.js 8.10**运行时的inspector-scheduled-run蓝图。
   - 您要使用此函数自动运行的评估模板。可通过为名为 assessmentTemplateArn 的环境变量提供此值来执行此操作。
   - 将处理程序设置为默认值 **index.handler**。
   - 使用角色字段的函数的权限。有关更多信息，请参阅 AWS Lambda 权限模型。

     要运行此函数，您需要一个 IAM 角色 AWS Lambda 来启动运行并将有关运行的日志消息（包括任何错误）写入 Amazon Lo CloudWatch gs。 AWS Lambda 在每次重复的自动运行中都担任此角色。例如，您可将以下示例策略附加到此 IAM 角色：

     JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 检查您的选择，然后选择创建函数。

设置 Amazon Inspector Classic 通知的 SNS 主题

Amazon Simple Notification Service (Amazon SNS) 是一项向订阅终端节点或客户端发送消息的 Web 服务。您可使用 Amazon SNS 为 Amazon Inspector Classic 设置通知。

为通知设置 SNS 主题

1. 创建一个 SNS 主题。请参阅教程：创建 Amazon SNS 主题。创建主题时，请展开访问策略 – 可选部分。然后，执行以下操作以允许评估向该主题发布消息：

   a. 对于 Choose method (选择方法)，请选择 Basic (基本)。

   b. 在 “定义谁可以向主题发布消息” 中，选择 “仅限指定的 AWS 账户”，然后输入要创建主题的区域中的账户的 ARN：

      - US East (Ohio) - arn:aws:iam::646659390643:root
      - US East (N. Virginia) - arn:aws:iam::316112463485:root
      - US West (N. California) - arn:aws:iam::166987590008:root
      - US West (Oregon) - arn:aws:iam::758058086616:root
      - Asia Pacific (Mumbai) - arn:aws:iam::162588757376:root
      - Asia Pacific (Seoul) - arn:aws:iam::526946625049:root
      - Asia Pacific (Sydney) - arn:aws:iam::454640832652:root
      - Asia Pacific (Tokyo) - arn:aws:iam::406045910587:root
      - Europe (Frankfurt) - arn:aws:iam::537503971621:root
      - Europe (Ireland) - arn:aws:iam::357557129151:root
      - Europe (London) - arn:aws:iam::146838936955:root
      - Europe (Stockholm) - arn:aws:iam::453420244670:root
      - AWS GovCloud (US-East)-arn:: iam:: 206278770380: aws-us-gov root
      - AWS GovCloud (US-West)-arn:: iam:: 850862329162: aws-us-gov root

   c. 在 “定义谁可以订阅此主题” 中，选择 “仅限指定的 AWS 账户”，然后输入您要创建该主题的区域中该账户的 ARN。

   d. 为防止 Inspector 被用作混淆代理人（如 IAM 用户指南中的混淆代理人问题中所述），请执行以下操作：

      i. 选择 Advanced（高级）。这将引导您进入 JSON 编辑器。

      ii. 添加以下条件：

```
"Condition": {
   "StringEquals": {
      "aws:SourceAccount": <your account Id here>,
```

```
          "aws:SourceArn": "arn:aws:inspector:*:*:*"
        }
      }
```

e. （可选）有关 aws: SourceAccount 和 aws: 的更多信息SourceArn，请参阅 IA M 用户指南中的全局条件上下文密钥。

f. 根据需要更新该主题的其他设置，然后选择 Create topic (创建主题)。

2. （可选）要创建加密的 SNS 主题，请参阅《SNS 开发者指南》中的静态加密。

3. 为防止 Inspector 被用作 KMS 密钥的混淆代理人，请按照以下其他步骤操作：

a. 在 KMS 控制台中转到您的 CMK。

b. 选择编辑。

c. 添加以下条件：

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. 为您创建的主题创建订阅。有关更多信息，请参阅教程：将终端节点订阅到 Amazon SNS 主题。

5. 要确认订阅是否已正确配置，请向该主题发布一则消息。有关更多信息，请参阅教程：向 Amazon SNS 主题发布消息。

Amazon Inspector Classic 能取得的结果

结果是 Amazon Inspector Classic 在评估您的评估目标期间发现的潜在安全问题。结果显示在 Amazon Inspector Classic 控制台上或通过 API 显示。结果包含安全问题的详细描述以及有关如何解决这些问题的建议。

