Concetti e procedure di rilevamento e risposta agli incidenti di AWS

Guida per l'utente di AWS Incident Detection and Response

Version December 8, 2025

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 degli 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: gli Incident Management Engineer (IMEs) monitorano i carichi di lavoro integrati 24 ore su 24, 7 giorni su 7 per rilevare incidenti critici. IMEs Risponde entro 5 minuti dall'attivazione di un allarme o in risposta a un caso di supporto critico per l'azienda da te segnalato a Incident Detection and Response.
- Risoluzione più rapida: IMEs utilizza runbook predefiniti e personalizzati sviluppati per i tuoi carichi di lavoro per rispondere entro 5 minuti, creare un caso di Support per tuo conto e gestire gli incidenti sul tuo carico di lavoro. IMEs garantisci la gestione degli incidenti in un unico thread e mantieni il contatto con gli esperti giusti fino alla loro risoluzione. AWS
- Riduzione del rischio di guasto: dopo la risoluzione, IMEs 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

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 Enterprise Support diretti e rivenduti dai partner.
- 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 diagrammi dell'architettura dei carichi di lavoro, dettagli sugli allarmi e i relativi runbook di gestione degli incidenti nei AWS Systems Manager documenti (per i dettagli, consulta Documenti).AWS Systems Manager Per saperne di più, consulta What is AWS Systems Manager.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
Architettura	Responsabile	Responsabile
Operazioni	Responsabile	Responsabile
Determina CloudWatch gli allarmi da configurare	Responsabile	Responsabile
Definisci un piano di risposta agli incidenti	Responsabile	Responsabile
Completamento del questionario di onboarding	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
CloudWatch Allarmi di prova	Responsabile	Responsabile
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
Revisione post-incidente		

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 attualmente disponibile in inglese e giapponese per gli account 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 Pacific (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 Pacific (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacifico (Malesia)	ap-southeast-5
Africa (Cape Town)	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 (Stati Uniti orientali)	us-gov-east-1
AWS GovCloud (Stati Uniti occidentali)	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 rapidamente 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.

Carichi di lavoro

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 in uno o piùAWS 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.

Per iniziare con l'onboarding del carico di lavoro, consulta Workload Onboarding e Workload Onboarding Questionnaire.

Allarmi

Gli allarmi sono una parte fondamentale del rilevamento e della risposta agli incidenti, in quanto forniscono visibilità sulle prestazioni delle applicazioni e dell'infrastruttura sottostante.AWSAWS collabora con voi per definire metriche e soglie di allarme appropriate che si attivano solo in caso di impatto critico sui carichi di lavoro monitorati. L'obiettivo è far sì che gli allarmi coinvolgano i risolutori specificati, che possono quindi collaborare con il team di gestione degli incidenti per mitigare rapidamente eventuali problemi. Gli allarmi devono essere configurati in modo da entrare 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 con l'inserimento degli allarmi, consulta la sezione Inserimento degli allarmi e Questionario sull'inserimento degli allarmi.

> **Note**
>
> Per apportare modifiche ai runbook, alle informazioni sul carico di lavoro o agli allarmi monitorati su AWS Incident Detection and Response, consulta. Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response

Introduzione al rilevamento e alla risposta agli incidenti

AWS collabora con te per integrare il carico di lavoro e gli allarmi in AWS Incident Detection and Response. Fornisci informazioni chiave AWS sul tuo carico di lavoro e sugli allarmi che desideri integrare utilizzando lo strumento Incident Detection and Response Customer Command Line Interface (CLI) o nel. Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response

Il diagramma seguente mostra il flusso per l'onboarding del carico di lavoro e l'inserimento degli allarmi in Incident Detection and Response:

Onboarding del carico di lavoro

Durante l'onboarding del carico di lavoro,AWS collabora con te per comprendere il carico di lavoro e come supportarti durante gli incidenti. Fornisci informazioni chiave sul tuo carico di lavoro che aiutano a mitigare l'impatto.

Risultati chiave:

- Informazioni generali sul carico di lavoro
- Dettagli sull'architettura, inclusi i diagrammi

- Informazioni sul runbook
- Incidenti avviati dal cliente

Ingestione degli allarmi

AWS collabora con te per integrare i tuoi allarmi. AWS Incident Detection and Response può importare allarmi da Amazon CloudWatch e strumenti di monitoraggio delle prestazioni delle applicazioni (APM) di terze parti tramite Amazon. EventBridge Gli allarmi di onboarding consentono il rilevamento proattivo degli incidenti e il coinvolgimento automatico. Per ulteriori informazioni, consulta Ingestisci allarmi APMs che hanno un'integrazione diretta con Amazon. EventBridge

Risultati chiave:

- Matrice di allarme

La tabella seguente elenca i passaggi necessari per effettuare l'onboarding di un carico di lavoro in AWS Incident Detection and Response. Questa tabella mostra esempi di durate di ogni attività. Le date effettive per ogni attività sono definite in base alla disponibilità del team e alla pianificazione.

Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response

Questa pagina 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 dovrebbero innescare la creazione di incidenti in Incident Detection and Response per il tuo carico di lavoro, oltre a informazioni di 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.

Scarica il questionario sull'ingestione degli allarmi.

Questionario sull'onboarding del carico di lavoro - Domande generali

Domande generali

Domanda	Risposta di esempio
Nome dell'azienda	Amazon Inc.
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.
Requisiti and/or normativi di conformità applicabili per questo carico di lavoro e qualsiasi azione richiesta AWS dopo un incidente.	Il carico di lavoro riguarda le cartelle cliniche dei pazienti, che devono essere mantenute protette e riservate.

Questionario di onboarding sul 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	Nome app: Optimax ambiente: Produzione

Domanda	Risposta di esempio
tag, tutte le risorse utilizzate da questo carico di lavoro devono avere gli stessi tag.	
Un elenco dei AWS servizi utilizzati da questo carico di lavoro e degli AWS account e delle regioni in cui si trovano. **Note** Crea una nuova riga per ogni servizio.	Route 53: indirizza il traffico Internet verso l'ALB. Conto: 123456789101 Regione: US-EAST-1, US-WEST-2
Un elenco dei AWS servizi utilizzati da questo carico di lavoro con l'AWS account e le aree geografiche in cui si trovano. **Note** Crea una nuova riga per ogni servizio.	ALB: indirizza il traffico in entrata verso un gruppo target di contenitori ECS. Conto: 123456789101 Regione: N/A
Un elenco dei AWS servizi utilizzati da questo carico di lavoro e degli AWS account e delle aree in cui si trovano. **Note** Crea una nuova riga per ogni servizio.	ECS: infrastruttura di calcolo per la principale flotta di logica aziendale. Responsabile della gestione delle richieste degli utenti in arrivo e dell'invio di query al livello di persistenza. Conto: 123456789101 Regione: US-EAST-1

Domanda	Risposta di esempio
Un elenco dei AWS servizi utilizzati da questo carico di lavoro e degli AWS account e delle regioni in cui si trovano. **Note** Crea una nuova riga per ogni servizio.	RDS: il cluster Amazon Aurora archivia i dati degli utenti a cui si accede tramite il livello di logica aziendale ECS. Account: 123456789101 Regione: US-EAST-1
Un elenco dei AWS servizi utilizzati da questo carico di lavoro e degli AWS account e delle regioni in cui si trovano. **Note** Crea una nuova riga per ogni servizio.	S3: memorizza le risorse statiche del sito Web. Conto: 123456789101 Regione: N/A
upstream/downstream Descrivi in dettaglio tutti i componenti non integrati che potrebber o influire su questo carico di lavoro in caso di interruzione.	Microservizio di autenticazione: impedirà agli utenti di caricare le proprie cartelle cliniche poiché non saranno autenticate.
Esistono componenti locali o non per questo carico di lavoro?AWS In caso affermativo, quali sono e quali funzioni vengono eseguite?	Tutto il traffico basato su Internet in/out di AWS viene instradato tramite il nostro servizio proxy locale.
Fornisci i dettagli di eventuali piani di failover/ disaster ripristino manuali o automatizzati nella zona di disponibilità e a livello regionale.	Standby a caldo. Failover automatico su US-WEST-2 durante un calo sostenuto della percentuale di successo.

Questionario sull'ingestione degli allarmi

Domande sul runbook

Domanda	Risposta di esempio
AWS coinvolgerà i contatti del carico di lavoro tramite il Supporto Case. 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

Domanda	Risposta di esempio
AWS comunica gli aggiornamenti tramite il caso di supporto a intervalli regolari durante l'incidente. Esistono altri contatti che dovrebbero ricevere questi aggiornamenti?	john.smith@example.com, jane.smith@example.com

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 rilevamento e risposta agli incidenti di AWS per le violazioni dei criteri:

Questi criteri possono essere valutati solo in case-by-case base al verificarsi degli eventi. Il team di gestione degli incidenti collabora con i vostri account manager tecnici (TAMs) per regolare gli allarmi e, in rari casi, disabilitare il monitoraggio se si sospetta che gli allarmi dei clienti non rispettino questi criteri e coinvolge 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

