Concetti e procedure di rilevamento e risposta agli incidenti di AWS

Guida per l'utente di AWS Incident Detection and Response

Version May 26, 2026

Guida per l'utente di AWS Incident Detection and Response: Concetti e procedure di rilevamento e risposta agli incidenti di AWS

Table of Contents

Cos'è AWS Incident Detection and Response?

AWS Incident Detection and Response offre ai clienti idonei di AWS Enterprise Support un coinvolgimento proattivo in caso di incidenti per ridurre il potenziale di guasto e accelerare il ripristino dei carichi di lavoro critici in caso di interruzioni. Incident Detection and Response facilita la collaborazione AWS per sviluppare runbook e piani di risposta personalizzati per ogni carico di lavoro integrato.

Incident Detection and Response offre le seguenti funzionalità chiave:

- Migliore osservabilità: AWS gli esperti forniscono indicazioni per aiutarvi a definire e correlare metriche e allarmi tra i livelli applicativo e infrastrutturale del carico di lavoro per rilevare tempestivamente le interruzioni.
- Tempo di risposta di 5 minuti: i tecnici addetti alla gestione degli incidenti interagiscono in modo proattivo entro 5 minuti dall'allarme, dai carichi di lavoro o in risposta a un caso critico da voi segnalato.
- Risoluzione più rapida: gli IME utilizzano runbook predefiniti e personalizzati sviluppati per i tuoi carichi di lavoro, creano un caso Support per tuo conto e gestiscono gli incidenti sul tuo carico di lavoro. Gli IME garantiscono la gestione degli incidenti in un unico thread e vi mantengono in contatto con gli esperti giusti fino alla risoluzione dell'incidente. AWS
- Riduzione del rischio di guasto: dopo la risoluzione, gli IME forniscono una revisione post-incidente (su richiesta). Inoltre, gli AWS esperti collaborano con voi per applicare le lezioni apprese per migliorare il piano di risposta agli incidenti e i runbook. Puoi anche sfruttare AWS Resilience Hub per il monitoraggio continuo della resilienza dei tuoi carichi di lavoro.

Argomenti

Registrati per un Account AWS

Per iniziare AWS, hai bisogno di un Account AWS. Per informazioni sulla creazione di un Account AWS, vedi Guida introduttiva a un Account AWS nella Guida Gestione dell'account AWS di riferimento.

Condizioni d'uso per il rilevamento e la risposta agli incidenti

L'elenco seguente descrive i requisiti e le limitazioni principali per l'utilizzo di AWS Incident Detection and Response. È importante comprendere queste informazioni prima di utilizzare il servizio, poiché riguardano aspetti come i requisiti del piano di supporto, il processo di onboarding e la durata minima dell'abbonamento.

- AWS Incident Detection and Response è disponibile per gli account Direct ed Partner-resold Enterprise Support.
- AWS Incident Detection and Response non è disponibile per gli account su Partner Led Support.
- È necessario mantenere AWS Enterprise Support in qualsiasi momento per tutta la durata del servizio Incident Detection and Response. Per informazioni, vedere Enterprise Support. La cessazione di Enterprise Support comporta la rimozione simultanea dal servizio AWS Incident Detection and Response.
- Tutti i carichi di lavoro su AWS Incident Detection and Response devono passare attraverso il processo di onboarding del carico di lavoro.
- La durata minima per sottoscrivere un account ad AWS Incident Detection and Response è di novanta (90) giorni. Tutte le richieste di cancellazione devono essere inviate trenta (30) giorni prima della data di entrata in vigore prevista per l'annullamento.
- AWS gestisce le tue informazioni come descritto nell'AWS Informativa sulla privacy.

> **Note**
>
> Per domande relative alla fatturazione con Incident Detection and Response, consulta Ottenere assistenza con la AWS fatturazione.

Architettura di rilevamento e risposta agli incidenti

AWS Incident Detection and Response si integra con l'ambiente esistente, come mostrato nel grafico seguente. L'architettura include i seguenti servizi:

- Amazon EventBridge: Amazon EventBridge funge da unico punto di integrazione tra i tuoi carichi di lavoro e AWS Incident Detection and Response. Gli allarmi vengono importati dai tuoi strumenti di monitoraggio, come Amazon, CloudWatch tramite Amazon EventBridge utilizzando regole predefinite gestite da. AWS Per consentire a Incident Detection and Response di creare e gestire la EventBridge regola, installi un ruolo collegato al servizio. Per ulteriori informazioni su questi servizi, consulta What is Amazon EventBridge and Amazon EventBridge rules, What is Amazon CloudWatch e Using service-linked roles for. AWS Health
- AWS Health: AWS Health offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità delle tue risorse Servizi AWS e dei tuoi account. Incident Detection and Response si utilizza AWS Health per tenere traccia degli eventi relativi ai carichi di lavoro Servizi AWS utilizzati dai tuoi carichi di lavoro e per avvisarti quando viene ricevuto un avviso dal tuo carico di lavoro. Per ulteriori informazioni AWS Health, consulta What is. AWS Health
- AWS Systems Manager: Systems Manager fornisce un'interfaccia utente unificata per l'automazione e la gestione delle attività tra le AWS risorse. AWS Incident Detection and Response ospita informazioni sui carichi di lavoro, inclusi dettagli sull'architettura del carico di lavoro, dettagli sugli allarmi e i relativi runbook di gestione degli incidenti nei AWS Systems Manager documenti (per i dettagli, consulta AWS Systems Manager Documenti). Per saperne di più AWS Systems Manager, consulta What is. AWS Systems Manager
- I tuoi runbook specifici: un runbook di gestione degli incidenti definisce le azioni che AWS Incident Detection and Response esegue durante la gestione degli incidenti. I tuoi runbook specifici indicano ad AWS Incident Detection and Response chi contattare, come contattarli e quali informazioni condividere.

Ruoli e responsabilità nel rilevamento e nella risposta agli incidenti

La tabella RACI (Responsible, Accountable, Consulted and Informed) di AWS Incident Detection and Response descrive i ruoli e le responsabilità per varie attività relative al rilevamento e alla risposta agli incidenti. Questa tabella aiuta a definire il coinvolgimento del cliente e del team AWS

Incident Detection and Response in attività come la raccolta dei dati, la revisione della fattibilità delle operazioni, la configurazione dell'account, la gestione degli incidenti e la revisione post-incidente.

Attività	Cliente	Rilevamento e risposta agli incidenti
Raccolta dei dati		
Introduzione al cliente e al carico di lavoro	Consultato	Responsabile
Architecture	Responsabile	Responsabile
Operazioni	Responsabile	Responsabile
Determina CloudWatch gli allarmi da configurare	Responsabile	Responsabile
Definisci un piano di risposta agli incidenti	Responsabile	Responsabile
Revisione della prontezza operativa		
Effettua una revisione ben architettata (WAR) sul carico di lavoro	Consultato	Responsabile
Convalida la risposta agli incidenti	Consultato	Responsabile
Convalida la matrice di allarme	Consultato	Responsabile
Identifica AWS i servizi chiave utilizzati dal carico di lavoro	Responsabile	Responsabile

Attività	Cliente	Rilevamento e risposta agli incidenti
Configurazione dell'account		
Crea un ruolo IAM nell'account del cliente	Responsabile	Informato
Installa la EventBridge regola gestita utilizzando il ruolo creato	Informato	Responsabile
Prova gli allarmi integrati (o APM) CloudWatch	Responsabile	Informato
Verifica che gli allarmi dei clienti coinvolgano il rilevamento e la risposta agli incidenti	Informato	Responsabile
Aggiorna gli allarmi	Responsabile	Consultato
Aggiorna i runbook	Consultato	Responsabile
Gestione degli incidenti		
Notifica in modo proattivo gli incidenti rilevati tramite Incident Detection and Response	Informato	Responsabile
Fornire una risposta agli incidenti	Informato	Responsabile
Fornisci la risoluzione degli incidenti e il ripristino dell'infrastruttura	Responsabile	Consultato
Post-incident recensione		

Attività	Cliente	Rilevamento e risposta agli incidenti
Richiedi una revisione post-incidente	Responsabile	Informato
Fornire una revisione post-incidente	Informato	Responsabile

Disponibilità regionale per il rilevamento e la risposta agli incidenti

AWS Incident Detection and Response è disponibile in inglese, giapponese, mandarino e coreano per gli account AWS Enterprise Support ospitati in uno dei seguenti paesi: Regioni AWS

Regione AWS	Nome
Stati Uniti orientali (Virginia settentrionale)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
Regione Stati Uniti occidentali (California settentrionale)	us-west-1
Stati Uniti occidentali (Oregon)	us-west-2
Regione Canada (Centrale)	ca-central-1
Regione Canada occidentale (Calgary)	ca-west-1
Sud America (San Paolo)	sa-east-1
Regione Europa (Francoforte)	eu-central-1
Europa (Irlanda)	eu-west-1

Regione AWS	Nome
Regione Europa (Londra)	eu-west-2
Regione Europa (Parigi)	eu-west-3
Regione Europa (Stoccolma)	eu-north-1
Regione Europa (Zurigo)	eu-central-2
Regione Europa (Milano)	eu-south-1
Regione Europa (Spagna)	eu-south-2
Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacifico (Malesia)	ap-southeast-5
Africa (Città del Capo)	af-south-1
Israele (Tel Aviv)	il-central-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1

Regione AWS	Nome
Medio Oriente (Bahrein)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Inizia a usare Incident Detection and Response

I carichi di lavoro e gli allarmi sono fondamentali per AWS Incident Detection and Response. AWS collabora a stretto contatto con te per definire e monitorare carichi di lavoro specifici che sono fondamentali per il tuo business. AWS ti aiuta a impostare allarmi che notificano al tuo team problemi significativi di prestazioni o impatto sui clienti. Gli allarmi configurati correttamente sono essenziali per il monitoraggio proattivo e la risposta rapida agli incidenti nell'ambito di Incident Detection and Response.

Informazioni sui carichi di lavoro relativi al rilevamento e alla risposta agli incidenti

Puoi selezionare carichi di lavoro specifici per il monitoraggio e la gestione degli incidenti critici utilizzando AWS Incident Detection and Response. Un carico di lavoro è una raccolta di risorse e codice che interagiscono per fornire valore aziendale. Un carico di lavoro può essere costituito da tutte le risorse e il codice che compongono il portale dei pagamenti bancari o un sistema di gestione delle relazioni con i clienti (CRM). Puoi ospitare un carico di lavoro singolo Account AWS o multiplo. Account AWS

Ad esempio, è possibile avere un'applicazione monolitica ospitata in un singolo account (ad esempio, Employee Performance App nel diagramma seguente). Oppure, potresti avere un'applicazione (ad esempio, Storefront Webapp nel diagramma) suddivisa in microservizi che si estendono su diversi account. Un carico di lavoro può condividere risorse, ad esempio un database, con altre applicazioni o carichi di lavoro, come illustrato nel diagramma seguente.

Per iniziare con l'onboarding dei carichi di lavoro, consulta. Incorpora i carichi di lavoro al rilevamento e alla risposta agli incidenti

Informazioni sugli allarmi in Incident Detection and Response

Gli allarmi sono una parte fondamentale del rilevamento e della risposta agli incidenti. Gli allarmi forniscono visibilità sulle prestazioni delle applicazioni e dell'infrastruttura sottostante AWS . AWS collabora con voi per definire metriche e soglie di allarme appropriate che si attivano solo quando c'è un impatto critico sui carichi di lavoro monitorati. L'obiettivo è far sì che gli allarmi coinvolgano i risolutori specificati, che poi collaborino con il team di gestione degli incidenti per

mitigare rapidamente i problemi. Configura gli allarmi in modo che entrino nello stato Allarme solo quando si verifica un peggioramento significativo delle prestazioni o dell'esperienza del cliente che richiede un'attenzione immediata. Alcuni tipi chiave di allarmi includono quelli che indicano l'impatto aziendale, Amazon CloudWatch Canaries e gli allarmi aggregati che monitorano le dipendenze.

Per iniziare a inserire gli allarmi, consulta. Ingestione degli allarmi

Incorpora i carichi di lavoro al rilevamento e alla risposta agli incidenti

AWS Incident Detection and Response consente il monitoraggio e la gestione degli incidenti critici per i carichi di lavoro selezionati. Un carico di lavoro è una raccolta di risorse che collaborano per fornire valore aziendale, ad esempio un portale di pagamento o un sistema di gestione delle relazioni con i clienti (CRM). Puoi ospitare questi carichi di lavoro in un unico account Account AWS o distribuiti su più account, a seconda dell'architettura.

Indice

Integrazione del rilevamento e della risposta agli incidenti con la CLI IDR

L'interfaccia a riga di comando di AWS Incident Detection and Response Customer Command Line Interface (IDR CLI) è uno strumento di interfaccia a riga di comando che semplifica l'onboarding di AWS Incident Detection and Response.

La CLI IDR viene eseguita per eseguire AWS CloudShell le seguenti funzioni:

- Raccogli informazioni sull'onboarding
- Raccogli dati AWS sulle risorse tramite l'API Resource Groups Tagging
- Gestisci i casi Supporto AWS
- Crea nuovi CloudWatch allarmi Amazon o inserisci quelli esistenti
- Implementa e testa l'infrastruttura AWS CloudFormation per consentire a strumenti di terze parti di inviare avvisi a Incident Detection and Response.

La CLI IDR può essere eseguita in modalità interattiva per guidarti nelle fasi di onboarding o in modalità offline per casi collettivi o d'uso. DevOps

Per ulteriori informazioni su come utilizzare la CLI IDR, tra cui installazione, prerequisiti ed esempi completi, consulta CLI for AWS Incident Detection and Response.

Supporto linguistico per la CLI IDR

AWS Incident Detection and Response è disponibile in inglese, giapponese, mandarino e coreano. Se hai bisogno di assistenza in giapponese, mandarino o coreano, contattaci AWS tramite il Supporto AWS caso creato dalla CLI IDR o contatta il tuo Technical Account Manager (TAM).

Opzioni alternative per l'onboarding dei carichi di lavoro

Se non riesci a utilizzare la CLI IDR per l'onboarding, consulta il tuo Technical Account Manager (TAM) per opzioni alternative. Per ulteriori informazioni, consulta Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response (percorso di eccezione)

Ingestione degli allarmi

L'interfaccia a riga di comando dei clienti di AWS Incident Detection and Response (IDR CLI) può creare nuovi allarmi CloudWatch Amazon o importare quelli esistenti e può implementare e testare l'infrastruttura per consentire a strumenti di terze parti di inviare AWS CloudFormation avvisi ad AWS Incident Detection and Response.

AWS Incident Detection and Response può importare allarmi da Amazon CloudWatch e strumenti di Application Performance Monitoring (APM) di terze parti tramite Amazon: EventBridge

- Ingestione di allarmi CloudWatch
- Inserimento di allarmi di monitoraggio delle prestazioni di applicazioni di terze parti

Fasi per l'inserimento degli allarmi

È necessario completare i seguenti passaggi per l'inserimento degli allarmi:

- Definizione di allarme
- Inserimento di allarmi tramite la CLI IDR

- Revisione e feedback degli allarmi
- Fornisci l'accesso per l'inserimento degli allarmi alla funzione Incident Detection and Response
- Gli allarmi diventano attivi

Opzioni alternative per l'ingestione degli allarmi

Se non riesci a utilizzare la CLI IDR per l'inserimento degli allarmi, consulta il tuo Technical Account Manager (TAM) per opzioni alternative. Per ulteriori informazioni, consulta Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response (percorso di eccezione)

Fornisci l'accesso per l'inserimento degli allarmi alla funzione Incident Detection and Response

> **Note**
>
> Se non hai creato il ruolo collegato al servizio (SLR) durante l'onboarding della CLI IDR, segui i passaggi seguenti per fornire manualmente l'accesso.

Per consentire ad AWS Incident Detection and Response di importare allarmi dal tuo account, crea la `AWSServiceRoleForHealth_EventProcessor` reflex. AWS presuppone che l'SLR crei una regola gestita EventBridge nel tuo account. La EventBridge regola gestita invia notifiche dal tuo account ad AWS Incident Detection and Response. Per informazioni su questa reflex, inclusa la policy AWS gestita associata, consulta Using service-linked roles nella User Guide.

Puoi creare questo ruolo collegato al servizio nel tuo account seguendo le istruzioni in Creare un ruolo collegato ai servizi nella Guida per l'utente.AWS Identity and Access Management In alternativa, puoi usare il seguente AWS Command Line Interface comando ():AWS CLI

```
aws iam create-service-linked-role --aws-service-name event-
processor.health.amazonaws.com
```

Uscite chiave

- Creazione riuscita del ruolo collegato al servizio nel tuo account.

> **Note**
>
> Il ruolo collegato al servizio - AWSServiceRoleForHealth _ EventProcessor deve essere creato in ogni account che utilizzerai per inviare allarmi ad AWS Incident Detection and Response.