在 Amazon Inspector 生成结果后，您可以通过为结果分配 Amazon Inspector Classic 属性来跟踪它们。这些属性包括键值对。

使用属性跟踪您的结果对于管理安全策略的工作流程非常有用。例如，在创建并运行评估后，它将根据您的安全目标和方法生成包含各种严重性、紧急性和相关性的结果的列表。您可能需要立即执行某个结果的建议步骤来解决潜在紧急安全问题。或者，在下一个即将来临的服务更新之前，您可能需要推迟解决其他结果。例如，要跟踪结果以立即解决，可创建结果并为其分配带键值对 **`Status`** / **`Urgent`** 的属性。您还可使用属性分发解决潜在安全问题的工作负载。例如，要为 Bob（您团队的安全工程师）提供解析结果的任务，您可将包含键值对 **`Assigned Engineer`** / **`Bob`** 的属性分配给结果。

处理调查发现

对生成的任何 Amazon Inspector Classic 结果完成以下过程。

查找、分析结果并为其分配属性

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 运行评估后，导航到 Amazon Inspector Classic 控制台中的结果页以查看您的结果。

   您也可在 Amazon Inspector Classic 控制台的控制面板页上的重要结果部分中查看结果。

   > **Note**
   >
   > 您无法查看由仍在进行的评估运行生成的结果。但是，如果您在评估完成前将其停止，则可查看部分结果。在生产环境中，建议您让每次评估都完全执行，以便它可以生成一组完整的结果。

3. 要查看特定结果的详细信息，请选择结果旁的 Expand 小组件。结果的详细信息包含以下内容：

   - 评估目标的名称，其中包括注册此发现的 EC2 实例。
   - 已用于生成此结果的评估模板的名称。

- 评估运行开始时间。
- 评估运行结束时间。
- 评估运行状态。
- 包含触发了此结果的规则的规则包的名称。
- 结果的名称。
- 结果的严重性。
- 来自通用漏洞评分系统 (CVSS) 的本机严重性详细信息。其中包括由常见漏洞和风险规则包中的规则触发的结果的 CVSS 矢量和 CVSS 评分指标（包括 CVSS 版本 2.0 和 3.0）。有关 CVSS 的详细信息，请参阅 https://www.first.org/cvss/。
- 互联网安全中心 (CIS) 提供的本地严重性详细信息。其中包括由 CIS 基准包中的规则触发的结果的 CIS 权重指标。有关 CIS 权重指标的更多信息，请参阅 https://www.cisecurity.org/。
- 结果的描述。
- 建议的步骤，您可完成这些步骤来修复结果描述的潜在安全问题。

4. 要将属性分配给结果，请选择结果，然后选择添加/编辑属性。

   您还可在创建评估模板时将属性分配给结果。要执行该操作，请将新模板配置为自动将属性分配给由评估运行生成的所有结果。您可以使用此评估的结果的标签字段中的密钥和值字段。有关更多信息，请参阅 Amazon Inspector Classic 评估模板和评估运行。

5. 要将结果导出到电子表格，请选择位于 Findings (结果) 页面右上角的向下箭头。在对话框中，选择 Export all columns (导出所有列) 或 Export visible columns (导出可见列)。

   请注意，在所导出的内容中，所有日期时间值都采用纪元时间戳。

6. 要筛选当前的检查结果，请在结果表上方的筛选栏中输入要筛选的单个字符串，例如实例 ID 或 CVE 编号。要显示或隐藏其他信息列，请选择检查结果页面右上角的设置图标。

7. 要删除结果，请导航到 Assessment runs (评估运行) 页面，并选择要删除的结果中生成的运行。然后选择删除。当系统提示您确认时，选择是。

   > **Important**
   >
   > 您无法在 Amazon Inspector Classic 中删除单个结果。当您删除某个评估运行时，该运行中所有结果和所有版本的报告也将被删除。

   您也可以使用 DeleteAssessmentRun API 删除评估运行。

评测报告

Amazon Inspector Classic 评估报告是一种文档，用于详细介绍评估运行的测试内容和评估结果。您可存储报告，与您的团队共享它们以作为修正措施，或使用它们补充您的合规性审计数据。您可在运行成功完成之后，生成评估运行报告。

> **Note**
>
> 只能为 2017 年 4 月 25 日（即 Amazon Inspector Classic 开始支持评估报告的日期）后进行的评估运行生成报告。

您可以查看以下类型的评估报告：

- 结果报告 - 这种报告中包含以下信息：
  - 评估的摘要
  - EC2 在评估运行期间评估的实例
  - 评估运行中包含的规则包
  - 有关每个发现的详细信息，包括发现的所有 EC2 实例
- 完整报告 – 此报告包括结果报告中包含的所有信息，并提供在评估目标中的实例上检查的规则的列表。