Nome della metrica/ARN/Threshold	Description	Note	Azioni richieste
Volume del carico di lavoro/ *CW Alarm ARN* / CallCount < 100000 per 5 punti dati entro 5 minuti, considera i dati mancanti come mancanti	Questa metrica rappresenta il numero di richieste in entrata che arrivano al carico di lavoro, misurato a livello di Application Load Balancer. Questo allarme è importante perché un calo significativo delle richieste in entrata può indicare problemi con la connettività di rete upstream o problemi con la nostra implementazione DNS che impediscono agli utenti di accedere al carico di lavoro.	L'allarme è entrato nello stato «Allarme» 10 volte nell'ultima settimana. Questo allarme è a rischio di falsi positivi. È prevista la revisione della soglia. Problemi? No o Sì (se No, lascia vuoto): questo allarme si attiva frequentemente durante l'esecuzione di un particolare processo in batch. Risolutori: tecnici addetti all'affidabilità del sito	Coinvolgete il team di Site Reliability Engineering inviando un'e-mail a *SRE@example.com* Crea un Supporto AWS caso per i nostri servizi ELB e Amazon Route 53. Se è necessaria un'azione IMMEDIATA: seleziona memory/disk Spazio EC2 libero e informa il *Example* team tramite e-mail di riavviare l'istanza , oppure esegui un log flush. (se non è necessaria un'azione

Nome della metrica/ARN/Threshold	Description	Note	Azioni richieste
			immediata, lascia vuoto)
Latenza delle richieste del carico di lavoro/ *CW Alarm ARN* / p90 Latenza > 100 ms per 5 punti dati entro 5 minuti, considera i dati mancanti come mancanti	Questa metrica rappresenta la latenza p90 per le richieste HTTP che devono essere soddisfatte dal carico di lavoro. Questo allarme rappresenta la latenza (misura important e dell'esperienza del cliente per il sito Web).	L'allarme è entrato nello stato «Allarme» 0 volte nell'ultima settimana. Problemi? No o Sì (se No, lascia vuoto): questo allarme si attiva frequentemente durante l'esecuzione di un particolare processo in batch. Risolutori: tecnici addetti all'affidabilità del sito	Coinvolgete il team di Site Reliability Engineering inviando un'e-mail a *SRE@example.com* Crea un Supporto AWS caso per i nostri servizi ECW e RDS. Se è necessaria un'azione IMMEDIATA: seleziona memory/disk Spazio EC2 libero e informa il *Example* team tramite e-mail di riavviare l'istanza , oppure esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)

Nome della metrica/ARN/Threshold	Description	Note	Azioni richieste
Disponibilità della richiesta del carico di lavoro/ *CW Alarm ARN* / Disponibilità < 95% per 5 punti dati entro 5 minuti, considera i dati mancanti come mancanti.	Questa metrica rappresenta la disponibilità delle richieste HTTP che devono essere soddisfatte dal carico di lavoro. (numero di HTTP 200/ numero di richieste) per periodo. Questo allarme rappresenta la disponibilità del carico di lavoro.	L'allarme è entrato nello stato «Allarme» 0 volte nell'ultima settimana. Problemi? No o Sì (se No, lascia vuoto): questo allarme si attiva frequentemente durante l'esecuzione di un particolare processo in batch. Risolutori: tecnici addetti all'affidabilità del sito	Coinvolgete il team di Site Reliability Engineering inviando un'e-mail a *SRE@example.com* Crea un Supporto AWS caso per i nostri servizi ELB e Amazon Route 53. Se è necessaria un'azione IMMEDIATA: seleziona memory/disk Spazio EC2 libero e informa il *Example* team tramite e-mail di riavviare l'istanza , oppure esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)
Esempio di New Relic Alarm			

Nome della metrica/ARN/Threshold	Description	Note	Azioni richieste
Test di integrazione dall'inizio alla fine/ *CW Alarm ARN* / Percentuale di errore del 3% per metriche di 1 minuto su una durata di 3 minuti, considera i dati mancanti come mancanti Identificatore del carico di lavoro: Workflow di test end-to-end,: US-EAST-1, ID Regione AWS: 012345678910 Account AWS	Questa metrica verifica se una richiesta può attraversare ogni livello del carico di lavoro. Se questo test fallisce, rappresenta un errore critico nell'elaborazione delle transazioni commerciali. Questo allarme rappresenta la capacità di elaborare transazioni commerciali per il carico di lavoro.	L'allarme è entrato nello stato «Allarme» 0 volte nell'ultima settimana. Problemi? No o Sì (se No, lascia vuoto): questo allarme si attiva frequentemente durante l'esecuzione di un particolare processo in batch. Risolutori: tecnici addetti all'affidabilità del sito	Coinvolgete il team di Site Reliability Engineering inviando un'e-mail a *SRE@example.com* Crea un Supporto AWS caso per i nostri servizi Amazon Elastic Container Service e Amazon DynamoDB. Se è necessaria un'azione IMMEDIATA: seleziona memory/disk Spazio EC2 libero e informa il *Example* team tramite e-mail di riavviare l'istanza oppure esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)