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- Utilizzo di ruoli collegati ai servizi per
- Creazione di un ruolo collegato al servizio
- AWS policy gestita: AWS Health_EventProcessorServiceRolePolicy

Definizione di allarme

Quando esegui l'onboarding dei tuoi allarmi in AWS Incident Detection and Response, sei responsabile della definizione delle metriche e delle configurazioni degli allarmi che forniscono visibilità sulle prestazioni delle tue applicazioni. Come parte di questo processo, devi anche identificare i team all'interno dell'organizzazione responsabili della risposta a questi allarmi.

Durante la preparazione degli allarmi, consigliamo le seguenti best practice:

- Gli allarmi entrano nello stato «Allarme» solo quando si verifica un impatto critico continuo sul carico di lavoro monitorato che richiede l'attenzione immediata del team e. AWS Gli allarmi che si attivano e non si ripristinano automaticamente richiedono ai tuoi team di unirsi a un incident bridge con AWS Incident Detection and Response.
- Assicurati che le informazioni di contatto fornite consentano ad AWS Incident Detection and Response di coinvolgere in modo affidabile i team appropriati all'interno della tua organizzazione per risolvere gli incidenti. 24/7

Risultati chiave

- Un elenco di allarmi e dettagli di contatto, che fornisci ad AWS Incident Detection and Response utilizzando la CLI IDR.

Per ulteriori informazioni sulla definizione e l'inserimento degli CloudWatch allarmi Amazon, consulta. Ingestione di allarmi CloudWatch

Per ulteriori informazioni sull'acquisizione di allarmi di monitoraggio delle prestazioni delle applicazioni di terze parti, consulta. Inserimento di allarmi di monitoraggio delle prestazioni di applicazioni di terze parti

Ingestione di allarmi CloudWatch

AWS Incident Detection and Response può inserire CloudWatch allarmi Amazon per fornire un monitoraggio proattivo dei carichi di lavoro critici. Inserendo i tuoi CloudWatch allarmi Amazon per il monitoraggio, AWS Incident Detection and Response può:

- Rileva automaticamente quando gli allarmi entrano nello stato «Allarme».
- Coinvolgi i tuoi team per rispondere e risolvere gli incidenti in modo collaborativo.

Per garantire l'efficacia degli allarmi integrati, AWS Incident Detection and Response consiglia le seguenti best practice:

- Configura gli allarmi con espressioni matematiche metriche per sopprimerli durante i periodi di manutenzione regolare o le esecuzioni di lavori in batch per evitare allarmi falsi positivi.
- Imposta il trattamento dei dati mancanti sugli allarmi in base alla frequenza di consegna prevista dei datapoint. Ad esempio, le metriche di monitoraggio degli allarmi che generano un flusso continuo di punti dati dovrebbero considerare i dati mancanti come «violazioni» (errati) poiché i punti dati mancanti potrebbero indicare un problema con la risorsa sottostante monitorata. Al contrario, le metriche di monitoraggio degli allarmi che segnalano raramente i punti dati, ad esempio le metriche di monitoraggio degli allarmi che registrano i punti dati solo quando si verifica un guasto o un errore, dovrebbero considerare i dati mancanti come (buoni). NotBreaching
- Definisci gli allarmi che entrano nello stato «Allarme» quando c'è un impatto critico e continuo sul tuo carico di lavoro. Ad esempio, configura gli allarmi in modo che si attivino dopo il tempo previsto necessario per sostituire automaticamente le risorse non integre, anziché dopo il rilevamento iniziale di risorse non integre.
- Identifica e crea allarmi per metriche personalizzate che rappresentano direttamente l'esperienza del cliente per il tuo carico di lavoro.

Per un elenco degli CloudWatch allarmi Amazon consigliati più comuni Servizi AWS, consulta le best practice per il rilevamento degli incidenti e gli allarmi di risposta su AWS re:POST.

Inserimento di allarmi di monitoraggio delle prestazioni di applicazioni di terze parti

AWS Incident Detection and Response supporta l'inserimento di allarmi da strumenti di Application Performance Monitoring (APM) di terze parti tramite Amazon. EventBridge Questa integrazione offre flessibilità grazie all'inserimento di avvisi APM, permettendo il routing degli eventi APM tramite vari canali verso Servizi AWS un bus di eventi Amazon EventBridge del tuo account.

Esempi di percorsi di integrazione:

- Fonte (APM) → AWS Servizio (esempio: Amazon API Gateway o Amazon SNS) → Funzione Transform Lambda → Amazon EventBridge Event Bus personalizzato → AWS Incident Detection and Response
- Fonte (APM) → Partner Amazon EventBridge Event Bus → Transform Lambda Function → EventBridge Amazon Event Bus personalizzato → AWS Incident Detection and Response

AWS Incident Detection and Response installa una regola gestita sul bus eventi personalizzato per importare gli avvisi inviati da Transform Lambda Functions. È importante notare che per SaaS Amazon EventBridge Integrations, il bus eventi partner non è il bus eventi su cui è installata una regola gestita. Per un elenco completo degli APM con integrazioni dei partner con Amazon EventBridge, consulta Amazon integrazioni. EventBridge

Esempio di integrazione utilizzando un bus di eventi partner o altre AWS fonti di bus di eventi

Il diagramma seguente mostra un esempio di integrazione utilizzando un bus di eventi partner o altre sorgenti di bus di AWS eventi.

Per un elenco completo degli APM con integrazioni dei partner con Amazon EventBridge, consulta Amazon integrazioni. EventBridge

Esempio di integrazione con Amazon API Gateway

Il diagramma seguente mostra un esempio di integrazione utilizzando un API Gateway.

Esempio di integrazione con Amazon Simple Notification Service

Il diagramma seguente mostra un esempio di integrazione con Amazon SNS.

Per semplificare il processo di integrazione, AWS Incident Detection and Response fornisce CloudFormation modelli per i tipi di integrazione più comunemente usati. Questi modelli automatizzano la configurazione delle AWS risorse e dei ruoli IAM necessari.

CloudFormation I modelli e le istruzioni per creare manualmente vari tipi di integrazione sono disponibili nella documentazione di integrazione corrispondente riportata di seguito:

- Inserisci allarmi dagli APM con integrazione diretta EventBridge
- Inserisci allarmi dagli APM senza integrazione diretta con EventBridge
- Inserisci allarmi dagli APM con integrazione diretta con Amazon SNS

> **Note**
>
> I CloudFormation modelli richiedono modifiche. Queste modifiche sono illustrate negli argomenti precedenti. Per ulteriori informazioni sul formato di payload richiesto per l'invio di avvisi APM ad AWS Incident Detection and Response, consulta. Requisiti di payload per l'acquisizione di avvisi APM con EventBridge

Requisiti di payload per l'acquisizione di avvisi APM con EventBridge

Da dove vengono acquisiti gli avvisi APM per Incident Detection and Response?

AWS Incident Detection and Response installa una regola gestita sul bus degli eventi a cui invii il payload finale trasformato. È consigliabile creare un bus di eventi personalizzato per questo scopo.

In che formato devono essere i payload?

Le seguenti coppie minime JSON chiave:valore sono richieste negli eventi del bus degli eventi acquisiti da AWS Incident Detection and Response:

```
{
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent"
    "detail": {
        "incident-detection-response-identifier": "Your alarm name from your APM",
    }
}
```

Gli esempi seguenti mostrano un evento proveniente da un bus di eventi partner prima e dopo la sua trasformazione.

Prima della trasformazione:


```
{
    "version": "0",
    "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
    "detail-type": "Datadog Alert Notification",
    "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
 "max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
 <= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
```

```
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

Nota che prima che l'evento venga trasformato `detail-type` e `source` indica i dettagli APM da cui ha avuto origine l'avviso. Questi devono essere modificati prima dell'ingestione. La `incident-detection-response-identifier` chiave non è ancora presente e deve essere aggiunta anche prima dell'ingestione.

Una funzione Lambda trasforma l'evento precedente e lo inserisce nel bus eventi di destinazione personalizzato o predefinito. Il payload trasformato deve includere le coppie chiave:valore richieste.

Dopo la trasformazione:

```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "UnHealthyHostCount",
```

```
        "alert_type": "error",
        "event_type": "query_alert_monitor",
        "meta": {
            "monitor": {
                "id": 222222,
                "org_id": 3333333333,
                "type": "query alert",
                "name": "UnHealthyHostCount",
                "message": "@awseventbridge-Datadog-aaa111bbbc",
                "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
<= 1",
                "created_at": 1686884769000,
                "modified": 1698244915000,
                "options": {
                    "thresholds": {
                        "critical": 1.0
                    }
                },
            },
            "result": {
                "result_id": 7281010972796602670,
                "result_ts": 1698244878,
                "evaluation_ts": 1698244868,
                "scheduled_ts": 1698244938,
                "metadata": {
                    "monitor_id": 222222,
                    "metric": "aws.applicationelb.un_healthy_host_count"
                }
            },
            "transition": {
                "trans_name": "Triggered",
                "trans_type": "alert"
            },
            "states": {
                "source_state": "OK",
                "dest_state": "Alert"
            },
            "duration": 0
        },
        "priority": "normal",
        "source_type_name": "Monitor Alert",
        "tags": [
```