要生成评测报告

1. 在 Assessment runs (评估运行) 页面上，找到要为其生成报告的评估运行。确保其状态设置为 Analysis complete (分析完成)。
2. 在该评估运行的 Reports (报告) 列下，选择报告图标。

   > **Important**
   >
   > 从 2025 年 3 月 24 日起，评估报告将不再包含网络可访问性发现的严重性信息。此信息可在亚马逊 Inspector 控制台中找到。

3. 在 Assessment report (评估报告) 对话框中，选择要查看的报告的类型（结果或完整报告）和报告格式（HTML 或 PDF）。然后选择 Generate report (生成报告)。

您也可以通过 GetAssessmentReport API 生成评估报告。

要删除评估报告，请执行以下过程。

删除报告

- 在 Assessment runs (评估运行) 页面上，选择要删除的报告基于其上的运行，然后选择 Delete (删除)。当系统提示您确认时，选择是。

  > **Important**
  >
  > 在 Amazon Inspector Classic 中，您无法删除个人报告。当您删除某个评估运行时，该运行中所有版本的报告和所有结果也将被删除。

  您也可以使用 DeleteAssessmentRun API 删除评估运行。

Amazon Inspector Classic 中的排除项

排除项是 Amazon Inspector Classic 评估运行的输出。排除项可呈现哪些安全检查无法完成以及如何解决这些问题。例如，问题可能是由于指定目标的 EC2 实例上缺少代理、使用了不支持的操作系统或意外错误所致。

您可以在控制台的 Assessment runs (评估运行) 页面上查看排除项。有关更多信息，请参阅 查看评估后的排除项。

为了避免产生不必要的 AWS 费用，Amazon Inspector Classic 允许您在进行评估之前预览排除项。您可以在控制台的 Assessment templates (评估模板) 页面上找到预览。有关更多信息，请参阅 预览排除项。

> **Note**
>
> 只能为 2018 年 6 月 25 日后执行的运行生成评估后的排除项。这是 Amazon Inspector Classic 开始支持排除项的日期。但排除项预览适用于所有评估模板，无论日期是何时。

主题

排除项类型

Amazon Inspector Classic 可以生成以下排除项类型。

排除项类型	说明	建议
目标	不存在带有评估目标	检查评估目标中的标签

排除项类型	说明	建议
中无实例	中指定标签的 EC2 实例。	是否与目标 EC2 实例的标签相匹配。
代理已运行	目标 EC2 实例的评估运行已在进行中。	等到目标 EC2 实例上运行的当前评估已完成。
未找到代理	在目标 EC2 实例上未找到 Amazon Inspector Classic 代理。	在目标 EC2 实例上安装或重新安装 Amazon Inspector Classic 代理。有关更多信息，请参阅 安装 Amazon Inspector Classic 代理。

排除项类型	说明	建议
代理运行不正常	目标 EC2 实例上的 Amazon Inspector Classic 代理处于不健康状态。	检查此实例上 Amazon Inspector Classic 代理的状态并采取必要措施。有关更多信息，请参阅 Inspector 代理。
不支持的操作系统版本	Amazon Inspector 经典评估不支持目标 EC2 实例的操作系统。	将目标 EC2 实例从评估目标中移除，或者创建一个不包含此实例的目标。如需支持的操作系统列表，请参阅 Amazon Inspector Classic 支持的操作系统和区域。

排除项类型	说明	建议
已淘汰的规则包	评估模板中包含已淘汰的规则包。	请创建不包含已淘汰规则包的评估模板，并在将来的评估运行中使用该模板。
操作系统不支持的规则包	评估模板中包含的规则包不支持目标 EC2 实例的操作系统。	创建不包含冲突规则包的评估模板或从评估模板中移除目标 EC2 实例。如需操作系统支持的规则包列表，请参阅规则包在受支持的操作系统中的可用性。

排除项类型	说明	建议
单一实例的规则评估错误	发生内部错误，导致此实例的规则评估失败。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。
规则评估错误	发生内部错误，导致您的评估的规则评估失败。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

排除项类型	说明	建议
网络可达性错误 – Intern	发生内部错误，导致针对从 Internet 通过检查端口是否可达的网络可到达性评估失败。您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

排除项类型	说明	建议
网络可到达性错误 – Intern 通过应用程序负载均衡器	发生内部错误，导致针对从 Internet 通过应用程序负载均衡器检查端口是否可达的网络可到达性评估失败。您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