Individuazione del carico di lavoro nel rilevamento e nella risposta agli incidenti

AWS collabora con te per comprendere il più possibile il contesto del tuo carico di lavoro. AWS Incident Detection and Response utilizza queste informazioni per creare runbook che ti supportino

durante gli incidenti. Le informazioni richieste vengono acquisite in. Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response È consigliabile registrare i carichi di lavoro su AppRegistry. Per ulteriori informazioni, consulta la Guida per l'utente AppRegistry .

Risultati chiave:

- Informazioni sul carico di lavoro, come la descrizione del carico di lavoro, i diagrammi dell'architettura, i dettagli dei contatti e dell'escalation.
- Dettagli su come il carico di lavoro utilizza i servizi in ciascuna regione.AWSAWS
- Allarmi utilizzati dal team per rilevare l'impatto critico del carico di lavoro.

Abbonati un carico di lavoro a Incident Detection and Response

Crea un caso di supporto per ogni carico di lavoro a cui desideri abbonare ad AWS Incident Detection and Response.

- Per i carichi di lavoro con un solo account: invia i dati dall'account del carico di lavoro o dal tuo account di pagamento.
- Per carichi di lavoro con più account: invia i dati dal tuo account di pagamento ed elenca tutti gli account. IDs

> **Important**
>
> L'invio di una richiesta di assistenza dall'account sbagliato per iscrivere un carico di lavoro a Incident Detection and Response potrebbe causare ritardi e richiedere informazioni aggiuntive.

Per sottoscrivere un carico di lavoro, completa i seguenti passaggi:

1. Apri il Supporto AWS Centro, quindi seleziona Crea caso. È possibile sottoscrivere carichi di lavoro solo da account registrati in Enterprise Support. L'esempio seguente mostra la console Support Center.

2. Per completare il modulo di richiesta di assistenza, inserisci le seguenti informazioni:

- Seleziona Supporto tecnico.
- Per Assistenza, scegli Incident Detection and Response.
- Per Categoria, scegli Nuovo carico di lavoro integrato.
- Per Severità, scegli Guida generale.

3. Inserisci un oggetto per questa modifica. Ad esempio, potresti inserire [Onboard] AWS Incident Detection and Response - *`workload_name`*.
4. Inserisci una descrizione per questa modifica. Ad esempio, puoi inserire This request is to onboard a workload 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. Questi sono gli account che desideri integrare in AWS Incident Detection and Response
   - Lingua: inglese o giapponese
5. Nella sezione Contatti aggiuntivi - opzionale, inserisci l'e-mail a IDs cui desideri ricevere la corrispondenza relativa a questa richiesta.

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

   > **Important**
   >
   > La mancata aggiunta di e-mail IDs nella sezione Contatti aggiuntivi - opzionale potrebbe ritardare il processo di onboarding di AWS Incident Detection and Response.

6. Seleziona Invia.

   Dopo aver inviato la richiesta, puoi aggiungere altre e-mail dalla tua organizzazione. Per aggiungere e-mail, rispondi al caso, quindi aggiungi l'e-mail IDs nella sezione Contatti aggiuntivi - opzionale.

   Di seguito è riportato un esempio del pulsante Rispondi e della sezione Contatti aggiuntivi - opzionale.

Dopo aver creato una richiesta di assistenza per la richiesta di abbonamento, tieni pronti i due documenti seguenti per procedere con il processo di onboarding del carico di lavoro:

- AWS diagramma dell'architettura del carico di lavoro.
- Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response: completa tutte le informazioni del questionario relative al carico di lavoro per il quale stai effettuando l'onboarding. Se hai più carichi di lavoro da integrare, crea un nuovo questionario di onboarding per ogni carico di lavoro. Se hai domande sulla compilazione del questionario di onboarding, contatta il tuo Technical Account Manager (TAM).

> **Note**
>
> NON allegate questi due documenti alla custodia utilizzando l'opzione Allega file. Il team di AWS Incident Detection and Response risponderà al caso con un link di caricamento di Amazon Simple Storage Service per consentirti di caricare i documenti.