```
            "aws_account:123456789012",
            "monitor"
        ]
    }
}
```

Nota che `detail-type` è oraams.monitoring/generic-apm, la fonte è ora `GenericAPMEvent` e sotto i dettagli c'è una nuova coppia chiave:valore:. `incident-detection-response-identifier`

Il `incident-detection-response-identifier` valore viene ricavato dal nome dell'avviso in base al payload inviato dall'APM. I percorsi dei nomi degli avvisi APM sono diversi da un APM all'altro. È necessario configurare una funzione Lambda per prendere il nome dell'allarme dal percorso corretto nel payload JSON APM ricevuto da Lambda e utilizzarlo per il valore. `incident-detection-response-identifier`

`incident-detection-response-identifier`i valori devono essere univoci per tipo di allarme inviato ad AWS Incident Detection and Response. Ogni nome univoco impostato su `incident-detection-response-identifier` deve essere fornito al team AWS Incident Detection and Response durante l'onboarding. Gli eventi che hanno un valore sconosciuto o mancante per la `incident-detection-response-identifier` chiave non vengono elaborati.

Inserisci allarmi dagli APM con integrazione diretta EventBridge

L'argomento seguente mostra il processo di invio di allarmi ad AWS Incident Detection and Response dagli strumenti di Application Performance Monitoring (APM) che hanno un'integrazione diretta con Amazon. EventBridge Per un elenco completo degli APM che hanno un'integrazione diretta con Amazon EventBridge, consulta le EventBridgeintegrazioni di Amazon.

Puoi distribuire il CloudFormation modello fornito o configurare manualmente questa integrazione. Prima di configurare l'integrazione, verifica che il ruolo AWS collegato al servizio (SLR) sia stato creato nei `AWSServiceRoleForHealth_EventProcessor` tuoi account.

Opzione 1: Utilizzo CloudFormation

È disponibile un CloudFormation modello per semplificare il processo di creazione dell'infrastruttura di integrazione necessaria per importare allarmi in AWS Incident Detection and Response dal tuo APM con integrazione Amazon. EventBridge

> **Note**
>
> - Sono previsti costi aggiuntivi per le risorse distribuite tramite questo CloudFormation modello (ad esempio: Lambda e). EventBridge Per ulteriori informazioni sui prezzi di questi servizi, consulta la sezione Prezzi.AWS
> - Implementa questo CloudFormation modello in ogni AWS account e regione in cui AWS Incident Detection and Response deve inserire allarmi. Gli incidenti e i casi di supporto vengono aperti sull' AWS account da cui è stato ricevuto l'avviso APM.
> - Questo documento utilizza New Relic come esempio, tuttavia il CloudFormation modello può essere utilizzato per qualsiasi APM che abbia un'integrazione SaaS con Amazon. EventBridge
> - Dopo aver testato l'integrazione, rimuovi le istruzioni logger.info () da `TransformLambdaFunction` per evitare che il payload venga visualizzato in Amazon Logs. CloudWatch

Prerequisiti per la distribuzione di questo modello: CloudFormation

- Una fonte per eventi partner deve essere configurata in Amazon EventBridge. Per istruzioni su come configurare il tuo APM come fonte di eventi, consulta Ricezione di eventi da un partner SaaS con Amazon nella EventBridge EventBridge Amazon User Guide.
- La `TransformLambdaFunction` (funzione Lambda) nel modello deve essere modificata per impostarla sul valore desiderato in base `["detail"]["incident-detection-response-identifier"]` al percorso JSON del nome dell'avviso nel payload APM.

Passaggi preliminari:

1. Apri la EventBridge console. Nel menu Integrazione, seleziona Partner event sources.
   - Cerca il tuo APM nella casella dei EventBridge partner di Amazon.
   - Scegli Setup, quindi segui le istruzioni fornite.
     - Nota: l'ultimo passaggio consiste nel scegliere Associa a Event Bus nella console per l'origine dell'evento Partner. Selezionando questa opzione, viene creato automaticamente un Partner Event Bus con lo stesso nome della fonte dell'evento Partner (i nomi devono corrispondere).

- Copia il nome del Partner Event Bus o della fonte. L'Event Bus o la fonte vengono utilizzati come parametro, denominato`PartnerEventBusNameParameter`, durante la distribuzione del CloudFormation modello.
  - Esempio per New Relic: `aws.partner/newrelic.com/1234567/source_name`
- Copia la prima parte del Partner Event Bus o del codice sorgente da inserire `PartnerEventBusPrefixParameter` durante la distribuzione del CloudFormation modello.
  - Un esempio per New Relic è `aws.partner/newrelic.com`

2. Scarica e modifica il CloudFormation modello.
   - `TransformLambdaFunction`Individua il file nel modello
   - È `def lambda_handler(event, context)` `event["detail"]["incident-detection-response-identifier"]` impostato sul percorso json in cui il nome dell'allarme appare nel payload JSON dell'allarme APM. Ogni APM avrà un percorso diverso. Di seguito sono riportati alcuni esempi, tuttavia i payload specifici potrebbero differire.
     - Esempio di New Relic:. `event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"]`
     - Esempio Datadog: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]`
     - Esempio Splunk: `event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]`
   - Salva il CloudFormation modello.

Distribuzione del CloudFormation modello:

1. Apri la CloudFormation console nell'account e nella regione di destinazione.
2. Scegli Crea stack, Con nuove risorse (standard)
   - Seleziona Scegli un modello esistente, Carica un file modello, Scegli file, quindi carica il CloudFormation modello che hai salvato localmente.
3. Specificate i dettagli dello stack:
   - Inserisci un nome per lo stack (esempio:`NewRelicIntegrationForIDR`).
   - Specificate i valori dei parametri ottenuti durante il completamento dei prerequisiti.
     - APMNameParameter(Esempio:`NewRelic`)

    - PartnerEventBusNameParameter(Esempio:`aws.partner/newrelic.com/1234567/source_name`)
    - PartnerEventBusPrefixParameter(Esempio:`aws.partner/newrelic.com`)
  - Scegli Next (Successivo).
4. Configura le opzioni dello stack:
  - Scorri fino alla fine della pagina e seleziona la casella per consentire la creazione CloudFormation di risorse IAM con nomi personalizzati.
5. Revisione e creazione:
  - Verifica che i valori dei parametri siano configurati correttamente e scegli Invia.
6. Lo CloudFormation stack distribuisce le risorse necessarie per integrare gli eventi APM in AWS Incident Detection and Response. Attendi che venga visualizzato lo stato dello stack. `CREATE_COMPLETE`
7. Lo CloudFormation stack crea le seguenti risorse, supponendo che i valori di esempio siano stati inseriti nei parametri di New Relic e siano stati eseguiti nella regione. US-EAST-1
  - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
  - EventBridgeRule: leggi. partner/newrelic. com/1234567/nome_fonte | NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
  - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
  - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
  - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission - [stringa_casuale]

Test di integrazione

Dopo aver distribuito lo stack, verifica l'integrazione inviando un payload di test dal tuo APM:

1. Vai alla console Lambda e seleziona la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` funzione. Selezionare la scheda Monitor (Monitora).
2. Cerca una chiamata riuscita nei grafici metrici.
3. Scegli Visualizza Amazon CloudWatch Logs per verificare la presenza di eventuali errori nei flussi di log del payload di test.

Condivisione dell'ARN del tuo Event Bus con AWS Incident Detection and Response

1. Apri la EventBridge console Amazon. Seleziona Event bus.
2. Copia l'ARN del bus di eventi personalizzato creato come parte dello CloudFormation stack, (esempio:.) `arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`
   - Aggiungi questo ARN al campo "EventBridge Event Bus ARN» nella sezione "Third-Party APM Alarms» del tuo. Questionario sull'ingestione degli allarmi - Panoramica
3. Durante il processo di onboarding, AWS Incident Detection and Response crea una EventBridge regola gestita su questo bus di eventi personalizzato per inserire gli allarmi APM.

Opzione 2: integrazione manuale

Completa i seguenti passaggi per ogni AWS account e AWS regione da cui AWS Incident Detection and Response deve importare gli allarmi. AWS Incident Detection and Response consiglia di impostare gli allarmi nello stesso AWS account e nella stessa regione delle risorse dell'applicazione per velocizzare l'identificazione e l'analisi delle risorse interessate. Gli incidenti e i casi di supporto vengono aperti sull' AWS account da cui è stato ricevuto l'avviso APM.

1. Crea un bus di eventi EventBridge partner configurando il tuo APM come fonte di eventi per EventBridge partner Amazon (ad esempio,`aws.partner/apm_name/integrationName`). Per linee guida sulla configurazione del tuo APM come fonte di eventi, consulta Ricezione di eventi da un partner SaaS con Amazon. EventBridge
2. Effettua una delle seguenti operazioni:
   - (Consigliato) Crea un bus di eventi EventBridge personalizzato denominato. `$YourApmName-AWSIncidentDetectionResponse-EventBus`
   - (Alternativa) Utilizzate il bus EventBridge eventi predefinito anziché un bus eventi personalizzato.

   AWS Incident Detection and Response installerà una regola gestita (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sul bus di eventi personalizzato o predefinito tramite `AWSServiceRoleForHealth_EventProcessor` SLR. L'origine della regola sarà il bus degli eventi personalizzato o predefinito, la destinazione della regola sarà AWS Incident Detection and Response e la regola corrisponderà allo schema per l'acquisizione di eventi APM di terze parti.

3. Crea una funzione Lambda denominata `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` per trasformare gli eventi del bus degli eventi partner. Gli eventi trasformati corrisponderanno alla regola `AWSHealthEventProcessorEventSource-DO-NOT-DELETE` gestita.
   - Gli eventi trasformati includono un identificatore AWS Incident Detection and Response univoco e impostano l'origine e il tipo di dettaglio dell'evento sui valori richiesti. Ciò consente alla struttura di payload JSON trasformata di corrispondere al modello di regole gestite.
   - Imposta la destinazione della funzione Lambda sul bus eventi personalizzato (consigliato) creato nel passaggio 2 o sul bus eventi predefinito.
4. Crea una EventBridge regola e definisci i modelli di eventi che corrispondono all'elenco di eventi che desideri inviare ad AWS Incident Detection and Response. L'origine della regola è il bus degli eventi partner che hai creato nella Fase 1 (`aws.partner/apm_name/integrationName`). L'obiettivo della regola è la funzione Lambda creata nel passaggio 3 ()`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`. Per linee guida sulla definizione della EventBridge regola, consulta EventBridge le regole di Amazon.

Per un esempio dettagliato su come configurare manualmente le integrazioni dei bus degli eventi dei partner con AWS Incident Detection and Response, consulta Integrazione delle notifiche da Datadog e Splunk.

Inserisci allarmi dagli APM senza integrazione diretta con EventBridge

AWS Incident Detection and Response supporta l'utilizzo di webhook per l'inserimento di allarmi da APM di terze parti che non hanno un'integrazione diretta con Amazon. EventBridge

Puoi distribuire un CloudFormation modello o configurare manualmente l'integrazione. Prima di configurare l'integrazione, verifica che il ruolo AWS collegato al servizio (SLR) sia stato creato nei `AWSServiceRoleForHealth_EventProcessor` tuoi account.

Opzione 1: Utilizzo CloudFormation Modello

È disponibile un CloudFormation modello per semplificare il processo di creazione dell'infrastruttura di integrazione necessaria per importare allarmi in AWS Incident Detection and Response dal tuo APM che non dispone dell'integrazione diretta con Amazon. EventBridge

Considerazioni prima di distribuire questo modello CloudFormation

- Questa soluzione utilizza un API Gateway Lambda Authorizer per confrontare un token segreto passato nel payload dall'APM con un token in ingresso. Gestione dei segreti AWS Se il token non corrisponde, verrà restituita una policy con un rifiuto esplicito. Per ulteriori informazioni, consulta Autorizzatori Lambda.
- Nell'ambito del modello di responsabilità AWS condivisa, è tua responsabilità assicurarti di utilizzare un approccio di autenticazione che soddisfi i requisiti di sicurezza della tua organizzazione. Ti consigliamo di utilizzare Gestione dei segreti AWS un servizio simile, invece di archiviare informazioni sensibili come chiavi API o token di autorizzazione come variabili codificate. Per ulteriori informazioni, consulta Creazione e gestione di segreti con Gestione dei segreti AWS.
- Per un ulteriore esempio di implementazione del Hash-Based Message Authentication Code (HMAC), consulta receive-webhooks nella pagina Github di aws-samples. Per ulteriori informazioni sull'implementazione dell'autorizzazione tramite token, consulta l'esempio della funzione Lambda dell'autorizzazione TOKEN dalla documentazione di API Gateway.
- La soluzione utilizza RateLimitBurstLimit, e Quota in API Gateway per controllare i volumi delle richieste. Questi strumenti limitano il numero di richieste che possono essere elaborate in un determinato periodo di tempo. Questo aiuta a prevenire il sovraccarico del sistema e mantiene stabile il servizio. Per ulteriori informazioni sulla limitazione, consulta l'API Gateway Developer Guide.
- Prendi in considerazione l'utilizzo di AWS Web Application Firewall (WAF) per proteggere l'API Gateway da noti indirizzi IP errati. Ciò riduce il rischio che gli aggressori inondino l'API con richieste false che potrebbero bloccare eventi di registro reali.
- Gestione dei segreti AWS i valori dei token devono essere archiviati nello strumento Apm (Application Performance Monitoring) come intestazione HTTP. Assicurati di ruotare il token regolarmente come best practice di sicurezza.
- Verranno sostenuti costi aggiuntivi per le risorse distribuite tramite questo CloudFormation modello (ad esempio: Lambda e). EventBridge Per ulteriori informazioni sui prezzi di questi servizi, consulta la sezione Prezzi.AWS
- Dopo aver testato l'integrazione, rimuovi le istruzioni logger.info () dalla (funzione `TransformLambdaFunction` Lambda) per evitare che i payload vengano visualizzati in Amazon Logs. CloudWatch
- Implementa questo CloudFormation modello in ogni AWS account e regione da cui AWS Incident Detection and Response deve importare allarmi.

Preparazione del modello: CloudFormation

Nota: le fasi di integrazione utilizzano Dynatrace come esempio, tuttavia questo modello può essere utilizzato per qualsiasi APM in grado di inviare payload a un API Gateway.

1. Scarica e apri il modello.CloudFormation
2. `APIGWUsagePlan`Individua nel modello. Rivedi i valori configurati per `RateLimitBurstLimit`, e `Quota Limit` che sono impostati su 20, 50 e 2000 per impostazione predefinita. Modifica i valori per soddisfare le tue esigenze.
3. `AuthorizerLambdaFunction`Individua nel modello. Questa funzione Lambda funge da esempio di meccanismo di autenticazione. Estrae un valore token da un'intestazione chiamata`authorizationToken`, che viene passata dall'APM. Puoi modificare questo codice per allinearlo alle politiche di sicurezza e ai requisiti APM della tua organizzazione.
4. Individualo `TransformLambdaFunction` nel modello. Sostituisci il percorso del dizionario con il percorso del nome dell'allarme inviato nel payload JSON dal tuo APM. `raw_json["detail"]["ProblemTitle"]` Lascialo così com'è per Dynatrace.

Distribuzione del modello: CloudFormation

1. Apri la CloudFormation console nel tuo account di destinazione e Regione AWS.
2. Scegli Crea stack, Con nuove risorse (standard).
   - Seleziona Scegli un modello esistente, Carica un file modello, Scegli file, quindi carica il CloudFormation modello che hai salvato localmente.
3. Specificate i dettagli dello stack:
   - Immettete il nome di uno stack (esempio, *`DynatraceIntegrationForIDR`*.)
   - APMNameParameter (esempio, *`Dynatrace`*.)
   - Scegli Next (Successivo).
4. Configura le opzioni dello stack:
   - Scorri fino alla fine della pagina e seleziona la casella per consentire la creazione CloudFormation di risorse IAM con nomi personalizzati.
5. Revisione e creazione:
   - Verifica che i valori dei parametri siano configurati correttamente e scegli Invia.
6. Lo CloudFormation stack distribuisce le risorse necessarie per integrare gli eventi APM in AWS Incident Detection and Response. Attendi che lo stato dello CloudFormation stack sia CREATE_COMPLETE.

7. Lo CloudFormation stack crea le seguenti risorse presupponendo che il valore di esempio sia `Dynatrace` stato inserito nei parametri ed eseguito nella regione. US-EAST-1
   - Nome segreto: DynatraceMySecretTokenName (verrà creato un valore segreto casuale rispetto alla chiave segreta) APMSecureToken
   - Risorse API Gateway:
     - Nome API: Dynatrace-AWSIncidentDetectionResponse-APIGW
     - Nome fase: Dynatrace-Stage-Prod
     - Autorizzatori: Dynatrace-APIGW-Authorizer
     - Piano di utilizzo: APIGW_ Throttling_Plan
   - Funzioni Lambda:
     - Funzione di autorizzazione: Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - Funzione di trasformazione: Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - EventBus Nome personalizzato: Dynatrace-AWSIncidentDetectionResponse-EventBus
   - Ruolo IAM:
     - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
     - AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1
8. Registra l'URL del Webhook e il valore del token:
   - Apri la console API Gateway e scegli il nome API creato come parte dello CloudFormation stack.
   - Scegli Stages dalla barra di navigazione a sinistra, espandi il nome dello stage usando il segno +, quindi scegli POST. Registra l'URL di Invoke. Configura questo URL nel tuo APM come destinazione per inviare webhook per eventi di allarme.
   - Apri la Gestione dei segreti AWS console e scegli il nome segreto creato come parte dello stack. CloudFormation (Esempio: DynatraceMySecretTokenName.)
     - Nella scheda Valore segreto, scegli Recupera valore segreto. Vedrai la chiave segreta come APMSecureToken. Registra il valore segreto. Non condividere questo valore segreto con nessuno.

Test di integrazione

Dopo aver distribuito lo stack, verifica l'integrazione inviando un payload di test dal tuo APM:

1. Vai alla console Lambda e seleziona `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` la funzione. Selezionare la scheda Monitor (Monitora).
2. Cerca una chiamata riuscita nei grafici metrici.
3. Scegli Visualizza Amazon CloudWatch Logs per verificare la presenza di eventuali errori nei flussi di log del payload di test.

Condivisione dell'ARN del tuo Event Bus con AWS Incident Detection and Response

1. Apri la EventBridge console Amazon. Seleziona Event bus.
2. Copia l'ARN del bus di eventi personalizzato creato come parte dello CloudFormation stack, esempio:. *`arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`*
   - Aggiungi questo ARN al campo "EventBridge Event Bus ARN» nella sezione "Third-Party APM Alarms» del tuo. Questionario sull'ingestione degli allarmi - Panoramica
3. Durante il processo di onboarding, AWS Incident Detection and Response creerà una EventBridge regola gestita su questo bus di eventi personalizzato per inserire gli allarmi APM.

Opzione 2: integrazione manuale

Utilizza i seguenti passaggi per configurare l'integrazione con AWS Incident Detection and Response.

1. Crea un Amazon API Gateway per accettare il payload dal tuo APM.
2. Definisci una funzione Lambda per l'autorizzazione utilizzando un token di autenticazione.
3. Effettua una delle seguenti operazioni:
   - (Consigliato) Crea un bus di eventi EventBridge personalizzato denominato`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternativa) Utilizzate il bus EventBridge eventi predefinito anziché un bus eventi personalizzato.
4. Definisci una funzione Transform Lambda per aggiungere l'identificatore AWS Incident Detection and Response al tuo payload. Puoi anche utilizzare questa funzione per filtrare gli eventi che desideri inviare ad AWS Incident Detection and Response.

- L'API Gateway deve richiamare la funzione Transform Lambda che trasformerà il payload passato dall'API Gateway.
- La funzione Transform Lambda deve scrivere eventi trasformati nel bus degli eventi definito al precedente punto 3.

5. Configura il tuo APM per inviare notifiche all'URL generato dall'API Gateway.

Inserisci allarmi dagli APM con integrazione diretta con Amazon SNS

Se il tuo APM supporta l'invio di allarmi ad argomenti di Amazon SNS, puoi seguire questa guida per inserire i tuoi allarmi APM in AWS Incident Detection and Response.

Puoi distribuire il CloudFormation modello fornito o configurare manualmente questa integrazione. Prima di configurare l'integrazione, verifica che il ruolo AWS collegato al servizio (SLR) sia stato creato nei `AWSServiceRoleForHealth_EventProcessor` tuoi account.

Opzione 1: Utilizzo CloudFormation

È disponibile un CloudFormation modello per semplificare il processo di creazione dell'infrastruttura di integrazione necessaria per importare allarmi in AWS Incident Detection and Response dal tuo APM con l'integrazione di Amazon SNS.

> **Note**
>
> - Verranno sostenuti costi aggiuntivi per le risorse distribuite tramite questo CloudFormation modello (ad esempio: Lambda e). EventBridge Per ulteriori informazioni sui prezzi di questi servizi, consulta la sezione Prezzi.AWS
> - Questo CloudFormation modello deve essere distribuito in ogni AWS account e regione da cui AWS Incident Detection and Response deve importare gli allarmi.