排除项类型	说明	建议
网络可到达性错误 – Intern通过弹性负载均衡负载均衡器	发生内部错误，导致针对从 Internet 通过弹性负载均衡负载均衡器检查端口是否可达的网络可到达性评估失败。您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

排除项类型	说明	建议
网络可到达性错误 – VPN	发生内部错误，导致针对从 VPN 检查端口是否可达的网络可到达性评估失败。您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。
网络可接通性错误 — AWS Direct Conne	内部错误导致网络可访问性评估在检查可访问的端口时失败。 AWS Direct Connect您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

排除项类型	说明	建议
网络可到达性错误 – VPC 对等连接	发生内部错误，导致针对从对等的 VPC 检查端口是否可达的网络可到达性评估失败。您可能会获得其他网络可到达性类型的结果。	尝试再次运行评估。如果排除项在您重新运行评估时仍然存在，请联系支持人员。

预览排除项

Amazon Inspector Classic 允许在运行评估之前预览潜在的排除项。

预览评估排除项

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择评估模板。
3. 展开一个模板，在 Assessment templates (评估模板) 部分中，选择 Preview exclusions (预览排除项)。
4. 检查检测到的所有排除项的描述，以及解决建议。

   您还可以列出和描述排除项，方法是分别使用 `ListExclusions` 和 `DescribeExclusions` 操作。

查看评估后的排除项

运行评估之后，您可以查看有关任何排除项的详细信息。

查看有关排除项的详细信息

1. 登录 AWS 管理控制台 并打开 Amazon Inspector Classic 控制台，网址为https://console.aws.amazon.com/inspector/。
2. 在导航窗格中，选择 Assessment runs (评估运行)。
3. 在 Exclusions (排除项) 列中，选择与某一评估运行关联的有效链接。
4. 检查检测到的所有排除项的描述，以及解决建议。

   您还可以列出和描述排除项，方法是分别使用 `ListExclusions` 和 `DescribeExclusions` 操作。

支持的操作系统的 Amazon Inspector Classic 规则包

您可以在评估目标中包含的 EC2 实例上运行 Amazon Inspector Classic 规则包。下表显示支持的操作系统的规则包的可用性。

> **Important**
>
> 无论操作系统如何，您都可在任何 EC2 实例上使用网络可到达性规则包运行无代理评估。

> **Note**
>
> 有关受支持的操作系统的更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域。

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Amaz Linux 2	支持	支持	支持	支持	已弃用
Amaz Linux 2018.	支持	支持	支持	支持	已弃用
Amaz Linux 2017.	支持	支持	支持	支持	已弃用

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Amaz Linux 2017.	支持	支持	支持	支持	已弃用
Amaz Linux 2016.	支持	支持	支持	支持	已弃用
Amaz Linux 2016.	支持	支持	支持	支持	已弃用
Amaz Linux 2015.	支持	支持	支持	支持	已弃用
Amaz Linux 2015.	支持	支持	支持	支持	已弃用
Amaz Linux 2014.	支持		支持	支持	
Amaz Linux 2014.	支持		支持	支持	

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Amaz Linux 2013.	支持		支持	支持	
Amaz Linux 2013.	支持		支持	支持	
Amaz Linux 2012.	支持		支持	支持	
Amaz Linux 2012.	支持		支持	支持	
Ubun 20.04 LTS	支持		支持	支持	
Ubun 18.04 LTS	支持	支持	支持	支持	已弃用
Ubun 16.04 LTS	支持	支持	支持	支持	已弃用

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Ubun 14.04 LTS	支持	支持	支持	支持	已弃用
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	支持		支持	支持	
RHEl 8.x	支持		支持	支持	
RHEl 7.6 - 7.x	支持	支持	支持	支持	
RHEl 6.2 - 6.9, 7.2 - 7.5	支持	支持	支持	支持	已弃用

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Cent(7.6 - 7.X	支持	支持	支持	支持	
Cent(6.2 - 6.9、 - 7.5	支持	支持	支持	支持	已弃用
Wind(Serve 2019 Base	支持		支持		
Wind(Serve 2016 Base	支持	支持	支持		已弃用
Wind(Serve 2012 R2	支持	支持	支持		已弃用

受支持的操作系统	常见漏洞和风险	CIS 基准	网络可到达性	安全最佳实践	运行时行为分析
Windows Server 2012	支持	支持	支持		已弃用
Windows Server 2008 R2	支持	支持	支持		已弃用