Per informazioni su come creare un caso con AWS Incident Detection and Response per richiedere modifiche a un carico di lavoro integrato esistente, consulta. Richiedi modifiche a un carico di lavoro integrato in Incident Detection and Response Per informazioni su come effettuare l'offboard di un carico di lavoro, consulta. Elimina un carico di lavoro da Incident Detection and Response

Definisci e configura gli allarmi in Incident Detection and Response

AWS collabora con te per definire metriche e allarmi per fornire visibilità sulle prestazioni delle tue applicazioni e della loro infrastruttura sottostante AWS. Chiediamo che gli allarmi rispettino i seguenti criteri durante la definizione e la configurazione delle soglie:

- Gli allarmi entrano nello stato «Allarme» solo quando si verifica un impatto critico sul carico di lavoro monitorato (perdita di ricavi o peggioramento dell'esperienza del cliente che riduce significativamente le prestazioni) che richiede l'attenzione immediata dell'operatore.
- Gli allarmi devono inoltre coinvolgere i risolutori specificati per il carico di lavoro contemporaneamente o prima di coinvolgere il team di gestione degli incidenti. I tecnici addetti alla gestione degli incidenti devono collaborare con i risolutori specificati nel processo di mitigazione, non fungere da soccorritori di prima linea e poi rivolgersi a voi.

- Le soglie di allarme devono essere impostate su una soglia e una durata appropriate in modo che ogni volta che scatta un allarme, sia necessaria un'indagine. Se un allarme oscilla tra lo stato «Allarme» e «OK», si verifica un impatto sufficiente a giustificare la risposta e l'attenzione dell'operatore.

Tipi di allarmi:

- Allarmi che illustrano il livello di impatto aziendale e trasmettono informazioni pertinenti per una semplice rilevazione dei guasti.
- CloudWatch Canarini Amazon. Per ulteriori informazioni, vedere Canaries and X-Ray tracing e X-Ray.
- Allarme aggregato (monitoraggio delle dipendenze)

La tabella seguente fornisce esempi di allarmi, tutti basati sul sistema di monitoraggio. CloudWatch

Nome della metrica/Soglia di allarme	ARN di allarme o ID della risorsa	Se questo allarme si attiva	Se richiesto, chiudi un Premium Support Case per questi servizi
Errori API/ Numero di errori >= 10 per 10 punti dati	arn:aws:cloudwatch:us-west- 2:000000000000:alarm:E2 Lambda-Errors MPmim	Ticket inviato al team di amministratori del database (DBA)	Lambda, API Gateway
ServiceUnavailable (Codice di stato Http 503)	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	Ticket consegnato al team di	Lambda, API Gateway

Nome della metrica/Soglia di allarme	ARN di allarme o ID della risorsa	Se questo allarme si attiva	Se richiesto, chiudi un Premium Support Case per questi servizi
Numero di errori >=3 per 10 punti dati (client diversi) in una finestra di 5 minuti		assistenza	
ThrottlingException (Codice di stato Http 400) Numero di errori >=3 per 10 punti dati (client diversi) in una finestra di 5 minuti	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	Ticket consegnato al team di assistenza	EC2, Amazon Aurora

Per ulteriori dettagli, consultare Monitoraggio e osservabilità di AWS Incident Detection and Response.

Se preferisci utilizzare strumenti di automazione per integrare gli allarmi, l'interfaccia CLI (Incident Detection and Response Command Line Interface) ti aiuta a implementare e integrare gli allarmi. Per ulteriori dettagli, consultare CLI AWS per il rilevamento e la risposta agli incidenti.

Risultati chiave:

- Definizione e configurazione degli allarmi sui carichi di lavoro.
- Completamento dei dettagli degli allarmi nel questionario di onboarding.

Argomenti

- Crea CloudWatch allarmi adatti alle tue esigenze aziendali in Incident Detection and Response

- Crea CloudWatch allarmi in Incident Detection and Response con modelli CloudFormation
- Esempi di casi d'uso degli CloudWatch allarmi in Incident Detection and Response

Crea CloudWatch allarmi adatti alle tue esigenze aziendali in Incident Detection and Response

Quando crei CloudWatch allarmi Amazon, puoi eseguire diversi passaggi per assicurarti che gli allarmi soddisfino al meglio le tue esigenze aziendali.

> **Note**
>
> Per alcuni esempi di CloudWatch allarmi consigliati Servizi AWS da integrare in Incident Detection and Response, consulta le Best Practices per il rilevamento e la risposta agli allarmi di risposta agli incidenti su.AWS re:Post

Esamina gli allarmi proposti CloudWatch

Esamina gli allarmi proposti per assicurarti che entrino nello stato «Allarme» solo quando c'è un impatto critico sul carico di lavoro monitorato (perdita di ricavi o peggioramento dell'esperienza del cliente che riduce significativamente le prestazioni). Ad esempio, ritenete che questo allarme sia sufficientemente importante da dover reagire immediatamente se entra nello stato «Allarme»?