> - Gli esempi forniti in questo documento si riferiscono a Grafana, tuttavia questo modello può essere utilizzato per qualsiasi APM che abbia un'integrazione diretta con Amazon Simple Notification Service.
> - Per motivi di sicurezza, AWS consiglia di rimuovere `logger.info()` le istruzioni da `TransformLambdaFunction` per evitare che il payload venga registrato in Amazon CloudWatch Logs.

Prerequisiti per la distribuzione di questo modello: CloudFormation

- È necessario creare un argomento Amazon Simple Notification Service standard per ricevere eventi di allarme dal tuo APM. Crea un argomento SNS nella console di Amazon Simple Notification Service.
- Il `TransformLambdaFunction` contenuto del modello deve essere modificato per `["detail"]["incident-detection-response-identifier"]` impostarlo sul valore desiderato in base all'APM utilizzato.

Completamento dei prerequisiti:

1. Apri la console Amazon SNS, quindi seleziona Argomenti. Copia l'ARN dell'argomento Standard Amazon SNS creato per ricevere eventi di allarme dal tuo APM.
   - Ad esempio: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. Scarica e apri il modello CloudFormation
   - `TransformLambdaFunction`Individua il file nel modello
     - Sotto `def lambda_handler(event, context)` `event["detail"]["incident-detection-response-identifier"]` impostato sul percorso json in cui appare il nome dell'allarme nel payload JSON del record SNS.
       - Qualsiasi evento inviato `TransformLambdaFunction` tramite SNS ha una struttura di payload principale come. `event["Records"][n]["Sns"]["Message"]` L'effettiva origine del payload dalla sorgente (APM) è racchiusa all'interno della struttura principale.
       - Esempio per Grafana: `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

Distribuzione del modello CloudFormation :

1. Accedi alla CloudFormation console nell'account e nella regione in cui devi configurare l'integrazione.
2. Vai a CloudFormation.
   - Scegli Crea stack, Con nuove risorse (standard)
     - Seleziona Scegli un modello esistente, Carica un file modello, Scegli file, quindi carica il CloudFormation modello che hai salvato localmente.
3. Specificate i dettagli dello stack:
   - Inserisci il nome di uno stack Esempio: `<your-apm-name>IntegrationForIDR`

- Specificare i valori dei parametri ottenuti durante il completamento dei prerequisiti
  - APMNameParameterEsempio: `Grafana`
  - Esempio di parametro TriggerSNS: `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
- Scegli Next (Successivo).

4. Configura le opzioni dello stack:
   - Scorri fino alla fine della pagina e conferma la casella di controllo per consentire la creazione CloudFormation di risorse IAM con nomi personalizzati.
5. Revisione e creazione:
   - Verifica che i valori dei parametri siano configurati correttamente, quindi scegli Invia.
6. Lo CloudFormation stack distribuirà le risorse necessarie per integrare gli eventi APM in AWS Incident Detection and Response. Attendi che lo stato dello CloudFormation stack sia CREATE_COMPLETE.
7. Lo CloudFormation stack crea le seguenti risorse supponendo che i valori di esempio siano stati inseriti nei parametri di Grafana e siano stati eseguiti nella Regione. EU-WEST-1
   - CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
   - Abbonamento SNS: arn:aws:sns:eu-west- 1:012345678912:grafana-sns: [random_string]
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-eu-west-1
   - TransformLambdaFunction: Grafana-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission GrafanaIntegrationForIDR-TransformLambdaPermission: - [stringa_casuale]

Test di integrazione

Dopo che lo CloudFormation stack è stato distribuito correttamente, puoi convalidare l'integrazione inviando un payload di test dal tuo APM. Una volta inviato il payload di test dal tuo APM:

1. Vai alla console Lambda e seleziona la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` funzione. Quindi, scegli la scheda Monitor.
2. Una chiamata riuscita deve essere osservata nei grafici metrici.

3. Seleziona Visualizza Amazon CloudWatch Logs. Puoi verificare dagli eventi di registro nei flussi di log per confermare che il payload di test inviato dal tuo APM sia presente o se sono stati riscontrati errori.

Condivisione dell'ARN del tuo Event Bus con AWS Incident Detection and Response

1. Accedi alla EventBridge console Amazon. Seleziona Event bus.
2. Registra l'ARN del bus di eventi personalizzato distribuito come parte dello CloudFormation stack, ad esempio:. `arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`
   - Fornisci l'ARN di questo bus di eventi personalizzato a AWS Incident Detection and Response nel campo "EventBridge Event Bus ARN» della sezione "Third-Party APM Alarms» del. Questionario sull'ingestione degli allarmi - Panoramica
3. Durante il processo di onboarding, AWS Incident Detection and Response creerà una EventBridge regola gestita su questo bus di eventi personalizzato per inserire gli allarmi APM.

Opzione 2: integrazione manuale

1. Apri la console Amazon SNS e crea un argomento Amazon SNS standard `[apm_name]-sns` denominato per ricevere eventi di allarme dal tuo APM. Assicurati di selezionare Standard (non FIFO) come tipo di argomento. Nota l'ARN dell'argomento Amazon SNS creato.
2. Effettua una delle seguenti operazioni:
   - (Consigliato) Crea un bus di eventi EventBridge personalizzato denominato. `[apm_name]-AWSIncidentDetectionResponse-EventBus`
   - (Alternativa) Utilizzate il bus EventBridge eventi predefinito anziché un bus eventi personalizzato.

   AWS Incident Detection and Response installerà una regola gestita (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sul bus di eventi personalizzato o predefinito tramite `AWSServiceRoleForHealth_EventProcessor` SLR. L'origine della regola sarà il bus degli eventi personalizzato o predefinito, la destinazione della regola sarà AWS Incident Detection and Response e la regola corrisponderà allo schema per l'acquisizione di eventi APM di terze parti.

3. Crea una funzione Lambda denominata `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` per trasformare i tuoi payload SNS.
   - Gli eventi trasformati devono soddisfare i requisiti di payload indicati in Requisiti di payload per l'acquisizione di avvisi APM con EventBridge
   - Imposta la destinazione della funzione Lambda sul bus eventi personalizzato (consigliato) creato nel passaggio 2 o sul bus eventi predefinito.
4. Imposta l'argomento SNS come trigger per la tua funzione `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` Lambda.
   - Nella pagina «Aggiungi trigger», cerca «SNS».
   - Aggiungi l'ARN del tuo argomento SNS dedicato creato nel passaggio 1.
   - Scegli «Aggiungi».
5. Segui la documentazione APM per configurare una destinazione SNS per i tuoi payload APM che devono essere acquisiti da AWS Incident Detection and Response.

AWS Incident Detection and Response installerà una regola gestita (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sul bus di eventi personalizzato o predefinito tramite `AWSServiceRoleForHealth_EventProcessor` SLR. L'origine della regola sarà il bus degli eventi personalizzato o predefinito, la destinazione della regola sarà AWS Incident Detection and Response e la regola corrisponderà allo schema per l'acquisizione di eventi APM di terze parti.

Ottimizzazione degli allarmi e regolazioni del monitoraggio

Per garantire un'accuratezza ottimale del rilevamento degli incidenti, i nostri ingegneri della gestione degli incidenti valutano continuamente le prestazioni degli allarmi rispetto ai carichi di lavoro critici. Forniamo le modifiche consigliate alla configurazione degli allarmi, che siete tenuti ad apportare, e collaboriamo in modo proattivo con voi e i vostri Technical Account Manager (TAM) per perfezionare queste impostazioni.

Quando i dati di monitoraggio indicano che gli allarmi potrebbero non essere allineati con le operazioni aziendali critiche, ad esempio quando gli avvisi si attivano senza il corrispondente impatto sul cliente o quando gli stati degli allarmi fluttuano frequentemente, consigliamo di eliminare gli allarmi non critici e gli allarmi di onboarding che riflettono meglio l'impatto del carico di lavoro critico. Questo aiuta a mantenere l'efficacia complessiva della copertura della risposta agli incidenti.

Revisione e feedback degli allarmi

AWS Incident Detection and Response effettua revisioni complete degli allarmi prima di attivarli per il monitoraggio. Gli allarmi vengono valutati sulla base di criteri tecnici di accettazione, tra cui parametri di configurazione, qualità dei dati ed efficacia degli avvisi.

Sulla base di questa recensione, vengono forniti due tipi di feedback:

- Requisiti di configurazione obbligatori: queste modifiche devono essere implementate per l'accettazione degli allarmi.
- Raccomandazioni di miglioramento opzionali: queste modifiche migliorano l'efficacia degli allarmi ma non sono obbligatorie per l'accettazione degli allarmi.

Dopo aver ricevuto questo feedback, puoi decidere di procedere solo all'onboarding degli allarmi accettati e di quelli che necessitano di miglioramenti opzionali, lavorando parallelamente alle modifiche alla configurazione degli allarmi con requisiti di configurazione obbligatori.

In alternativa, puoi implementare tutte le modifiche prima della pubblicazione. Questo approccio estende la tempistica di onboarding, in base al numero di allarmi che richiedono regolazioni.

Gli allarmi diventano attivi

Al termine dell'inserimento degli allarmi, AWS Incident Detection and Response consente il monitoraggio del carico di lavoro. Da questo momento in poi, gli allarmi integrati vengono monitorati attivamente e AWS Incident Detection and Response ti coinvolge in base al runbook del carico di lavoro quando gli allarmi integrati entrano nello stato ALARM.

Uscite chiave

- Il carico di lavoro viene confermato come attivo e monitorato da AWS Incident Detection and Response.

Fasi successive

- Per verificare che gli allarmi integrati utilizzino AWS Incident Detection and Response come previsto, consulta. Testa i carichi di lavoro integrati in Incident Detection and Response
- Per apportare modifiche agli allarmi integrati, al runbook o alle informazioni sul carico di lavoro, consulta. Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response

Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response (percorso di eccezione)

> **Note**
>
> Se non riesci a utilizzare la CLI IDR per l'onboarding del tuo carico di lavoro, utilizza i seguenti questionari per l'onboarding del carico di lavoro e degli allarmi.

Questo argomento fornisce i questionari da completare durante l'onboarding di un carico di lavoro in AWS Incident Detection and Response e durante la configurazione degli allarmi da inserire nel servizio. Il questionario di onboarding del carico di lavoro contiene informazioni generali sul carico di lavoro, i dettagli dell'architettura e i contatti per la risposta agli incidenti. Nel questionario di inserimento degli allarmi, specifichi gli allarmi critici che innescano la creazione di incidenti in Incident Detection and Response per il tuo carico di lavoro, oltre a fornire informazioni sul runbook su chi contattare e quali azioni intraprendere. La corretta compilazione di questi questionari è un passaggio fondamentale nella configurazione dei processi di monitoraggio e risposta agli incidenti per i carichi di lavoro. AWS

Scarica il questionario di onboarding sul carico di lavoro:

- Versione inglese
- Versione giapponese

Scarica il questionario sull'ingestione degli allarmi:

- Versione inglese
- Versione giapponese

Questionario di onboarding sul carico di lavoro - Domande generali

Domande generali

Domanda	Risposta di esempio
Nome dell'azienda	Amazon Inc.

Domanda	Risposta di esempio
Nome di questo carico di lavoro (includi eventuali abbreviazioni)	Amazon Retail Operations (ARO)
Utente finale principale e funzione di questo carico di lavoro.	Questo carico di lavoro è un'applicazione di e-commerce che consente agli utenti finali di acquistare vari articoli. Questo carico di lavoro è il principale generatore di entrate per la nostra attività.

Questionario sull'onboarding del carico di lavoro - Domande sull'architettura

Domande sull'architettura

Domanda	Risposta di esempio
Un elenco di tag di AWS risorsa utilizzati per definire le risorse che fanno parte di questo carico di lavoro. AWS utilizza questi tag per identificare le risorse di questo carico di lavoro e velocizzare il supporto durante gli incidenti. **Note** I tag rispettano la distinzione tra maiuscole e minuscole. Se fornisci più tag, tutte le risorse utilizzate da questo carico di lavoro devono avere gli stessi tag.	Nome app: Optimax ambiente: Produzione
Un elenco degli Servizio AWS elementi utilizzati da questo carico di lavoro, con l' Account AWS indicazione degli elementi Regione AWS in cui si trovano.	Servizi AWS: Route 53, ALB, ECS,... Conti: 123456789101, 123456789102,... US-EAST-1Regioni: US-WEST-2,,...

Questionario sull'ingestione degli allarmi - Panoramica

Nel questionario di inserimento degli allarmi, specifichi gli allarmi critici per il carico di lavoro che desideri coinvolgere AWS Incident Detection and Response, nonché i contatti che desideri che un Incident Management Engineer coinvolga quando questi allarmi si attivano.

L'Alarm Ingestion Questionnaire è suddiviso nelle seguenti sezioni:

- Sezione Contatti: per prima cosa, specifica il/i contatto/i primario/i da includere nel Supporto caso creato con AWS Incident Detection and Response quando si attiva un allarme, nonché la tua applicazione di conferenza preferita per i ponti incidenti. Se non viene fornita alcuna preferenza per il bridge, AWS Incident Detection and Response creerà un incident bridge durante gli incidenti. Successivamente, specifica i contatti di riferimento e gli intervalli di tempo per coinvolgerli quando i contatti principali non sono raggiungibili. Infine, elenca tutti i contatti che dovrebbero ricevere aggiornamenti regolari sullo stato degli incidenti tramite la richiesta di assistenza per tutta la durata dell'incidente.
- Matrice degli allarmi: elenca il set di allarmi che attiveranno AWS Incident Detection and Response quando vengono attivati. Consulta i «Criteri di allarme critici» definiti da AWS Incident Detection and Response quando selezioni gli allarmi per l'onboarding. Per ulteriori informazioni, consulta Definizione di allarme.
  - Amazon CloudWatch Alarms (lascia vuota questa sezione se non disponi di CloudWatch allarmi Amazon)
  - Allarmi APM di terze parti (lascia vuota questa sezione se non disponi di allarmi APM di terze parti)
    - EventBridge EventBus ARN: è l'ARN dell'ARN personalizzato che hai creato in o EventBus . Inserisci allarmi dagli APM con integrazione diretta EventBridge Inserisci allarmi dagli APM senza integrazione diretta con EventBridge
    - Identificatori di allarme: condividi il numero di account, la regione e il nome dell'allarme APM.

Questionario sull'ingestione degli allarmi - Domande del runbook

Domande sul runbook

Domanda	Risposta di esempio
AWS coinvolge i contatti del carico di lavoro attraverso il caso. Supporto Chi è il contatto principale quando si attiva un allarme per questo carico di lavoro? Specificate la vostra applicazione di conferenz a preferita e AWS richiederete questi dettagli durante un incidente. **Note** Se non viene fornita un'applicazione di conferenza preferita, ti AWS contatter à durante un incidente e ti fornirà un bridge Chime a cui unirti.	Team di candidatura app@example.com +61 2 3456 7890
Se il contatto principale non è disponibi le durante un incidente, fornisci i contatti di riferimento e la tempistica nell'ordine di comunicazione preferito.	1. Dopo 10 minuti, se il contatto principale non risponde, contatta: John Smith - Supervisore delle applicazioni john.smith@example.com +61 2 3456 7890 2. Dopo 10 minuti, se John Smith non risponde, contatta: Jane Smith - Responsabile delle operazioni jane.smith@example.com +61 2 3456 7890

Matrice di allarme

Fornisci le seguenti informazioni per identificare il set di allarmi che utilizzeranno AWS Incident Detection and Response per creare incidenti per conto del tuo carico di lavoro. Una volta che gli ingegneri di AWS Incident Detection and Response avranno esaminato i tuoi allarmi, verranno fornite ulteriori fasi di onboarding.

Criteri di allarme critici di AWS per il rilevamento e la risposta agli incidenti:

- Gli allarmi AWS Incident Detection and Response devono entrare nello stato «Allarme» solo in caso di impatto aziendale significativo sul carico di lavoro monitorato (perdita dell'esperienza del revenue/degraded cliente) che richiede l'attenzione immediata dell'operatore.
- Gli allarmi AWS Incident Detection and Response devono inoltre coinvolgere i resolver per il carico di lavoro contemporaneamente o prima dell'intervento. AWS Gli Incident Manager collaborano con i tuoi resolver nel processo di mitigazione e non fungono da soccorritori di prima linea che poi si rivolgono a te.
- Le soglie di allarme AWS Incident Detection and Response devono essere impostate su una soglia e una durata appropriate in modo che ogni volta che viene attivato un allarme debba aver luogo un'indagine. Se un allarme passa dallo stato «Alarm» a «OK», si verifica un impatto sufficiente a giustificare la risposta e l'attenzione dell'operatore.

Policy di AWS Incident Detection and Response per le violazioni dei criteri:

Questi criteri possono essere valutati solo caso per caso al verificarsi degli eventi. Il team di gestione degli incidenti collabora con i responsabili tecnici degli account (TAM) per regolare gli allarmi e, in rari casi, disabilita il monitoraggio se si sospetta che gli allarmi dei clienti non rispettino questi criteri e coinvolga regolarmente il team di gestione degli incidenti inutilmente.

> **Important**
>
> Quando fornisci gli indirizzi di contatto, fornisci un gruppo di indirizzi e-mail di distribuzione, in modo da poter controllare le aggiunte e le eliminazioni dei destinatari senza dover aggiornare i runbook.
> Fornisci il numero di telefono di contatto del tuo team di ingegneria dell'affidabilità del sito (SRE) se desideri che il team di AWS Incident Detection and Response li chiami dopo aver inviato un'e-mail di coinvolgimento iniziale.

Tabella delle matrici di allarme per gli CloudWatch allarmi

CloudWatch allarme ARN	Contatto principale per questo allarme. (Se diverso dal contatto principale del carico di lavoro)	Specificate il più pertinent e Servizio AWS per questo allarme per coinvolgere il tecnico giusto. Inserisci N/A se non necessario.
Esempio: `arn:aws:cloudwatch:us-east-1:123456789012:alarm:ALB_5xx_Target_Response`	Esempio: Sam Smith - Gestore delle applicazioni sam.smith@example.com +61 2 3456 7890	Esempio: ECS

Tabella delle matrici di allarme per allarmi APM di terze parti

EventBridge Event Bus ARN
 	
(Questo è stato creato come parte dell'integrazione APM di terze parti per indirizzare gli avvisi verso AWS Incident Detection and Response).
	Esempio: (Ci sarà un bus di eventi per combinazione) Account/Region
	
	`arn:aws:events:us-east-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`
	
	`arn:aws:events:us-west-1:123456789012:event-bus/APMName-AWSIncidentDetectionResponse-EventBus`

Identificatore di allarme	Cosa rappresenta questa metrica? Perché questo allarme è importante?	Contatto principale per questo allarme. (Se diverso dal contatto principale del carico di lavoro)	Specificate il più pertinente Servizio AWS per questo allarme per coinvolgere il tecnico giusto.

			Inserisci N/A se non necessario.
Esempio: ALB_5xx_ Target_Response ID dell'account: 123456789012 Regione: us-east-1	Esempio: Questa metrica rappresenta le risposte alle transazioni provenienti dai target alla base dell'ALB. Se gli errori 5XX superano la soglia, rappresenta un errore critico nell'elaborazione delle transazioni commerciali.	Esempio: Sam Smith - Gestore delle applicazioni sam.smith@example.com +61 2 3456 7890	Esempio: ECS

Gestisci i carichi di lavoro nel rilevamento e nella risposta agli incidenti

Un elemento fondamentale per una gestione efficace degli incidenti è disporre dei processi e delle procedure corretti per l'onboarding, il test e la manutenzione dei carichi di lavoro monitorati. Questa sezione descrive i passaggi essenziali, tra cui lo sviluppo di runbook e piani di risposta completi per guidare i team negli incidenti, il test e la convalida approfonditi di nuovi carichi di lavoro, la richiesta di modifiche per aggiornare il monitoraggio dei carichi di lavoro e l'offboarding corretto dei carichi di lavoro quando necessario.

Argomenti

Sviluppa runbook e piani di risposta per rispondere a un incidente in Incident Detection and Response

AWS Incident Detection and Response utilizza le informazioni acquisite dall'onboarding della CLI IDR per sviluppare runbook per la gestione degli incidenti che influiscono sui carichi di lavoro. I runbook documentano i passaggi che gli Incident Manager intraprendono quando rispondono a un incidente. Un piano di risposta è mappato su almeno uno dei tuoi carichi di lavoro. Il team di gestione degli incidenti crea questi modelli sulla base delle informazioni fornite dall'utente durante l'onboarding del carico di lavoro.

Risultati chiave:

- Completamento della definizione del carico di lavoro su AWS Incident Detection and Response.
- Completamento di allarmi e runbook su AWS Incident Detection and Response.

Puoi anche scaricare un esempio di AWS Incident Detection and Response Runbook: aws-idr-runbook-example.zip.

Runbook di esempio

Example Runbook di esempio

Description

Questo documento è destinato a [CustomerName] - [WorkloadName].

Fase: Priorità

Azioni prioritarie

1. Invia la prima corrispondenza sul Supporto caso al cliente come indicato di seguito.