使用记录 Amazon Inspector 经典 API 调用 AWS CloudTrail

Amazon Inspector Classic 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Amazon Inspector Classic 中采取的操作的记录。 CloudTrail 将亚马逊 Inspector Classic 的所有 API 调用捕获为事件，包括来自亚马逊 Inspector Classic 控制台的调用和对亚马逊 Inspector Classic API 操作的代码调用 如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Amazon Inspector Classic 的事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台的 Event history (事件历史记录) 中查看最新事件。使用收集的信息 CloudTrail，您可以确定向 Amazon Inspector Classic 发出的请求、发出请求的 IP 地址、谁发出了请求、何时提出请求等。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。有关 Amazon Inspector Classic API 操作的完整列表，请参阅 Amazon Inspector Classic API 参考中的操作。

Amazon Inspector 经典信息位于 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Amazon Inspector Classic 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括 Amazon Inspector Classic 的活动，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台上创建跟踪时，此跟踪应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和从多个账户接收 CloudTrail日志文件

CloudTrail 记录所有 Amazon Inspector Classic 操作`DescribeAssessmentTargets`，包括只读操作（例如和）以及管理操作（例如`AddAttributesToFindings`和）`CreateAssessmentTemplate`。`ListAssessmentRuns`

> **Note**
>
> CloudTrail 仅记录 Amazon Inspector Classic 只读操作的请求信息。对于所有其他 Amazon Inspector Classic 操作，则同时记录请求和响应信息。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出
- 请求是使用角色还是联合用户的临时安全凭证发出的
- 请求是否由其他 AWS 服务发出

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon Inspector Classic 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间以及其他请求参数的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

以下示例显示了一个演示 Amazon Inspector Classic `CreateResourceGroup` 操作的 CloudTrail 日志条目：

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

使用亚马逊监控亚马逊 Inspector Classic CloudWatch

您可以使用亚马逊监控 Amazon Inspector Classic CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。默认情况下，Amazon Inspector Classic 会 CloudWatch 在 5 分钟内向发送指标数据。您可以使用 AWS 管理控制台 AWS CLI、或 API 来查看 Amazon Inspector Classic 发送到的指标 CloudWatch。

有关亚马逊的更多信息 CloudWatch，请参阅亚马逊 CloudWatch 用户指南。

Amazon Inspector 经典 CloudWatch 指标

Amazon Inspector Classic 中的命名空间包括以下指标。

`AssessmentTargetARN` 指标：

指标	说明
`TotalMatchingAgents`	与此目标匹配的代理的数量
`TotalHealthyAgents`	与此目标匹配且正常运行的代理的数量
`TotalAssessmentRuns`	此目标的评估运行的数量
`TotalAssessmentRun Findings`	此目标的结果的数量

`AssessmentTemplateARN` 指标：

指标	说明
`TotalMatchingAgents`	与此模板匹配的代理的数量
`TotalHealthyAgents`	与此模板匹配且正常运行的代理的数量
`TotalAssessmentRuns`	此模板的评估运行的数量
`TotalAssessmentRun Findings`	此模板的结果的数量

聚合指标

指标	说明
TotalAssessmentRuns	此 AWS 账户中运行的评估次数

使用配置 Amazon Inspector 经典版 AWS CloudFormation

有关支持的 Amazon Inspector Classic 资源的参考信息 AWS CloudFormation，请参阅以下主题：

- AWS::Inspector::AssessmentTarget
- AWS::Inspector::AssessmentTemplate
- AWS::Inspector::ResourceGroup

> **Important**
>
> 有关支持 AWS 区域的 Amazon Inspector Classic 规则包列表，请参阅适用于规则包的 Amazon Inspector Classic ARNS。 ARNs

与集成 AWS Security Hub CSPM

AWS Security Hub CSPM为您提供安全状态的全面视图， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。Security Hub CSPM 从 AWS 账户、服务和支持的第三方合作伙伴产品中收集安全数据，并帮助您分析安全趋势并确定优先级最高的安全问题。

Amazon Inspector 与 Security Hub CSPM 的集成使您可以将亚马逊检查员的调查结果发送到 Security Hub CSPM。然后，Security Hub CSPM 可以将这些发现纳入其对您的安全态势的分析中。

目录

Amazon Inspector 如何向 Security Hub CSPM 发送调查结果

在 Security Hub CSPM 中，安全问题按调查发现进行跟踪。一些发现来自其他 AWS 服务或第三方合作伙伴检测到的问题。Security Hub CSPM 还有一套用于检测安全问题和生成调查发现的规则。

Security Hub CSPM 提供了用于管理来自所有这些来源的调查发现的工具。您可以查看和筛选调查发现列表，并查看调查发现的详细信息。请参阅 AWS Security Hub 用户指南中的查看结果。您还可以跟踪调查发现的调查状态。请参阅 AWS Security Hub 用户指南中的对调查发现采取措施。