Di seguito sono riportate le metriche suggerite che potrebbero rappresentare un impatto aziendale critico, ad esempio influire sull'esperienza degli utenti finali con un'applicazione:

- CloudFront: Per ulteriori informazioni, consulta Visualizzazione CloudFront e metriche delle funzioni edge.
- Application Load Balancer: è consigliabile creare i seguenti allarmi per Application Load Balancers, se possibile:
  - HTTPCode_ELB_5xx_Count
  - HTTPCode_Target_5xx_Count

  Gli allarmi precedenti consentono di monitorare le risposte dei target che si trovano dietro l'Application Load Balancer o ad altre risorse. Ciò semplifica l'identificazione della fonte degli errori 5XX. Per ulteriori informazioni, consulta le CloudWatch metriche per il tuo Application Load Balancer.

- Amazon API Gateway: se utilizzi l' WebSocket API in Elastic Beanstalk, prendi in considerazione l'utilizzo delle seguenti metriche:
  - Tassi di errore di integrazione (filtrati fino a 5XX errori)
  - Latenza di integrazione
  - Errori di esecuzione

  Per ulteriori informazioni, consulta Monitoraggio dell'esecuzione delle WebSocket API con CloudWatch metriche.
- Amazon Route 53: monitora la EndPointUnhealthyENICountmetrica. Questa metrica indica il numero di interfacce di rete elastiche nello stato di ripristino automatico. Questo stato indica i tentativi del resolver di ripristinare una o più interfacce di rete Amazon Virtual Private Cloud associate all'endpoint (specificato da). EndpointId Nel processo di ripristino, l'endpoint funziona con una capacità limitata. L'endpoint non può elaborare le query DNS finché non viene completamente ripristinato. Per ulteriori informazioni, consulta Monitoraggio degli endpoint Amazon Route 53 Resolver con Amazon. CloudWatch

Convalida le configurazioni degli allarmi

Dopo aver verificato che gli allarmi proposti soddisfino le esigenze aziendali, convalida la configurazione e la cronologia degli allarmi:

- Convalida la soglia per la metrica per accedere allo stato «Allarme» rispetto all'andamento del grafico della metrica.
- Convalida il periodo utilizzato per i punti dati di polling. I dati di sondaggio a 60 secondi aiutano a rilevare precocemente gli incidenti.
- Convalida la configurazione. DatapointToAlarm Nella maggior parte dei casi, è consigliabile impostarlo su 3 su 3 o 5 su 5. In caso di incidente, l'allarme si attiva dopo 3 minuti se impostato come [metriche di 60 secondi con 3 su 3 DatapointToAlarm] o 5 minuti se impostato come [metriche di 60 secondi con 5 su 5]. DatapointToAlarm Utilizzate questa combinazione per eliminare gli allarmi rumorosi.

> **Note**
>
> I consigli precedenti potrebbero variare a seconda di come si utilizza un servizio. Ogni AWS servizio funziona in modo diverso all'interno di un carico di lavoro. Inoltre, lo stesso servizio

potrebbe funzionare in modo diverso se utilizzato in più luoghi. È necessario assicurarsi di comprendere in che modo il carico di lavoro utilizza le risorse che alimentano l'allarme, nonché gli effetti a monte e a valle.

Verifica il modo in cui i tuoi allarmi gestiscono i dati mancanti

Alcune fonti metriche non inviano dati a CloudWatch intervalli regolari. Per queste metriche, è consigliabile considerare i dati mancanti come NotBreach. Per ulteriori informazioni, consulta Configurazione del modo in cui gli CloudWatch allarmi trattano i dati mancanti e Evitare transizioni premature allo stato di allarme.

Ad esempio, se una metrica monitora un tasso di errore e non vi sono errori, la metrica non riporta alcun dato (zero). Se configuri l'allarme in modo che i dati mancanti vengano considerati mancanti, un singolo punto dati di violazione seguito da due punti dati privi di dati (nulli) fa sì che la metrica passi allo stato «Allarme» (per 3 punti dati su 3). Questo perché la configurazione dei dati mancanti valuta l'ultimo punto dati noto nel periodo di valutazione.

Nei casi in cui le metriche monitorano un tasso di errore, in assenza di un peggioramento del servizio si può presumere che l'assenza di dati sia una buona cosa. È consigliabile considerare i dati mancanti come NotBreach in modo che i dati mancanti vengano trattati come «OK» e la metrica non entri nello stato «Alarm» su un singolo punto dati.

Rivedi la cronologia di ogni allarme

Se la cronologia di un allarme mostra che spesso entra nello stato «Allarme» e poi si ripristina rapidamente, l'allarme potrebbe diventare un problema per te. Assicurati di regolare l'allarme per evitare rumori o falsi allarmi.