```
Hello,

This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has
 triggered for your workload <<Application_Name>>. I am currently investigating and
 will update you in a few minutes once I have finished initial investigation.

Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
```

Fase 2: Informazioni

Piani di coinvolgimento

Questa sezione descrive i piani di coinvolgimento applicabili a questo runbook e contiene solo i dettagli di contatto. I piani di coinvolgimento verranno indicati nei piani di comunicazione dettagliati.

- Impegno iniziale

  AWS Incident Detection and Response Team aggiunge gli indirizzi degli stakeholder dei clienti di seguito al Supporto caso. AWS gli stakeholder si rivolgono ad altri stakeholder che potrebbero aver bisogno di essere messi al corrente di eventuali problemi.

  - Stakeholder del cliente: customeremail1; customeremail2; mobile1
  - AWS Soggetti interessati: aws-idr-oncall@amazon.com; tam-team-email; ecc.

  - Contatti monouso: [Si tratta di contatti e-mail inclusi solo nella prima comunicazione. Rimuovi questi contatti dopo l'interruzione della prima comunicazione. Potrebbero trattarsi di indirizzi e-mail che cercano i clienti, ad esempio Pager-Duty, che non devono essere cercati per ogni corrispondenza. Aggiungi esplicitamente istruzioni nella sezione «Priorità», «Piani di comunicazione», su come utilizzarli solo se è disponibile l'opzione Contatti monouso.]
- Configurazione delle chiamate impreviste

  Indica se il cliente richiede AWS Incident Detection and Response per creare un bridge, se utilizza un bridge statico o se fornirà un bridge all'apertura di un incidente.

  (Scegli un'opzione in base alle preferenze del cliente)

  - AWS Incident Detection and Response crea un Amazon Chime/Zoom Bridge
  - Bridge statico fornito dal cliente
    - Numero della conferenza: **<** Insert Conference number **>**
  - Il cliente fornisce i dettagli del bridge per ogni incidente rispondendo alle comunicazioni inviate dal team AWS Incident Detection and Response.
  - Altro: specifica i dettagli.
- Inasprimento del coinvolgimento

  AWS Incident Detection and Response contatterà i seguenti contatti quando i contatti del piano di coinvolgimento iniziale non rispondono agli incidenti.

  Per ogni contatto di Escalation indica se deve essere aggiunto alla Supporto custodia, telefonato o entrambi.

  - Assicurati di aver chiamato il contatto di Initial Engagement, se applicabile, prima di procedere con l'escalation.
  - Primo contatto di escalation: [escalation EmailAddress #1]/[PhoneNumber] - Attendi XX minuti prima di passare a questo contatto.
    - [Aggiungi contatto a Case/Phone] questo contatto.
  - Secondo contatto di escalation: [escalation EmailAddress #2]/[PhoneNumber] - Attendi XX minuti prima di passare a questo contatto.
    - [Aggiungi contatto alla casa/telefono] questo contatto.
  - ecc.

Piani di comunicazione

Questa sezione descrive come gli ingegneri addetti alla gestione degli incidenti comunicano con le parti interessate designate al di fuori dei canali di chiamata e comunicazione degli incidenti.

- Piano di comunicazione d'impatto

  Questo piano viene avviato quando AWS Incident Detection and Response ha stabilito in fase di Triage che un avviso indica un potenziale impatto su un cliente.

  AWS Incident Detection and Response richiederà al cliente di unirsi al bridge predeterminato come indicato in Engagement plans - Incident call setup.

  (Scegline uno in base alla disponibilità o meno di One Time Only Contacts).

  1. Garantisci la partecipazione dei clienti ai piani di coinvolgimento: il coinvolgimento iniziale viene aggiunto al case CC.

  O

  1. Assicuratevi che i clienti interessati e i contatti occasionali previsti dai piani di coinvolgimento rientrino nell'ambito dei piani di coinvolgimento: il coinvolgimento iniziale viene aggiunto al case CC.
  2. Invia la notifica di coinvolgimento al cliente in base al seguente modello:

     (Scegline uno)

     Modello Impact - Amazon Chime Bridge

     ```
     The following alarm has engaged AWS Incident Detection and Response to an Incident
      bridge:
         Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
         Alarm State Change Reason - <insert_state_change_reason>
         Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
     Please join the Amazon Chime Bridge below so we can start the steps outlined in
      your Runbook:
         Amazon Chime Meeting ID: <insert_Meeting_ID_here>
         Link to Amazon Chime Bridge: <insert_Link_here>
         International dial-in numbers: https://chime.aws/dialinnumbers/
     ```

     Modello di impatto - Bridge fornito dal cliente

```
The following alarm has engaged AWS Incident Detection and Response:
    Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025 3:30 PM UTC>
Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
```

Modello di impatto - Customer Static Bridge

```
The following alarm has engaged AWS Incident Detection and Response to an Incident
 bridge:
    Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
Please join the Bridge below so we can start the steps outlined in your Runbook:
    Conference Number: <insert_conference_number>
    Conference URL: <insert_bridge_URL>
```

3. Imposta il caso su Intervento in sospeso del cliente.
4. RIMUOVI i contatti monouso dalla custodia dopo aver inviato la comunicazione Impact di cui sopra. (Se è disponibile l'opzione Contatti monouso).
5. Segui il piano Engagement Escalation come indicato sopra.
6. Se il cliente non risponde entro 30 minuti, disattivalo e continua a monitorare fino al ripristino dell'allarme.

- Piano di comunicazione senza impatto

Questo piano viene avviato quando viene ripristinato un allarme prima che il rilevamento e la risposta agli incidenti abbiano completato il triage iniziale.

1. Prima di inviare la notifica di assenza di impatto, verifica e quindi rimuovi i contatti dei clienti and/or aggiunti da Supporto Case CC in base ai contatti elencati nel piano Engagement plans - Initial Engagement Engagement plan.

   ["NON aggiungere contatti monouso."] (Applicabile se è disponibile l'opzione Contatti monouso).
2. Invia una notifica di assenza di coinvolgimento al cliente in base al modello seguente:

   Modello No Impact

```
AWS Incident Detection and Response received an alarm that has recovered for your
 workload.
    Alarm Identifier - <insert_CloudWatch_Alarm_ARN_or_APM_Response_Identifier>
    Alarm State Change Reason - <insert_state_change_reason>
    Alarm Start Time - <Example: 1 January 2025, 3:30 PM UTC>
    Alarm End Time - <Example: 1 January 2025, 3:35 PM UTC>
This may indicate a brief customer impact that is currently not ongoing.
If there is an ongoing impact to your workload, please let us know and we will
 engage to assist.
```

3. Inserisci il caso nella sezione Pending Customer Action.
4. Se il cliente non risponde entro 30 minuti, risolvi il caso.

Panoramica dell'architettura delle applicazioni

Questa sezione fornisce una panoramica dell' application/workload architettura per la conoscenza di Incident Management Engineer e Operations Engineer.

- AWS Account e regioni con servizi chiave: elenco di AWS account con regioni che supportano questa applicazione. Assiste gli ingegneri nella valutazione dell'infrastruttura sottostante che supporta l'applicazione.
  - 123456789012
    - US-EAST-1 - una breve descrizione, se del caso
      - Amazon EC2: breve descrizione a seconda dei casi
      - DynamoDB: descrizione breve, se del caso
      - ecc.
    - US-WEST-1 - una breve descrizione, se del caso
      - ecc.
  - un altro account
    - ecc.

Testa i carichi di lavoro integrati in Incident Detection and Response

Ingestione degli allarmiAl termine, AWS Incident Detection and Response abilita il monitoraggio del carico di lavoro e invia una Go-Live conferma. Il tuo carico di lavoro viene monitorato attivamente da questo momento in poi.

Il test degli allarmi verifica che gli allarmi integrati attivino AWS Incident Detection and Response come previsto, attivino i runbook appropriati e qualsiasi altra azione desiderata, come la creazione automatica di casi in auto, se selezionata durante l'inserimento degli allarmi.

I test sono facoltativi ma fortemente consigliati. Sei responsabile della convalida delle disposizioni di risposta prima che si verifichi un incidente reale.

Opzioni di test

AWS Incident Detection and Response offre due opzioni di test.

Opzione 1: pianificata GameDay (consigliata)

Una pianificazione GameDay è una simulazione end-to-end dal vivo di ciò che potrebbe accadere durante un incidente reale. AWS Incident Detection and Response segue i passaggi del runbook prescritti per fornirti informazioni su come potrebbe svolgersi un incidente reale. GameDay È un'opportunità per porre domande o perfezionare le istruzioni per migliorare il coinvolgimento.

Per pianificare un GameDay, completa i seguenti passaggi:

1. Invia una notifica ad AWS Incident Detection and Response con una data preferita e una finestra oraria di 1 ora, incluso il fuso orario. Fornisci almeno 48 ore di lead time.
2. Pianifica le risorse per GameDay, tra cui il tuo SRE/Ops team e i contatti per l'escalation.

GameDay programma:

1. Tu e AWS Incident Detection and Response partecipate alla chiamata.
2. Disabiliti le azioni di allarme, se applicabile.
3. È possibile impostare manualmente gli allarmi sullo stato ALARM utilizzando le istruzioni inCome testare i tuoi allarmi.

4. AWS Incident Detection and Response conferma la ricezione della notifica di allarme.
5. AWS Incident Detection and Response risponde all'allarme e si unisce al bridge prescritto nel runbook.
6. Tu e AWS Incident Detection and Response confermate il GameDay risultato.

Opzione 2: test degli allarmi offline

È possibile testare gli allarmi in modo indipendente in qualsiasi momento senza pianificare una chiamata. L'attivazione di un allarme attiva AWS Incident Detection and Response in base al runbook, proprio come si farebbe durante un incidente reale.

Per eseguire il test degli allarmi offline, completa i seguenti passaggi:

1. Per evitare azioni involontarie, disattiva qualsiasi azione di CloudWatch allarme di Amazon.
2. Attiva gli allarmi utilizzando le istruzioni contenute in. Come testare i tuoi allarmi
3. Entro 5 minuti, viene creato un caso di supporto per tuo conto e AWS Incident Detection and Response ti coinvolge come specificato nel runbook.
4. Informa l'Incident Manager che stai eseguendo un test di allarme offline.
5. L'Incident Manager conferma quali modifiche dello stato di allarme sono state ricevute e convalida le disposizioni di risposta.

Se non viene creato un caso di supporto entro 5 minuti, invia una richiesta di incidente per attivare manualmente AWS Incident Detection and Response per la risoluzione dei problemi.

Come testare i tuoi allarmi

CloudWatch Allarmi Amazon

> **Note**
>
> L' AWS Identity and Access Management utente o il ruolo che usi per i test degli allarmi deve avere `cloudwatch:SetAlarmState` l'autorizzazione.

Usa AWS Command Line Interface o AWS CloudShellper impostare manualmente la sveglia sullo stato ALARM. Questi comandi modificano lo stato dell'allarme senza influire sul carico di lavoro.

Per evitare azioni indesiderate, ad esempio il riavvio delle istanze Amazon EC2, disabilita CloudWatch qualsiasi azione di allarme prima di modificare lo stato dell'allarme. Puoi riattivare le azioni di CloudWatch allarme dopo il completamento del test. Per ulteriori informazioni su come disabilitare o abilitare le azioni di allarme, consulta DisableAlarmActionse EnableAlarmActionsconsulta Amazon CloudWatch API Reference.

Disattiva le azioni di allarme:

```
aws cloudwatch disable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

Imposta lo stato di allarme su ALARM:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-
reason "Testing AWS Incident Detection and Response" --region us-east-1
```

Re-enable azioni di allarme dopo il test:

```
aws cloudwatch enable-alarm-actions --alarm-names "ExampleAlarm" --region us-east-1
```

Lo stato di allarme torna automaticamente a OK entro pochi secondi.

Allarmi compositi

Il **`set-alarm-state`** comando non garantisce che gli allarmi compositi tornino allo stato OK. Come procedura ottimale, verifica lo stato degli allarmi compositi dopo il test. Per resettare manualmente un allarme composito, usa il seguente comando:

```
aws cloudwatch set-alarm-state --alarm-name "ExampleCompositeAlarm" --state-value OK --
state-reason "Testing AWS Incident Detection and Response" --region us-east-1
```

Per ulteriori informazioni sulla modifica manuale dello stato degli CloudWatch allarmi, consulta SetAlarmStateAmazon CloudWatch API Reference.

Per ulteriori informazioni sulle autorizzazioni richieste per le operazioni CloudWatch API, consulta Amazon CloudWatch permissions reference.

Third-party Allarmi APM

I carichi di lavoro che utilizzano uno strumento APM (Application Performance Monitoring) di terze parti, come Datadog, Splunk, New Relic o Dynatrace, richiedono istruzioni diverse per simulare un allarme.

1. Disattiva le azioni di allarme nel tuo APM per prevenire azioni indesiderate.
2. Modifica la soglia di allarme o l'operatore di confronto per forzare l'allarme allo stato ALARM. Ciò attiva un payload per AWS Incident Detection and Response.
3. Al termine del test, ripristina la soglia o le modifiche dell'operatore di confronto per riportare l'allarme allo stato OK.

Principali risultati

Dopo il successo dei test:

- L'inserimento dell'allarme è confermato e la configurazione dell'allarme è corretta.
- Gli allarmi vengono ricevuti da AWS Incident Detection and Response.
- Viene creato un caso di supporto e i contatti prescritti vengono avvisati.
- AWS Incident Detection and Response ti coinvolge con i mezzi di conferenza prescritti.
- Tutti gli allarmi e i casi di assistenza generati durante i test sono stati risolti.

Domande frequenti

Il test degli allarmi è obbligatorio?

No I test sono facoltativi ma fortemente consigliati per convalidare le disposizioni di risposta end-to-end prima che si verifichi un incidente reale.

Il mio carico di lavoro ne risentirà?

No. Tuttavia, durante il test, tutte le azioni di allarme configurate sugli allarmi vengono attivate a meno che non le disabiliti. Disattiva le azioni di allarme prima del test per evitare impatti indesiderati.

Chi viene avvisato durante il test?

Durante una pianificazione GameDay, tutti i contatti e i percorsi di escalation presenti nel runbook vengono contattati per la verifica. Durante il test degli allarmi offline, viene notificato solo il contatto iniziale specificato durante l'attivazione degli allarmi.

Posso rispondere via e-mail agli aggiornamenti dei casi?

No Le copie via e-mail delle corrispondenze relative ai Supporto casi vengono inviate da un indirizzo senza risposta. Per aggiornare un caso, usa il. AWS Support Center Console

Come posso richiedere un GameDay post go-live?

Rispondi al tuo caso di supporto all'onboarding esistente, se esiste, o crea un. Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response

Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response

Per richiedere modifiche a un carico di lavoro integrato, completa i seguenti passaggi per creare un caso di supporto con AWS Incident Detection and Response.

1. Vai al Supporto AWS Centro, quindi seleziona Crea caso, come mostrato nell'esempio seguente:

2. Scegli Tecnico.
3. Per Assistenza, scegli Incident Detection and Response.
4. Per Categoria, scegli Richiesta di modifica del carico di lavoro.
5. Per Severità, scegli Guida generale.
6. Inserisci un oggetto per questa modifica. Esempio:

   Rilevamento e risposta agli incidenti di AWS - *`workload_name`*
7. Inserisci una descrizione per questa modifica. Ad esempio, inserisci «Questa richiesta riguarda le modifiche a un carico di lavoro esistente onboardato in AWS Incident Detection and Response». Assicurati di includere le seguenti informazioni nella tua richiesta:

   - Nome del carico di lavoro: il nome del tuo carico di lavoro.
   - ID account: ID1, ID2, ID3 e così via.

- Dettagli della modifica: inserisci i dettagli della modifica richiesta.

8. Nella sezione Contatti aggiuntivi - facoltativa, inserisci gli ID e-mail a cui desideri ricevere la corrispondenza relativa a questa modifica.

   Di seguito è riportato un esempio della sezione Contatti aggiuntivi - opzionale.

   > **Important**
   >
   > La mancata aggiunta degli ID e-mail nella sezione Contatti aggiuntivi - opzionale potrebbe ritardare il processo di modifica.

9. Seleziona Invia.

   Dopo aver inviato la richiesta di modifica, puoi aggiungere altre email dalla tua organizzazione. Per aggiungere e-mail, scegli Rispondi nei dettagli del caso, come mostrato nell'esempio seguente:

   Quindi, aggiungi gli ID e-mail nella sezione Contatti aggiuntivi - opzionale.

   Di seguito è riportato un esempio della pagina Rispondi che mostra dove è possibile inserire altre e-mail.

Sopprimi gli allarmi attivando il rilevamento e la risposta agli incidenti

Specificate quali allarmi di carico di lavoro integrati interagiscono con il monitoraggio di AWS Incident Detection and Response sopprimendoli temporaneamente o secondo una pianificazione. Ad esempio, potresti sopprimere temporaneamente gli allarmi relativi al carico di lavoro durante la manutenzione pianificata per evitare che gli allarmi attivino Incident Detection and Response. In alternativa, puoi sopprimere gli allarmi in base a una pianificazione se hai un'attività di riavvio giornaliera. Puoi sopprimere gli allarmi alla fonte dell'allarme, come Amazon CloudWatch, oppure puoi inviare una richiesta di modifica del carico di lavoro.

Argomenti

- Sopprimi gli allarmi alla fonte dell'allarme
- Invia una richiesta di modifica del carico di lavoro per eliminare gli allarmi
- Tutorial: Usa una funzione matematica metrica per sopprimere un allarme
- Tutorial: rimuovi una funzione matematica metrica per annullare la soppressione di un allarme

Sopprimi gli allarmi alla fonte dell'allarme

Specificate quali allarmi interagiscono con Incident Detection and Response e quando lo fanno, sopprimendo gli allarmi alla fonte dell'allarme.

Argomenti

- Usa una funzione matematica metrica per sopprimere un allarme CloudWatch
- Rimuovi una funzione matematica metrica per annullare la soppressione di un allarme CloudWatch
- Esempi di funzioni matematiche metriche e casi d'uso associati
- Sopprimi gli allarmi provenienti da un APM di terze parti

Usa una funzione matematica metrica per sopprimere un allarme CloudWatch

Per sopprimere il monitoraggio degli CloudWatch allarmi Amazon Incident Detection and Response, utilizza una funzione matematica metrica per impedire che gli CloudWatch allarmi entrino `ALARM` nello stato durante una finestra designata.

> **Note**
>
> La disabilitazione delle azioni di allarme su un CloudWatch allarme non sopprime il monitoraggio degli allarmi tramite Incident Detection and Response. Le modifiche allo stato degli allarmi vengono acquisite tramite Amazon EventBridge, non tramite azioni di CloudWatch allarme.

Per utilizzare una funzione matematica metrica per sopprimere un CloudWatch allarme, completa i seguenti passaggi:

1. Accedi a Console di gestione AWS e apri la console all' CloudWatch indirizzo. https://console.aws.amazon.com/cloudwatch/

2. Scegli Allarmi, quindi individua l'allarme a cui desideri aggiungere la funzione matematica metrica.
3. Scegli Azioni, quindi seleziona Modifica per modificare l'allarme.
4. Scegli Modifica metrica per modificare la metrica dell'allarme.
5. Scegli Aggiungi matematica, Inizia con un'espressione vuota.
6. Inserisci la tua espressione matematica, quindi scegli Applica.
7. Deseleziona la metrica esistente monitorata dall'allarme.
8. Seleziona l'espressione che hai appena creato, quindi scegli Seleziona metrica.
9. Scegliete Salta all'anteprima e create.
10. Controlla le modifiche per assicurarti che la funzione matematica metrica venga applicata come previsto, quindi scegli Aggiorna allarme.

Per un esempio dettagliato di soppressione di un CloudWatch allarme con una funzione matematica metrica, consulta. Tutorial: Usa una funzione matematica metrica per sopprimere un allarme

Per ulteriori informazioni sulla sintassi e sulle funzioni disponibili, consulta Metric Math syntax and functions nella Amazon User Guide. CloudWatch

Rimuovi una funzione matematica metrica per annullare la soppressione di un allarme CloudWatch

Annulla la soppressione di un allarme rimuovendo la funzione matematica metrica CloudWatch . Per rimuovere una funzione matematica metrica da un avviso, completare i seguenti passaggi:

1. Accedi a Console di gestione AWS e apri la CloudWatch console all'indirizzo. https://console.aws.amazon.com/cloudwatch/
2. Scegli Allarmi, quindi individua l'allarme o gli allarmi da cui desideri rimuovere l'espressione matematica metrica.
3. Nella sezione matematica metrica, scegli Modifica.
4. Per rimuovere la metrica dall'allarme, scegli Modifica sulla metrica, quindi scegli il pulsante x accanto all'espressione matematica della metrica.
5. Seleziona la metrica originale, quindi scegli Seleziona metrica.
6. Scegli Vai all'anteprima e crea.

7. Controlla le modifiche per assicurarti che la funzione matematica metrica venga applicata come previsto, quindi scegli Aggiorna allarme.

Esempi di funzioni matematiche metriche e casi d'uso associati

La tabella seguente contiene esempi di funzioni matematiche metriche, insieme ai casi d'uso associati e una spiegazione di ciascun componente metrico.

Funzione matematica metrica	Caso d’uso	Spiegazione
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	Sopprimi l'allarme tra le 1:00 e le 3:00 UTC di ogni martedì sostituendo i punti dati reali con 0 durante questa finestra.	• DAY (m1) == 2: Assicura che sia martedì (lunedì = 1, domenica = 7). • ORA (m1) >= 1 && ORA (m1) > 3: specifica l'intervallo di tempo dall'1:00 alle 3:00 UTC. • IF (condition, value_if_true, value_if_false) :Se le condizioni sono vere, sostituisci il valore della metrica con 0. Altrimenti, restituisci il valore originale (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	Sopprimi l'allarme tra le 23:00 e le 4:00 UTC, ogni giorno sostituendo i punti dati reali con 0 durante questa finestra.	• HOUR (m1) >= 23: registra le ore a partire dalle 23:00 UTC. • ORA (m1) < 4: registra le ore fino (ma non incluse) alle 04:00 UTC. • ||: Logical OR assicura che la condizione si applichi in due intervalli: le ore notturne e le prime ore del mattino.

Funzione matematica metrica	Caso d’uso	Spiegazione
		• IF (condition, value_if_true, value_if_false): restituis ce 0 durante l'intervallo di tempo specificato. Mantiene il valore metrico originale m1 al di fuori di tale intervall o.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	Sopprimi l'allarme tra le 11:00 e le 13:00 UTC ogni giorno sostituendo i punti dati reali con 0 durante questa finestra.	• ORA (m1) >= 11 && ORA (m1) < 13: acquisisce l'intervallo di tempo dalle 11:00 alle 13:00 UTC. • IF (condition, value_if_ true, value_if_false): Se la condizione è vera (ad esempio, l'ora è compresa tra le 11:00 e le 13:00 UTC), restituisci 0, se la condizion e è falsa, conserva il valore metrico originale (m1).

Funzione matematica metrica	Caso d’uso	Spiegazione
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	Sopprimi l'allarme tra l'1:00 e le 3:00 UTC di ogni martedì sostituendo i punti dati reali con 99 durante questa finestra.	• DAY (m1) = 2: Assicura che sia martedì (lunedì = 1, domenica = 7). • ORA (m1) >= 1 && ORA (m1) < 3: specifica l'intervallo di tempo dall'1:00 alle 3:00 UTC. • IF (condition, value_if_true, value_if_false): se le condizioni sono vere, sostituisci il valore della metrica con 99. Altrimenti, restituisci il valore originale (m1).
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	Sopprimi l'allarme tra le 23:00 e le 4:00 UTC, ogni giorno sostituendo i punti dati reali con 100 durante questa finestra.	• HOUR (m1) >= 23: registra le ore a partire dalle 23:00 UTC. • ORA (m1) < 4: registra le ore fino (ma non incluse) alle 04:00 UTC. • ||: Logical OR assicura che la condizione si applichi in due intervalli: le ore notturne e le prime ore del mattino. • IF (condition, value_if_true, value_if_false): restituisce 100 durante l'intervallo di tempo specificato. Mantiene il valore metrico originale m1 al di fuori di tale intervallo.

Funzione matematica metrica	Caso d'uso	Spiegazione
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	Sopprimi l'allarme tra le 11:00 e le 13:00 UTC ogni giorno sostituendo i punti dati reali con 99 durante questa finestra.	• ORA (m1) >= 11 && ORA (m1) < 13: acquisisce l'intervallo di tempo dalle 11:00 alle 13:00 UTC. • IF (condition, value_if_ true, value_if_false): se la condizione è vera (ad esempio, l'ora è compresa tra le 11:00 e le 13:00 UTC), restituisci 99. Se la condizione è falsa, mantieni il valore metrico originale (m1).

Sopprimi gli allarmi provenienti da un APM di terze parti

Consultate la documentazione del vostro fornitore APM terzo per istruzioni su come sopprimere gli allarmi. Esempi di fornitori APM di terze parti sono New Relic, Splunk, Dynatrace, Datadog e. SumoLogic

Invia una richiesta di modifica del carico di lavoro per eliminare gli allarmi

Se non riesci a sopprimere gli allarmi alla fonte come descritto nella sezione precedente, invia una richiesta di modifica del carico di lavoro per indicare a Incident Detection and Response di sospendere manualmente il monitoraggio di alcuni o tutti gli allarmi del tuo carico di lavoro.

Per istruzioni dettagliate su come creare una richiesta di modifica del carico di lavoro, consulta Richiedere modifiche a un carico di lavoro integrato in Incident Detection and Response. Quando invii una richiesta di modifica del carico di lavoro per richiedere la soppressione degli allarmi, assicurati di fornire le seguenti informazioni obbligatorie

- Nome del carico di lavoro: il nome del tuo carico di lavoro.
- ID account: ID1, ID2 ID3, e così via.
- Dettagli della modifica: Soppressione degli allarmi

- Ora di inizio della soppressione: data, ora e fuso orario.
- Ora di fine della soppressione: data, ora e fuso orario.
- Allarmi da sopprimere: un elenco di CloudWatch allarmi ARNs o identificatori di eventi APM di terze parti da sopprimere.

Dopo aver creato la richiesta di modifica del carico di lavoro per la soppressione degli allarmi, ricevi le seguenti notifiche da Incident Detection and Response:

- Riconoscimento della richiesta di modifica del carico di lavoro.
- Notifica quando gli allarmi vengono soppressi.
- Notifica quando gli allarmi vengono riattivati per il monitoraggio.

Tutorial: Usa una funzione matematica metrica per sopprimere un allarme

Il seguente tutorial spiega come sopprimere un CloudWatch allarme utilizzando la matematica metrica.

Scenario di esempio

C'è un'attività pianificata che si svolge tra le 1:00 e le 3:00 UTC del martedì prossimo. Vuoi creare una funzione matematica CloudWatch metrica che sostituisca i punti dati reali durante questo periodo, con 0 (un punto dati che scende al di sotto della soglia impostata).

1. Valuta i criteri che determinano l'attivazione dell'allarme. La schermata seguente fornisce un esempio di criteri di allarme:

   L'allarme mostrato nella schermata precedente monitora la `UnHealthyHostCount` metrica per un gruppo target di Application Load Balancer. Questo allarme entra `ALARM` nello stato quando la `UnHealthyHostCount` metrica è maggiore o uguale a 3 per 5 punti dati su 5. L'allarme considera i dati mancanti come errati (superando la soglia configurata).
2. Crea la funzione matematica metrica.

   In questo esempio, l'attività pianificata si svolge tra le 1:00 e le 3:00 UTC del martedì successivo. Quindi, crea una funzione matematica CloudWatch metrica che sostituisca i punti dati reali durante questo periodo, con 0 (un punto dati che scende al di sotto della soglia impostata).

Nota che il punto dati sostitutivo che devi configurare varia a seconda della configurazione dell'allarme. Ad esempio, se disponi di un allarme che monitora la percentuale di successo HTTP, con una soglia inferiore a 98, sostituisci i punti dati reali durante l'attività pianificata con un valore superiore alla soglia configurata, 100. Di seguito è riportato un esempio di funzione matematica metrica per questo scenario.