Security Hub CSPM 中的所有发现都使用一种称为 AWS 安全调查结果格式 (ASFF) 的标准 JSON 格式。ASFF 包含有关问题根源、受影响资源以及调查发现当前状态的详细信息。请参阅 AWS Security Hub 用户指南中的 AWS Security Finding 格式 (ASFF) 。

Amazon Inspector 是向 Security Hub CSPM 发送调查结果的 AWS 服务之一。

Amazon Inspector 发送的结果类型

Amazon Inspector 将其生成的所有调查结果发送给 Security Hub CSPM。

Amazon Inspector 使用安全调查结果格式 (ASFF) 将调查结果发送给 Sec AWS urity Hub CSPM。在 ASFF 中，Types 字段提供调查发现类型。来自 Amazon Inspector 的结果可能具有 Types的以下值。

- 软件和配置 Checks/Vulnerabilities/CVE
- 软件和配置 Checks/AWS 安全性最佳 Practices/Network 可达性
- 软件和配置 Checks/Industry 以及监管 Standards/CIS 主机强化基准

发送调查发现的延迟

当 Amazon Inspector 创建新发现时，通常会在五分钟内将其发送到 Security Hub CSPM。

Security Hub CSPM 不可用时重试

如果 Security Hub CSPM 不可用，Amazon Inspector 会重试发送调查结果，直到收到调查结果。

更新 Security Hub CSPM 中的现有调查发现

在向 Security Hub CSPM 发送调查结果后，Amazon Inspector 会更新调查结果以反映对发现活动的其他观察结果。这将导致亚马逊检查员在 Security Hub CSPM 中发现的次数少于在 Amazon Inspector 中发现的内容。

来自 Amazon Inspector 的典型结果

Amazon Inspector 使用安全调查结果格式 (ASFF) 将调查结果发送给 Sec AWS urity Hub CSPM。

下面是 Amazon Inspector 典型结果的示例。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
```

```
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
 is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
 reachable from the internet. You can install the Inspector agent on this instance
 and re-run the assessment to check for any process listening on this port. The
 instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
 eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
 the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
 from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
```

```
    "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": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


启用和配置集成

若要使用与 Security Hub CSPM 的集成，您必须启用 Security Hub CSPM。有关如何启用 Security Hub CSPM 的信息，请参阅《AWS Security Hub User Guide》中的 Setting up Security Hub。

当你同时启用 Amazon Inspector 和 Security Hub CSPM 时，集成将自动启用。Amazon Inspector 开始向 Security Hub CSPM 发送调查结果。

如何停止发送调查发现

要停止向 Security Hub CSPM 发送调查发现，您可以使用 Security Hub CSPM 控制台或 API。

请参阅用户指南中AWS Security Hub 的禁用和启用来自集成的结果流（控制台） 或禁用来自集成的结果流（Security Hub API、AWS CLI）。

亚马逊 Inspector 经典版 ARNs

Amazon Inspector Classic 中的每个资源类型和规则包均有相关联的唯一 Amazon 资源名称 (ARN)。

目录

ARNs 适用于 Amazon Inspector 经典版

在 Amazon Inspector Classic 中，主要资源包括资源组、评估目标、评估模板、评估运行和结果。这些资源具有与之关联的唯一 Amazon 资源名称 (ARNs)，如下表所示。

资源类型	ARN 格式
资源组	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:resourcegroup/` *`ID`*
评估目标	`arn:aws:inspector:` *`region`*`:`*`account-id`* `:target/`*`ID`*

资源类型	ARN 格式
评估模板	arn:aws:inspector: *region*:*account-id* :target/*ID*:template: *ID*
评估运行	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*
调查发现	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*/finding/ *ID*

适用于规则包的 Amazon Inspector Classic ARNS

下表显示了所有支持区域中 ARNs 适用于 Amazon Inspector Classic 的规则包。

主题

美国东部（俄亥俄州）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85
CIS 操作系统安全配置基准	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh
网络可到达性	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30
安全最佳实践	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX

美国东部（弗吉尼亚州北部）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7
CIS 操作系统安全配置基准	arn:aws:inspector:us-east-1:31611246

规则包名称	进行筛选
	3485:rulespackage/0-rExsr2X8
网络可到达性	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
安全最佳实践	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

美国西部（北加利福尼亚）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa
CIS 操作系统安全配置基准	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
网络可到达性	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF
安全最佳实践	arn:aws:inspector:us-west-1:16698759