Convalida le metriche per le risorse sottostanti

Assicurati che le tue metriche prendano in considerazione risorse sottostanti valide e utilizzino le statistiche corrette. Se un allarme è configurato per esaminare i nomi delle risorse non validi, l'allarme potrebbe non essere in grado di tenere traccia dei dati sottostanti. Ciò potrebbe far sì che l'allarme entri nello stato «Allarme».

Crea allarmi compositi

Se offri alle operazioni di rilevamento e risposta agli incidenti un gran numero di allarmi per l'onboarding, ti potrebbe essere chiesto di creare allarmi compositi. Gli allarmi compositi riducono il numero totale di allarmi che devono essere integrati.

Crea CloudWatch allarmi in Incident Detection and Response con modelli CloudFormation

AWS Fornisce modelli per accelerare l'onboarding verso AWS Incident Detection and Response e ridurre lo sforzo necessario per creare allarmi.CloudFormation Questi modelli includono impostazioni di allarme ottimizzate per i servizi di bordo più comuni, come Application Load Balancer, Network Load Balancer e Amazon. CloudFront

Crea allarmi con modelli CloudWatch CloudFormation

1. Scarica un modello utilizzando i link forniti:

NameSpac	Metriche	ComparisonOperator (Soglia)	Periodo	DatapointsToAlarm	TreatMissingData	Statistic	Link al modello
Applicazione Elastic Load Balancer	(m1+m2)/(m1+m2+mm4) *100 m1=_Target_2xx_Count m2=_Target_3xx_Count m3=_Target_4xx_Count m4=_Target_5	LessThanThreshold(95)	60	3 su 3	perso	Somma	Template (Modello)

NameSpac	Metriche	ComparisonOperator (Soglia)	Periodo	DatapointsToAlarm	TreatMissingData	Statistic	Link al modello
	xx_count HTTPCode HTTPCode HTTPCode HTTPCode						
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3 su 3	Non violare	Media	Template (Modello)
Applicazione Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 su 3	Non violare	Massimo	Template (Modello)
Elastic Load Balancer di rete	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 su 3	Non violare	Massimo	Template (Modello)

2. Controlla il file JSON scaricato per assicurarti che soddisfi i processi operativi e di sicurezza della tua organizzazione.
3. Crea uno CloudFormation stack:

> **Note**
>
> I passaggi seguenti utilizzano il processo di creazione dello CloudFormation stack standard. Per i passaggi dettagliati, vedi Creazione di uno stack sulla CloudFormation console.

   a. Apri la AWS CloudFormation console in https://console.aws.amazon.com/cloudformation.
   b. Seleziona Crea stack.

c. Scegli Template is ready, quindi carica il file del modello dalla cartella locale.

   Di seguito è riportato un esempio della schermata Create stack.

d. Scegli Next (Successivo).

e. Immetti le seguenti informazioni necessarie:

   - AlarmNameConfige AlarmDescriptionConfig: inserisci un nome e una descrizione per la sveglia.

   - ThresholdConfig: Modifica il valore della soglia per soddisfare i requisiti dell'applicazione.

   - Distribuzione IDConfig: assicurati che l'ID di distribuzione indichi le risorse corrette nell'account in cui stai creando lo CloudFormation stack.

f. Scegli Next (Successivo).

g. Controlla i valori predefiniti nei DatapointsToAlarmConfigcampi PeriodConfigEvalutionPeriodConfig, e. È consigliabile utilizzare i valori predefiniti per questi campi. È possibile apportare modifiche, se necessario, per soddisfare i requisiti dell'applicazione.

h. Se necessario, inserisci i tag e le informazioni di notifica SNS. È consigliabile attivare la protezione dalla terminazione per evitare la cancellazione accidentale dell'allarme. Per attivare la protezione dalla terminazione, seleziona il pulsante di opzione Attivato, come mostrato nell'esempio seguente:

i. Scegli Next (Successivo).

j. Controlla le impostazioni dello stack, quindi scegli Crea stack.

k. Dopo aver creato lo stack, l'allarme viene visualizzato nell'elenco Amazon CloudWatch Alarm, come mostrato nell'esempio seguente:

4. Dopo aver creato tutti gli allarmi nell'account e nella AWS regione corretti, invia una notifica al Technical Account Manager (TAM). Il team di AWS Incident Detection and Response esamina lo stato dei nuovi allarmi, quindi continua l'onboarding.

Esempi di casi d'uso degli CloudWatch allarmi in Incident Detection and Response

I seguenti casi d'uso forniscono esempi di come utilizzare gli CloudWatch allarmi Amazon in Incident Detection and Response. Questi esempi dimostrano come è possibile configurare gli CloudWatch allarmi per monitorare le metriche e le soglie chiave di vari AWS servizi, consentendoti di identificare e rispondere a potenziali problemi che potrebbero influire sulla disponibilità e sulle prestazioni delle applicazioni e dei carichi di lavoro.