```
IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
```

La precedente funzione matematica metrica contiene i seguenti elementi:

- DAY (m1) == 2: Assicura che sia martedì (lunedì = 1, domenica = 7).
- ORA (m1) >= 1 && ORA (m1) < 3: specifica l'intervallo di tempo dall'1:00 alle 3:00 UTC.
- IF (condition, value_if_true, value_if_false): se le condizioni sono vere, la funzione sostituisce il valore della metrica con 0. Altrimenti, viene restituito il valore originale (m1).

Per ulteriori informazioni sulla sintassi e sulle funzioni disponibili, consulta Metric Math Syntax and functions nella Amazon User Guide CloudWatch

3. Accedi Console di gestione AWS e apri la console all'indirizzo. CloudWatch https://console.aws.amazon.com/cloudwatch/
4. Scegli Allarmi, quindi individua l'allarme a cui desideri aggiungere la funzione matematica metrica.
5. Nella sezione matematica metrica, scegli Modifica.
6. Scegli Aggiungi matematica, Inizia con un'espressione vuota.
7. Inserisci la tua espressione matematica, quindi scegli Applica.

   La metrica esistente monitorata dall'allarme diventa automaticamente m1 e l'espressione matematica è e1, come mostrato nell'esempio seguente:

8. (Facoltativo) Modifica l'etichetta dell'espressione matematica metrica per aiutare gli altri a comprenderne la funzione e il motivo per cui è stata creata, come mostrato nell'esempio seguente:

9. Deseleziona m1, seleziona e1, quindi scegli Seleziona metrica. Questo imposta l'allarme per monitorare direttamente l'espressione matematica anziché la metrica sottostante.

10. Scegli Salta all'anteprima e crea.
11. Verifica che l'allarme sia configurato come previsto, quindi scegli Aggiorna allarme per salvare la modifica.

Nell'esempio precedente, senza l'applicazione della funzione matematica metrica, la `UnHealthyHostCount` metrica reale sarebbe stata riportata durante l'attività pianificata. Ciò avrebbe comportato l'ingresso dell' CloudWatch allarme `ALARM` nello stato e l'attivazione del rilevamento e della risposta agli incidenti, come mostrato nell'esempio seguente:

Una volta attivata la funzione matematica metrica, i punti dati reali vengono sostituiti con 0 durante l'attività e l'allarme rimane attivo, impedendo l'attivazione `OK` del rilevamento e della risposta agli incidenti.

Tutorial: rimuovi una funzione matematica metrica per annullare la soppressione di un allarme

Se sopprimi un CloudWatch allarme per un'attività occasionale, rimuovi la funzione matematica metrica dall'allarme dopo il completamento dell'attività per riprendere il monitoraggio regolare dell'allarme. Per disattivare l'allarme in base a una pianificazione regolare, ad esempio, se hai una routine di patch settimanale pianificata che comporta riavvii nello stesso giorno e ora ogni settimana, lascia attiva la funzione matematica metrica.

Il seguente tutorial illustra come rimuovere una funzione matematica metrica per annullare la soppressione di un allarme CloudWatch

1. Accedi a Console di gestione AWS e apri la console all'indirizzo. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. Scegli Allarmi, quindi individua l'allarme a cui desideri aggiungere la funzione matematica metrica.
3. Nella sezione matematica metrica, scegli Modifica.
4. Per rimuovere la soppressione dall'allarme, seleziona il pulsante x accanto all'espressione matematica metrica.

5. Seleziona la metrica per riprendere il monitoraggio della metrica reale, quindi scegli Seleziona metrica.

6. Scegli Salta all'anteprima e crea.
7. Verifica che l'allarme sia configurato come previsto, quindi scegli Aggiorna allarme per salvare la modifica.

Elimina un carico di lavoro da Incident Detection and Response

Per eseguire l'offboard di un carico di lavoro da AWS Incident Detection and Response, crea un nuovo caso di supporto per ogni carico di lavoro. Quando crei il caso di supporto, tieni presente quanto segue:

- Per eliminare un carico di lavoro relativo a un unico AWS account, crea la richiesta di assistenza dall'account del carico di lavoro o dal tuo account di pagamento.
- Per eliminare un carico di lavoro che si estende su più AWS account, crea la richiesta di assistenza dal tuo account di pagamento. Nel corpo della richiesta di assistenza, elenca tutti gli ID degli account da offboard.

> **Important**
>
> Se crei una richiesta di assistenza per trasferire un carico di lavoro dall'account errato, potresti riscontrare ritardi e richieste di informazioni aggiuntive prima che i carichi di lavoro possano essere scaricati.

Richiesta di esternalizzazione di un carico di lavoro

1. Vai al Supporto AWS Centro, quindi seleziona Crea caso.
2. Scegli Tecnico.
3. Per Assistenza, scegli Incident Detection and Response.
4. Per Categoria, scegli Workload Offboarding.
5. Per Severità, scegli General Guidance.
6. Inserisci un oggetto per questa modifica. Esempio:

[Offboard] Rilevamento e risposta agli incidenti di AWS - *workload_name*

7. Inserisci una descrizione per questa modifica. Ad esempio, inserisci «Questa richiesta è per l'offboarding di un carico di lavoro esistente inserito in AWS Incident Detection and Response». Assicurati di includere le seguenti informazioni nella tua richiesta:

   - Nome del carico di lavoro: il nome del tuo carico di lavoro.
   - ID account: ID1, ID2, ID3 e così via.
   - Motivo dell'offboarding: fornisci un motivo per l'offboarding del carico di lavoro.

8. Nella sezione Contatti aggiuntivi - opzionale, inserisci gli eventuali ID e-mail a cui desideri ricevere la corrispondenza relativa a questa richiesta di offboarding.
9. Seleziona Invia.

Monitoraggio e osservabilità di AWS Incident Detection and Response

AWS Incident Detection and Response offre una guida esperta sulla definizione dell'osservabilità per tutti i carichi di lavoro, dal livello applicativo all'infrastruttura sottostante. Il monitoraggio ti dice che qualcosa non va. L'osservabilità utilizza la raccolta di dati per dirti cosa c'è che non va e perché è successo.

Il sistema Incident Detection and Response monitora i AWS carichi di lavoro alla ricerca di guasti e peggioramento delle prestazioni sfruttando servizi nativi AWS come Amazon e CloudWatch Amazon EventBridge per rilevare eventi che potrebbero influire sul carico di lavoro. Il monitoraggio fornisce notifiche in caso di guasti imminenti, in corso, recessivi o potenziali o di peggioramento delle prestazioni. Quando si integra l'account in Incident Detection and Response, si selezionano gli allarmi del proprio account che devono essere monitorati dal sistema di monitoraggio Incident Detection and Response e si associano tali allarmi a un'applicazione e a un runbook utilizzati durante la gestione degli incidenti.

Incident Detection and Response utilizza Amazon CloudWatch e altri Servizi AWS per creare la tua soluzione di osservabilità. AWS Incident Detection and Response ti aiuta con l'osservabilità in due modi:

- Metriche dei risultati aziendali: l'osservabilità su AWS Incident Detection and Response inizia con la definizione delle metriche chiave che monitorano i risultati dei carichi di lavoro o dell'esperienza dell'utente finale. AWS gli esperti collaborano con te per comprendere gli obiettivi del tuo carico di lavoro, gli output o i fattori chiave che possono influire sull'esperienza utente e per definire i parametri e gli avvisi che rilevano qualsiasi peggioramento di tali metriche chiave. Ad esempio, una metrica aziendale chiave per un'applicazione di chiamata mobile è la percentuale di successo della configurazione delle chiamate (monitora la percentuale di successo dei tentativi di chiamata degli utenti), mentre una metrica chiave per un sito Web è la velocità della pagina. Il coinvolgimento degli incidenti viene attivato in base alle metriche dei risultati aziendali.
- Metriche a livello di infrastruttura: in questa fase, identifichiamo la base Servizi AWS e l'infrastruttura che supporta l'applicazione e definiamo metriche e allarmi per monitorare le prestazioni di questi servizi infrastrutturali. Queste possono includere metriche come quelle relative alle `ApplicationLoadBalancerErrorCount` istanze di Application Load Balancer. Ciò inizia dopo l'onboarding del carico di lavoro e l'impostazione del monitoraggio.

Implementazione dell'osservabilità su AWS Incident Detection and Response

Poiché l'osservabilità è un processo continuo che potrebbe non essere completato in un esercizio o in un intervallo di tempo, AWS Incident Detection and Response implementa l'osservabilità in due fasi:

- Fase di onboarding: l'osservabilità durante l'onboarding si concentra sul rilevamento di quando i risultati aziendali dell'applicazione sono compromessi. A tal fine, l'osservabilità durante la fase di onboarding si concentra sulla definizione delle metriche chiave dei risultati aziendali a livello di applicazione per notificare le interruzioni dei carichi di lavoro. AWS In questo modo è AWS possibile rispondere prontamente a queste interruzioni e fornire assistenza per il ripristino. Per ulteriori informazioni sull'utilizzo dell'interfaccia a riga di comando del cliente AWS Incident Detection and Response per automatizzare questi passaggi, consulta la CLI for AWS Incident Detection and Response.
- Post-onboarding fase: AWS Incident Detection and Response offre una serie di servizi proattivi per l'osservabilità, tra cui la definizione di parametri a livello di infrastruttura, l'ottimizzazione dei parametri e la configurazione di tracce e log in base al livello di maturità del cliente. L'implementazione di questi servizi può durare diversi mesi e coinvolgere più team. AWS Incident Detection and Response fornisce indicazioni sulla configurazione dell'osservabilità e i clienti sono tenuti a implementare le modifiche richieste nel loro ambiente di carico di lavoro. Per ricevere assistenza nell'implementazione pratica delle funzionalità di osservabilità, invia una richiesta ai tuoi Technical Account Manager (TAM).

Gestione degli incidenti con Incident Detection and Response

AWS Incident Detection and Response ti offre 24 ore al giorno, 7 giorni alla settimana, monitoraggio proattivo e gestione degli incidenti forniti da un team designato di responsabili degli incidenti. Il seguente diagramma delinea il processo standard di gestione degli incidenti quando un allarme di un'applicazione innesca un incidente, tra cui la generazione di allarmi, il coinvolgimento di AWS Incident Manager, la risoluzione degli incidenti e la revisione post-incidente.

1. Generazione di allarmi: gli allarmi attivati sui carichi di lavoro vengono inviati tramite Amazon EventBridge ad AWS Incident Detection and Response. AWS Incident Detection and Response richiama automaticamente il runbook associato all'allarme e notifica un incident manager. Se si verifica un incidente critico sul tuo carico di lavoro che non viene rilevato dagli allarmi monitorati da AWS Incident Detection and Response, puoi creare un caso di supporto per richiedere un Incident Response. Per ulteriori informazioni sulla richiesta di un Incident Response, consulta. Richiedi una risposta all'incidente
2. AWS Intervento dell'Incident Manager: il gestore degli incidenti risponde all'allarme e coinvolge l'utente in una teleconferenza o come diversamente specificato nel runbook. Il responsabile degli incidenti verifica lo stato dell'allarme Servizi AWS per determinare se l'allarme è correlato a problemi Servizi AWS utilizzati dal carico di lavoro e fornisce informazioni sullo stato dei servizi sottostanti. Se necessario, il responsabile degli incidenti crea quindi un caso per vostro conto e coinvolge gli esperti giusti AWS per il supporto. Poiché AWS Incident Detection and Response monitora Servizi AWS specificamente le tue applicazioni, AWS Incident Detection and Response potrebbe determinare che l'incidente è correlato a un Servizio AWS problema prima che venga dichiarato un Servizio AWS evento. In questo scenario, il gestore degli incidenti fornisce informazioni sullo stato dell' Servizio AWS evento Servizio AWS, attiva il flusso di lavoro di gestione degli incidenti e segue il team di assistenza in merito alla risoluzione. Le informazioni fornite offrono l'opportunità di implementare tempestivamente i piani di ripristino o le soluzioni alternative per mitigare l'impatto dell'evento. Servizio AWS

   A volte gli allarmi si attivano e si ripristinano rapidamente. In questo scenario, il responsabile dell'incidente invia una corrispondenza in cui comunica che l'allarme è stato ripristinato, ma non contatta l'utente. Tuttavia, se un allarme si attiva più di una volta nell'arco di 15 minuti, l'Incident Manager contatta l'utente in base alle istruzioni del runbook, anche se l'allarme si riattiva.

3. Risoluzione degli incidenti: il responsabile degli incidenti coordina l'incidente tra i AWS team necessari e si assicura che restiate in contatto con AWS gli esperti giusti fino a quando l'incidente non viene mitigato o risolto.
4. Revisione post-incidente (se richiesta): dopo un incidente, AWS Incident Detection and Response può eseguire una revisione post-incidente su tua richiesta e generare un rapporto post-incidente. Il rapporto post incidente include una descrizione del problema, dell'impatto, dei team coinvolti e delle soluzioni alternative o delle azioni intraprese per mitigare o risolvere l'incidente. Il rapporto post incidente potrebbe contenere informazioni che possono essere utilizzate per ridurre la probabilità di recidiva dell'incidente o per migliorare la gestione delle future occorrenze di un incidente simile. Il Post Incident Report non è un'analisi delle cause principali (RCA). Puoi richiedere un RCA in aggiunta al Post Incident Report. Un esempio di rapporto post incidente è fornito nella sezione seguente.

> **Important**
>
> Il seguente modello di report è solo un esempio.

```
Post ** Incident ** Report ** Template
Post Incident Report - 0000000123
Customer: Example Customer
Supporto AWS case ID(s): 0000000000
Customer internal case ID (if provided): 1234567890
Incident start: 2023-02-04T03:25:00 UTC
Incident resolved: 2023-02-04T04:27:00 UTC
Total Incident time: 1:02:00 s
Source Alarm ARN: arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-
impaired-useast1-P95

Problem Statement:
Outlines impact to end users and operational infrastructure impact.
 Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage
 of their workload that lasted one hour and two minutes and spanning across all
 Availability Zones where the application is deployed. During impact, end users were
 unable to connect to the workload's Application Load Balancers (ALBs) which service
 inbound communications to the application.

Incident Summary:
```

```
Summary of the incident in chronological order and steps taken by AWS Incident Managers
 to direct the incident to a path to mitigation.
  At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical
 incident for the workload. AWS Incident Detection and Response Managers responded to
 the alarm, checking AWS service health and steps outlined in the workload’s runbook.
  At 2023-02-04T03:28:00 UTC, ** per the runbook, the alarm had not recovered and the
 Incident Management team sent the engagement email to the customer’s Site Reliability
 Team (SRE) team, created a troubleshooting bridge, and an Supporto support case on
 behalf of the customer.
  At 2023-02-04T03:32:00 UTC, ** the customer’s SRE team, and Supporto Engineering
 joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to
 services the workload depends on. The investigation shifted to the specific resources
 in the customer account.
  At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase
 in traffic volume was causing a drop in connections. The customer confirmed this
 ALB was newly provisioned to handle an increase in workload traffic for an on-going
 promotional event.
  At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The
 Incident Manager worked with the Cloud Support Engineer to raise an escalation a
 higher support level to quickly scale the ALB per the runbook.
  At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The
 back-off/retry logic yields mild recovery but timeouts are still being seen for some
 clients.
 By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to
 pre-incident levels. Connection timeouts subside.
  At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes
 of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

Mitigation:
Describes what was done to mitigate the issue. NOTE: this is not a Root Cause Analysis
 (RCA).
  Back-off and retries yielded mild recovery. Full mitigation happened after escalation
 to ALB support team (per runbook) to scale the newly provisioned ALB.

Follow up action items (if any):
Action items to be reviewed with your Technical Account Manager (TAM), if required.
Review alarm thresholds to engage AWS Incident Detection and Response closer to the
 time of impact.
Work with Supporto AWS and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

Argomenti

Fornire l'accesso a AWS Support Center Console per i team applicativi

AWS Incident Detection and Response comunica con te attraverso i Supporto casi durante il ciclo di vita di un incidente. Per comunicare con Incident Manager, i tuoi team devono avere accesso al Centro. Supporto

Per ulteriori informazioni sulla fornitura dell'accesso, consulta Gestire l'accesso al Supporto Centro nella Guida per l'Supporto utente.

Richiedi una risposta all'incidente

Se si verifica un incidente critico sul tuo carico di lavoro che non viene rilevato dagli allarmi monitorati da AWS Incident Detection and Response, puoi creare un caso di supporto per richiedere un Incident Response. Puoi richiedere un Incident Response per qualsiasi carico di lavoro sottoscritto ad AWS Incident Detection and Response, compresi i carichi di lavoro in fase di onboarding, utilizzando l' AWS Support Center Console API, o. Supporto AWS AWS Support App in Slack

Il diagramma seguente illustra il flusso di lavoro completo per un AWS cliente che richiede assistenza agli incidenti al team di rilevamento e risposta agli incidenti, descrivendo in dettaglio i passaggi dalla richiesta iniziale all'indagine, alla mitigazione e alla risoluzione.

Per richiedere una risposta agli incidenti per un incidente che ha un impatto attivo sul tuo carico di lavoro, crea un caso. Supporto Una volta sollevata la richiesta di supporto, AWS Incident Detection and Response ti coinvolge in un conference bridge con gli AWS esperti necessari per accelerare il recupero del tuo carico di lavoro.

Richiedi un Incident Response utilizzando il AWS Support Center Console

Per richiedere una risposta all'incidente, completa i seguenti passaggi:

1. Apri AWS Support Center Consoleper creare un nuovo caso di supporto.
2. In Oggetto, inserisci un breve riepilogo dell'incidente. Ad esempio, `AWS Incident Detection and Response - Active Incident - workload_name`.
3. In Descrizione, inserire i dettagli dell'incidente. Ti consigliamo di includere i seguenti dettagli nella tua richiesta di assistenza:
   - ARN della AWS risorsa interessata, nome del carico di lavoro e relativa funzione
   - Descrizione dell'impatto sull'azienda
   - (Facoltativo) L'URL del tuo conference bridge preferito. Se non fornisci i dettagli del bridge, AWS Incident Detection and Response crea un bridge per AWS conferenze e ti invia un invito con l'URL del bridge.
4. (Facoltativo) Allega file che possono aiutare a descrivere l'incidente, come schermate o estratti di log.
5. Configura i seguenti campi di classificazione dei casi:
   - Tipo di caso: tecnico
   - Servizio: rilevamento e risposta agli incidenti
   - Categoria: Incidente attivo
   - Severità: Business-critical sistema inattivo
6. Fornisci un contesto aggiuntivo per aiutare AWS Incident Detection and Response a coinvolgere più rapidamente AWS gli esperti, ad esempio l'impatto Servizio AWS, l'impatto aziendale Regione AWS, l'impatto sull'orario di inizio e le risorse interessate.
7. Seleziona Invia.
8. AWS Incident Detection and Response riconosce il tuo caso entro cinque minuti e ti coinvolge in una conferenza con gli esperti appropriati AWS .

Richiedi un Incident Response utilizzando il Supporto AWS "Hello, World!"

Puoi utilizzare l' Supporto AWS API per creare casi di supporto in modo programmatico. Per ulteriori informazioni, consulta Informazioni sull' Supporto AWS API nella Guida per l'Supporto AWS utente.

Richiedi una risposta all'incidente utilizzando il AWS Support App in Slack

Per utilizzare il AWS Support App in Slack per richiedere un Incident Response, completa i seguenti passaggi:

1. Apri il canale Slack in cui hai AWS Support App in Slack configurato.
2. Immetti il comando seguente:

```
/awssupport create
```

3. Inserisci un oggetto per questo incidente. Ad esempio, inserisci AWS Incident Detection and Response - Active Incident - workload_name.
4. Inserisci la descrizione del problema per questo incidente. Aggiungi i seguenti dettagli:

   Informazioni tecniche:

   Servizio/i interessato/i:

   Risorsa/e interessata/e:

   Regione/i interessato/i:

   Nome del carico di lavoro:

   Informazioni aziendali:

   Descrizione dell'impatto sull'attività:

   [Facoltativo] Dettagli di Customer Bridge:
5. Scegli Next (Successivo).

6. Per Tipo di problema, scegli Supporto tecnico.
7. Per Assistenza, scegli Incident Detection and Response.
8. Per Categoria, scegli Active Incident.
9. Per Severità, scegli Business-critical System down.

10. Facoltativamente, inserisci fino a 10 contatti aggiuntivi nel campo Altri contatti da notificare, separati da virgole. Questi contatti aggiuntivi ricevono copie della corrispondenza e-mail relativa a questo incidente.

11. Scegli Rivedi.

12. Un nuovo messaggio visibile solo a te appare nel canale Slack. Controlla i dettagli del caso, quindi scegli Crea caso.

13. Il tuo Case ID viene fornito in un nuovo messaggio da. AWS Support App in Slack
14. Incident Detection and Response riconosce il tuo caso entro 5 minuti e ti coinvolge in una conferenza con gli esperti appropriati AWS .
15. La corrispondenza di Incident Detection and Response viene aggiornata nel thread del caso.

Gestisci i casi di supporto per il rilevamento e la risposta agli incidenti con AWS Support App in Slack

Con AWS Support App in Slack, puoi gestire i tuoi Supporto casi in Slack, ricevere notifiche su nuovi incidenti avviati da allarmi sul tuo carico di lavoro AWS Incident Detection and Response e creare richieste di risposta agli incidenti.

Per configurare AWS Support App in Slack, segui le istruzioni fornite nella Guida per l'utente.Supporto

> **Important**
>
> - Per ricevere notifiche in Slack per tutti gli incidenti provocati da allarmi sul tuo carico di lavoro, devi configurarle AWS Support App in Slack per tutti gli account del tuo carico di lavoro che vengono inseriti in AWS Incident Detection and Response. I casi di supporto vengono creati nell'account da cui ha avuto origine l'allarme del carico di lavoro.
> - Durante un incidente è possibile aprire più casi di supporto ad alta gravità per coinvolgere i risolutori. Supporto Ricevi notifiche in Slack per tutti i casi di assistenza aperti durante un incidente che corrispondono alla configurazione delle notifiche per il canale Slack.
> - Le notifiche che ricevi tramite AWS Support App in Slack non sostituiscono i contatti iniziali e crescenti del carico di lavoro che vengono contattati via e-mail o telefonata tramite Incident Detection and Response durante un AWS incidente.