规则包名称	进行筛选
	0008:rulespackage/0-byoQRFYm

美国西部（俄勒冈州）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p
CIS 操作系统安全配置基准	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc
网络可到达性	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl
安全最佳实践	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ

亚太地区（孟买）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:ap-south-1:1625887

规则包名称	进行筛选
	57376:rulespackage/0-LqnJE9dO
CIS 操作系统安全配置基准	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m
网络可到达性	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1
安全最佳实践	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj

亚太地区（首尔）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc
CIS 操作系统安全配置基准	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-T9srhg1z
网络可到达性	arn:aws:inspector:ap-northeast-2:526

规则包名称	进行筛选
	946625049:rulespac kage/0-s3OmLzhL
安全最佳实践	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

亚太地区（悉尼）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
CIS 操作系统安全配置基准	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
网络可到达性	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
安全最佳实践	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-asL6HRgN

亚太地区（东京）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-gHP9oWNT
CIS 操作系统安全配置基准	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-7WNjqgGu
网络可到达性	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7
安全最佳实践	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq

欧洲地区（法兰克福）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-wNqHa8M9
CIS 操作系统安全配置基准	arn:aws:inspector:eu-central-1:53750

规则包名称	进行筛选
	3971621:rulespackage/0-nZrAVuv8
网络可到达性	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
安全最佳实践	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

欧洲地区（爱尔兰）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
CIS 操作系统安全配置基准	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
网络可到达性	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SPzU33xe
安全最佳实践	arn:aws:inspector:eu-west-1:35755712

规则包名称	进行筛选
	9151:rulespackage/0-SnojL3Z6

欧洲地区（伦敦）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
CIS 操作系统安全配置基准	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
网络可到达性	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
安全最佳实践	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

欧洲地区（斯德哥尔摩）

规则包名称	进行筛选
常见漏洞和风险	arn:aws:inspector:eu-north-1:4534202

规则包名称	进行筛选
	44670:rulespackage/0-IgdgIewd
CIS 操作系统安全配置基准	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f
网络可到达性	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu
安全最佳实践	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf

AWS GovCloud（美国东部）

规则包名称	进行筛选
常见漏洞和风险	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFuOb
CIS 操作系统安全配置基准	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-pTLCdIww

规则包名称	进行筛选
安全最佳实践	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud（美国西部）

规则包名称	进行筛选
常见漏洞和风险	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
CIS 操作系统安全配置基准	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
安全最佳实践	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

文档历史记录

下表介绍了 2018 年 5 月之后 Amazon Inspector Classic 的文档发布历史记录。

变更	说明	日期
终止支持通知	终止支持通知：2026年5月20日， AWS 将终止对 Amazon Inspector Classic的支持。2026 年 5 月 20 日之后，您将无法再访问亚马逊 Inspector Classic 控制台或亚马逊 Inspector Classic 资源。有关更多信息，请参阅 Amazon Inspector Classic 终止支持。	2025 年 5 月 20 日
更新了密码安全最佳实践	针对 EC2 实例密码长度和密码复杂性的 Amazon Inspector Classic 安全最佳实践要求已更新。请参阅配置密码最小长度和配置密码复杂性	2021 年 3 月 8 日
增加了对较新操作系统版本的支持	Amazon Inspector Classic 现在支持以下操作系统版本：Ubuntu 20.4 LTS、Debian 10.x、RHEL 8.x 和 Windows Server 2019 Base。	2020 年 10 月 15 日
安全信息已合并到一个新的安全章节中	Amazon Inspector Classic 的安全信息（包括有关管理 Identity and Access Management 的信息）已合并到一个安全章节中。请参阅 Amazon Inspector Classic 安全性。	2020 年 4 月 7 日

更新了文档，以删除针对运行时行为分析规则包的支持。	更新了多个主题，以删除有关不再受支持的运行时行为分析规则包的信息。	2019 年 9 月 5 日
增加了操作系统支持	增加了 Amazon Inspector Classic 对 CentOS 7.6 的支持。有关更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域和规则包在受支持的操作系统中的可用性。	2018 年 12 月 3 日
新增内容	增加了 Amazon Inspector Classic 网络可到达性规则包，允许用户运行无代理评估，分析网络配置是否存在安全漏洞。有关更多信息，请参阅网络可到达性。	2018 年 11 月 9 日
增加了操作系统支持	增加了 Amazon Inspector Classic 对 RHEL 7.6 的支持。有关更多信息，请参阅Amazon Inspector Classic 支持的操作系统和区域和规则包在受支持的操作系统中的可用性。	2018 年 10 月 30 日
添加了操作系统支持	添加了对各种操作系统到 CIS 准则规则包。有关更多信息，请参阅 Center for Internet Security (CIS) 基准和规则包在受支持的操作系统中的可用性。	2018 年 8 月 13 日
增加了区域支持	增加了对 AWS GovCloud (US) 的区域支持。	2018 年 13 月 6 日