Argomenti

- Crea una richiesta di risposta agli incidenti in Slack

Notifiche di incidenti avviate da allarmi in Slack

Dopo averlo configurato AWS Support App in Slack nel tuo canale Slack, ricevi notifiche sugli incidenti avviati dagli allarmi sul carico di lavoro monitorato di AWS Incident Detection and Response.

L'esempio seguente mostra come vengono visualizzate le notifiche per gli incidenti avviati da allarmi in Slack.

Esempio di notifica

Quando l'incidente avviato da un allarme viene riconosciuto da AWS Incident Detection and Response, in Slack viene generata una notifica simile alla seguente:

Per visualizzare la corrispondenza completa aggiunta da AWS Incident Detection and Response, scegli Vedi dettagli.

Ulteriori aggiornamenti di AWS Incident Detection and Response vengono visualizzati nel thread del caso.

Scegli Vedi dettagli per visualizzare la corrispondenza completa aggiunta da AWS Incident Detection and Response.

Crea una richiesta di risposta agli incidenti in Slack

Per istruzioni su come creare una richiesta di risposta agli incidenti tramite il AWS Support App in Slack, vediRichiedi una risposta all'incidente.

Segnalazione nel rilevamento e nella risposta agli incidenti

AWS Incident Detection and Response fornisce dati operativi e prestazionali per aiutarti a capire come è configurato il servizio, la cronologia degli incidenti e le prestazioni del servizio Incident Detection and Response. Questa pagina descrive i tipi di dati disponibili, inclusi dati di configurazione, dati sugli incidenti e dati sulle prestazioni.

Dati di configurazione

- Tutti gli account registrati
- Nomi di tutte le applicazioni
- Gli allarmi, i runbook e i profili di supporto associati a ciascuna applicazione

Dati sugli incidenti

- Le date, il numero e la durata degli incidenti per ciascuna applicazione
- Le date, il numero e la durata degli incidenti associati a un allarme specifico
- Rapporto successivo all'incidente

Dati sulle prestazioni

- Prestazioni del Service Level Objective (SLO)

Rivolgiti al tuo Technical Account Manager per i dati operativi e prestazionali di cui potresti aver bisogno.

Sicurezza e resilienza del rilevamento e della risposta agli incidenti

Il modello di responsabilitàAWS condivisa si applica alla protezione dei dati in Supporto. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza relative a Servizi AWS ciò che utilizzi.

Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati.

Per informazioni sulla protezione dei dati in Europa, consulta il modello di responsabilitàAWS condivisa e il post sul blog sul GDPR sul AWS Security Blog.

Ai fini della protezione dei dati, ti consigliamo di proteggere le credenziali degli AWS account e di configurare account utente individuali con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza i certificati Secure Sockets Layer/Transport Layer Security (SSL/TLS () per comunicare con AWS le risorse. È consigliabile TLS 1.2 o versioni successive. Per informazioni, consulta Cos'è un certificato SSL/TLS? .
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni, consultare AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3. Per informazioni su Amazon Macie, consulta Amazon Macie.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per informazioni sugli endpoint FIPS disponibili, vedere Federal Information Processing Standard (FIPS) 140-2.

Ti suggeriamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero, ad esempio un campo Nome. Ciò include quando lavori Supporto o Servizi AWS utilizzi la console, l'API, la AWS CLI o. AWS SDKs I dati inseriti nei tag o nei campi in formato libero utilizzati per i nomi possono essere utilizzati per i log di fatturazione o di diagnostica. Quando fornisci un URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

Accesso AWS Incident Detection and Response ai tuoi account

AWS Identity and Access Management (IAM) è un servizio web che ti aiuta a controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse.

AWS Incident Detection and Response e dati sugli allarmi

Per impostazione predefinita, Incident Detection and Response riceve il nome della risorsa Amazon (ARN) e lo stato di ogni CloudWatch allarme nel tuo account, quindi avvia il processo di rilevamento e risposta agli incidenti quando l'allarme integrato passa allo stato ALARM. Se desideri personalizzare le informazioni che il rilevamento e la risposta agli incidenti ricevono dagli allarmi dal tuo account, contatta il tuo Technical Account Manager.

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione della guida IDR.

Modifica	Descrizione	Data
Argomento Amazon SNS standard chiarito per l'integrazione APM	Ha chiarito che i clienti devono creare un argomento Amazon Simple Notification Service standard (non FIFO) quando integrano gli allarmi APM di terze parti con AWS Incident Detection and Response. Per ulteriori informazioni, consulta Inserisci allarmi dagli APM con integrazione diretta con Amazon SNS.	26 maggio 2026
GameDay è ora facoltativo, con questionario di onboarding semplificato e sviluppo di runbook aggiornati	Il test degli allarmi aggiornato (GameDay) sarà facoltativo dopo Go-Live, con due opzioni di test: test degli allarmi programmato o offline. GameDay Semplificati i questionari di onboarding del carico di lavoro e inserimento degli allarmi. Sviluppo aggiornato del runbook per rimuovere i riferimenti ai documenti. AWS Systems Manager Per ulteriori informazioni, consultare Testa i carichi di lavoro integrati in Incident Detection and Response, Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response (percorso di eccezione) e Sviluppa runbook e piani di risposta per rispondere a un incidente in Incident Detection and Response.	26 maggio 2026

Modifica	Descrizione	Data
Procedura di richiesta di risposta agli incidenti aggiornata	È stata aggiornata la procedura Request an Incident Response in modo che corrisponda all' AWS Support Center Console interfaccia utente corrente, ha aggiunto una guida sull'URL del bridge e rimosso gli screenshot obsoleti. Per ulteriori informazioni, consulta Richiedi un Incident Response utilizzando il AWS Support Center Console.	12 maggio 2026
Onboarding aggiornato per Approach CLI-first	È stato aggiornato il capitolo Get started per promuovere l'interfaccia a riga di comando AWS Incident Detection and Response Customer Command Line Interface come metodo di onboarding principale e ha reso obsoleti il Workload Onboarding Questionn aire e il Alarm Ingestion Questionnaire come percorso di onboarding predefinito. I questiona ri rimangono disponibili solo in via eccezionale per i clienti che non possono utilizzare la CLI IDR. Per ulteriori informazioni, consultare Incorpora i carichi di lavoro al rilevamento e alla risposta agli incidenti e Ingestione degli allarmi.	12 maggio 2026
Aggiunti i link ai questionari in giapponese	Sono stati aggiunti i link per Japanese-language il download del questionario di onboarding del carico di lavoro e del questiona rio di inserimento degli allarmi. Per ulteriori informazioni, consulta Questionari di onboarding del carico di lavoro e inserimen to degli allarmi in Incident Detection and Response (percorso di eccezione).	20 aprile 2026

Modifica	Descrizione	Data
Riferimenti architettonici aggiornati	Rimossi i riferimenti ai diagrammi di architettura e sostituiti con dettagli di architettura. Per ulteriori informazioni, consultare Architettura di rilevamento e risposta agli incidenti e Informazioni sui carichi di lavoro relativi al rilevamento e alla risposta agli incidenti.	31 marzo 2026
Carichi di lavoro integrati di test aggiornati in Incident Detection and Response	Sono state aggiunte informazioni sulla disabilitazione delle azioni di CloudWatch allarme prima di modificare lo stato dell'allarme durante il test. Per ulteriori informazioni, consulta Testa i carichi di lavoro integrati in Incident Detection and Response.	2 marzo 2026
Gestione aggiornata degli incidenti con Incident Detection and Response	Sono state aggiunte informazioni sul comportamento ricorrente degli allarmi e sul coinvolgimento del responsabile degli incidenti. Per ulteriori informazioni, consulta Gestione degli incidenti con Incident Detection and Response.	2 marzo 2026
Passaggi aggiornati nella sezione Utilizzare una funzione matematica metrica per sopprimere un allarme CloudWatch	Passaggi aggiornati nella sezione Utilizzare una funzione matematica metrica per sopprimere un allarme. CloudWatch Per ulteriori informazioni, consulta Sopprimi gli allarmi alla fonte dell'allarme.	3 febbraio 2026

Modifica	Descrizione	Data
È stato aggiunto il coreano come lingua supportata	È stato aggiunto il coreano come lingua supportata. Per ulteriori informazioni, consulta Disponibilità regionale per il rilevamento e la risposta agli incidenti.	22 gennaio 2026
È stato aggiunto il mandarino come lingua supportata	È stato aggiunto il mandarino come lingua supportata. Per ulteriori informazioni, consulta Disponibilità regionale per il rilevamento e la risposta agli incidenti.	13 gennaio 2026
Aggiunta una nuova sezione: AWS Incident Detection and Response Customer Command Line Interface	È stata aggiunta la sezione IDR CLI e aggiornato il capitolo Get started per includere informazioni sull'interfaccia a riga di comando AWS Incident Detection and Response Customer. Per ulteriori informazioni, consulta CLI for AWS Incident Detection and Response.	8 dicembre 2025
Diverse sezioni aggiornate: questionari sull'onboarding del carico di lavoro e sull'inserimento degli allarmi in Incident Detection and Response e Introduzione al rilevamento e risposta agli incidenti	Il processo di gestione Servizio AWS degli eventi non fa più parte di AWS Incident Detection and Response. Le sezioni di questa guida per l'utente sono state aggiornate per rimuovere i riferimenti a questo processo. Continuerai a ricevere notifiche sugli eventi di servizio tramite il AWS Service Health Dashboard. I clienti di AWS Incident Detection and Response possono utilizzare una richiesta Incident Response per ricevere assistenza durante gli eventi di servizio, se necessario. Per ulteriori informazioni, consulta Richiedi una risposta all'incidente.	14 ottobre 2025

Modifica	Descrizione	Data
Sezione eliminata: gestione degli incidenti per gli eventi di servizio	Il processo di gestione Servizio AWS degli eventi non fa più parte di AWS Incident Detection and Response. Questa sezione della guida per l'utente è stata rimossa per rifletter e questa modifica. Continuerai a ricevere notifiche sugli eventi di servizio tramite il AWS Service Health Dashboard. I clienti di AWS Incident Detection and Response possono utilizzare una richiesta Incident Response per ricevere assistenza durante gli eventi di servizio, se necessario. Per ulteriori informazi oni, consulta Richiedi una risposta all'incidente.	14 ottobre 2025
Sezione aggiornata: disponibi lità regionale per il rilevamento e la risposta agli incidenti	AWS Incident Detection and Response è ora disponibile in AWS GovCloud (US-East) e AWS GovCloud (US-West). Per ulteriori informazioni, consulta Disponibilità regionale per il rilevamen to e la risposta agli incidenti	5 ottobre 2025
Sezione aggiornata: questiona ri sull'onboarding del carico di lavoro e sull'inserimento degli allarmi in Incident Detection and Response	Indirizzo e-mail di esempio aggiornato per la tabella delle matrici di allarme.	26 agosto 2025
Sezione aggiornata: sottoscri vi un carico di lavoro ad AWS Incident Detection and Response	È stato rimosso il riferimento al campo della data di inizio dell'abbonamento nella sezione Descrizione della finestra Crea caso. Sezione aggiornata: sottoscrivi un carico di lavoro ad AWS Incident Detection and Response	4 agosto 2025

Modifica	Descrizione	Data
Nuova funzione: elimina gli allarmi utilizzando Incident Detection and Response	Sono state aggiunte nuove sezioni ai carichi di lavoro gestiti che forniscono informazioni su come sopprimere gli allarmi temporaneamente o in base a una pianificazione Nuova sezione: Sopprimi gli allarmi attivando il rilevamento e la risposta agli incidenti	9 aprile 2025
Istruzioni aggiornate per Request an Incident Response utilizzando il AWS Support Center Console	Sono stati aggiunti dettagli sulle informazioni da inserire nel campo Descrizione del problema. Sezione aggiornata: Richiedi una risposta all'incidente	6 febbraio 2025
Regioni AWS Aggiunto altro	Sono Regioni AWS stati aggiunti altri elementi alla sezione sulla disponibilità di Incident Detection and Response. Sezione aggiornata: Disponibilità regionale per il rilevamento e la risposta agli incidenti	1 novembre 2024
Aggiornamenti ai casi di supporto relativi alla gestione del rilevamento e della risposta agli incidenti con la AWS Support App in Slack pagina	Pagina spostata in Incident Management, testo modificato e schermate sostituite. Sezione aggiornata: Gestisci i casi di supporto per il rilevamento e la risposta agli incidenti con AWS Support App in Slack	10 ottobre 2024
Aggiunta una nuova pagina AWS Support App in Slack Gestione aggiornata degli incidenti con AWS Incident Detection and Response	È stata aggiunta una nuova pagina per AWS Support App in Slack Gestione degli incidenti aggiornata con AWS Incident Detection and Response per aggiunger e una nuova sezione, «Richiedi una risposta agli incidenti utilizzando AWS Support App in Slack».	10 settembre 2024

Modifica	Descrizione	Data
Abbonamento aggiornato all'account	È stata aggiornata la sezione Abbonamento all'account per includere dettagli su dove aprire una richiesta di assistenza quando si richiede di sottoscrivere un account. Sezione aggiornata: sottoscrivi un carico di lavoro ad AWS Incident Detection and Response	12 giugno 2024
Aggiunta una nuova sezione: Offboard a workload	È stata aggiunta la sezione Offload a workload in Guida introduttiva per includere informazioni sui carichi di lavoro di offboarding Per ulteriori informazioni, consulta Elimina un carico di lavoro da Incident Detection and Response.	28 marzo 2024
Abbonamento aggiornato all'account	È stata aggiornata la sezione Abbonamento all'account per includere informazioni sui carichi di lavoro relativi all'offboarding Per ulteriori informazioni, consulta Sottoscrivere un carico di lavoro ad AWS Incident Detection and Response	28 marzo 2024
Test aggiornati	È stata aggiornata la sezione Test per includere informazioni sui test del giorno di gioco come ultima fase del processo di onboarding. Sezione aggiornata: Testa i carichi di lavoro integrati in Incident Detection and Response	29 febbraio 2024
Aggiornato Cos'è AWS Incident Detection and Response	È stata aggiornata la sezione Cos'è AWS Incident Detection and Response. Sezione aggiornata: Cos'è AWS Incident Detection and Response?	19 febbraio 2024

Modifica	Descrizione	Data
Sezione Questionario aggiornata	È stato aggiornato il questionario di onboarding del carico di lavoro e aggiunto il questionario di inserimento degli allarmi. La sezione è stata rinominata da Questionario di onboarding a Questionari di onboarding del carico di lavoro e Alarm ingestion.	2 febbraio 2024
Informazioni AWS aggiornate sugli eventi di servizio e sull'onboarding	Sono state aggiornate diverse sezioni con nuove informazioni per l'onboarding. Sezioni aggiornate: • Incorpora i carichi di lavoro al rilevamento e alla risposta agli incidenti • Sottoscrivi un carico di lavoro ad AWS Incident Detection and Response Nuove sezioni • Fornire l'accesso a AWS Support Center Console per i team applicativi	31 gennaio 2024
È stata aggiunta una sezione di informazioni correlate	È stata aggiunta una sezione di informazioni correlate nel provisioning degli accessi. Sezione aggiornata: Fornisci l'accesso per l'inserimento degli allarmi alla funzione Incident Detection and Response	17 gennaio 2024
Passaggi di esempio aggiornati	È stata aggiornata la procedura per i passaggi 2,3 e 4 in Esempio: integrazione delle notifiche da Datadog e Splunk. Sezione aggiornata: Esempio: integrazione delle notifiche da Datadog e Splunk	21 dicembre 2023

Modifica	Descrizione	Data
Grafica e testo introduttivi aggiornati	Grafica aggiornata negli allarmi Ingest dagli APM che hanno l'integrazione diretta con Amazon. EventBridge Sezione aggiornata: Sviluppa runbook e piani di risposta per rispondere a un incidente in Incident Detection and Response	21 dicembre 2023
Modello di runbook aggiornato	È stato aggiornato il modello di runbook in Developing runbook for AWS Incident Detection and Response. Sezione aggiornata: Sviluppa runbook e piani di risposta per rispondere a un incidente in Incident Detection and Response	04 dicembre 2023
Configurazioni di allarme aggiornate	Configurazioni di allarme aggiornate con informazioni dettagliate sulla configurazione degli CloudWatch allarmi. Nuova sezione: Crea CloudWatch allarmi adatti alle tue esigenze aziendali in materia di rilevamento e risposta agli incidenti Nuova sezione: crea CloudWatch allarmi in Incident Detection and Response con modelli CloudFormation Nuova sezione: esempi di casi d'uso per gli CloudWatch allarmi in Incident Detection and Response	28 settembre 2023

Modifica	Descrizione	Data
Aggiornamento: Guida introduttiva	Guida introduttiva aggiornata con informazioni sulle richieste di modifica del carico di lavoro. Nuova sezione: Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response Sezione aggiornata: sottoscrivi un carico di lavoro ad AWS Incident Detection and Response	05 settembre 2023
Nuova sezione in Guida introduttiva	Aggiunti avvisi di importazione in AWS Incident Detection and Response.	30 giugno 2023
Documento originale	AWS Incident Detection and Response pubblicato per la prima volta	15 marzo 2023

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.