下表介绍了 2018 年 6 月之前 Amazon Inspector Classic 的文档发布历史记录。

更改	描述	日期
新增内容	添加了将一个账户中的所有 Amazon EC2 实例作为目标的功能。有关更多信息，请参阅 Amazon Inspector Classic 评估目标。	2018 年 5 月 24 日
添加了操作系统支持	增加了 Amazon Inspector Classic 对 Amazon Linux 2018.03 和 Ubuntu 18.04 的支持。	2018 年 5 月 15 日
新增内容	添加了设置周期性 Amazon Inspector Classic 评估的功能。	2018 年 4 月 30 日
新增内容	添加了通过控制台安装 Amazon Inspector Classic 代理的功能。	2018 年 4 月 30 日
添加了操作系统支持	添加了 Amazon Inspector Classic 对 Amazon Linux 2 的支持。	2018 年 3 月 13 日
添加了操作系统支持	增加了对 Windows Server 2016 Base 的 Amazon Inspector Classic 评估支持。	2018 年 2 月 20 日
增加了区域支持	增加了 Amazon Inspector Classic 对 US East (Ohio) 区域的支持。	2018 年 2 月 7 日
新增内容	Amazon Inspector Classic 评估现在可在内核模块不可用的情况下运行。	2018 年 1 月 11 日

更改	描述	日期
增加了区域支持	增加了 Amazon Inspector Classic 对 EU（Frankfurt） 区域的支持。	2017 年 12 月 19 日
新增内容	添加了使用 Amazon Inspector Classic API 和控制台检查 Amazon Inspector Classic 代理运行状况的功能。	2017 年 12 月 15 日
新增内容	添加了以下功能： • 服务相关角色的使用 • Amazon Inspector Classic 代理 AMI 已在 AWS 市场上市 • 亚马逊 Inspector 经典 CloudFormation 版模板	2017 年 12 月 5 日
添加了操作系统支持	添加了 Amazon Inspector Classic 对 CentOS 7.4 的评估支持。	2017 年 11 月 9 日
添加了操作系统支持	添加了对 Amazon Linux 2017.09 的 Amazon Inspector Classic 评估支持。	2017 年 10 月 11 日
添加了操作系统支持	添加了 Amazon Inspector Classic 对 RHEL 7.4 的评估支持。	2018 年 2 月 20 日
添加了 HIPAA 资格	Amazon Inspector Classic 现已符合 HIPAA 要求。	2017 年 7 月 31 日

更改	描述	日期
新增内容	增加了通过亚马逊 CloudWatch 活动自动触发 Amazon Inspector Classic 安全评估的功能。	2017 年 7 月 27 日
增加了区域支持	增加了 Amazon Inspector Classic 对 US West (N. California) 区域的支持。	2018 年 6 月 6 日
添加了操作系统支持	添加了 Amazon Inspector Classic 对 RHEL 6.2-6.9、RHEL 7.2-7.3、CentOS 6.9 和 CentOS 7.2-7.3 的评估支持。	2017 年 5 月 23 日
添加了操作系统支持	添加了对 Amazon Linux 2017.03 的 Amazon Inspector Classic 评估支持。	2017 年 4 月 25 日
新内容和新增的操作系统支持	增加了： • Amazon Inspector Classic 支持 Ubuntu 16.04。 • 可使用 Lambda 蓝图自动进行 Amazon Inspector Classic 操作。	2017 年 1 月 5 日
新增操作系统支持	添加了 Amazon Inspector Classic 对 Microsoft Windows 的支持。	2016 年 8 月 26 日
增加了区域支持	增加了 Amazon Inspector Classic 对 Asia Pacific (Seoul) 区域的支持。	2016 年 8 月 26 日

更改	描述	日期
增加了区域支持	增加了 Amazon Inspector Classic 对 Asia Pacific (Mumbai) 区域的支持。	2016 年 4 月 25 日
增加了区域支持	增加了 Amazon Inspector Classic 对 Asia Pacific (Sydney) 区域的支持。	2016 年 4 月 25 日
服务启动	Amazon Inspector Classic 服务已发布。	2015 年 10 月 7 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。