Esempio di utilizzo A: Application Load Balancer

È possibile creare il seguente CloudWatch allarme che segnala il potenziale impatto sul carico di lavoro. Per fare ciò, si crea una metrica matematica che avvisa quando le connessioni riuscite scendono al di sotto di una certa soglia. Per le metriche disponibili, consulta CloudWatch le CloudWatch metriche per il tuo Application Load Balancer

Metrica: `HTTPCode_Target_3XX_Count;HTTPCode_Target_4XX_Count;HTTPCode_Target_5XX_Count. (m1+m2)/(m1+m2+m3+m4)*100 m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 = HTTP Code 4xx || m4 = HTTP Code 5xx`

NameSpace:AWS/ApplicationELB

ComparisonOperator(Soglia): Meno di x (x = soglia del cliente).

Periodo: 60 secondi

DatapointsToAlarm: 3 su 3

Trattamento dei dati mancanti: considera i dati mancanti come una violazione.

Statistica: Sum

Il diagramma seguente mostra il flusso per lo Use Case A:

Esempio di utilizzo B: Amazon API Gateway

È possibile creare il seguente CloudWatch allarme che segnala il potenziale impatto sul carico di lavoro. Per fare ciò, crei una metrica composita che avvisa quando c'è un'elevata lantenza o un

numero medio elevato di errori 4XX nell'API Gateway. Per i parametri disponibili, consulta Dimensioni e metriche di Amazon API Gateway

Metrica: `compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))`

NameSpace:AWS/API Gateway

ComparisonOperator(Soglia): maggiore di (soglie x o y del cliente)

Periodo: 60 secondi

DatapointsToAlarm: 1 su 1

Trattamento dei dati mancanti: considera i dati mancanti come non una violazione.

Statistica:

Il diagramma seguente mostra il flusso per lo Use Case B:

Esempio di utilizzo C: Amazon Route 53

Puoi monitorare le tue risorse creando controlli sullo stato di Route 53 che raccolgono ed elaborano dati grezzi in metriche leggibili quasi in tempo reale. CloudWatch È possibile creare il seguente CloudWatch allarme che segnala il potenziale impatto sul carico di lavoro. Puoi utilizzare le CloudWatch metriche per creare un allarme che si attiva quando supera la soglia stabilita. Per le metriche disponibili, consulta CloudWatch le metriche per i controlli sanitari di CloudWatch Route 53

Metrica: `R53-HC-Success`

NameSpace:AWS/Itinerario 53

Soglia HealthCheckStatus: HealthCheckStatus < x per 3 punti dati entro 3 minuti (corrispondente alla soglia x del cliente)

Periodo: 1 minuto

DatapointsToAlarm: 3 su 3

Trattamento dei dati mancanti: considera i dati mancanti come una violazione.

Statistica: Minimum

Il diagramma seguente mostra il flusso per lo Use Case C:

Esempio di utilizzo D: monitora un carico di lavoro con un'app personalizzata

È fondamentale dedicare del tempo alla definizione di un controllo sanitario appropriato in questo scenario. Se verifichi solo che la porta di un'applicazione sia aperta, significa che non hai verificato che l'applicazione funzioni. Inoltre, effettuare una chiamata alla home page di un'applicazione non è necessariamente il modo corretto per determinare se l'app funziona. Ad esempio, se un'applicazione dipende sia da un database che da Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3), il controllo dello stato deve convalidare tutti gli elementi. Un modo per farlo è creare una pagina Web di monitoraggio, ad esempio /monitor. La pagina web di monitoraggio effettua una chiamata al database per assicurarsi che possa connettersi e ottenere dati. Inoltre, la pagina Web di monitoraggio effettua una chiamata ad Amazon S3. Quindi, indirizza il controllo dello stato del sistema di bilanciamento del carico alla pagina /monitor.

Il diagramma seguente mostra il flusso per lo Use Case D:

Inserisci allarmi in AWS Incident Detection and Response

AWS Incident Detection and Response supporta l'inserimento di allarmi tramite Amazon. EventBridge Questa sezione descrive come integrare AWS Incident Detection and Response con diversi strumenti di Application Performance Monitoring (APM) CloudWatch, tra cui Amazon, APMs con integrazione diretta con Amazon EventBridge (ad esempio, Datadog e New Relic) e APMs senza integrazione diretta con Amazon. EventBridge Per un elenco completo delle integrazioni dirette APMs con Amazon EventBridge, consulta Amazon EventBridge integrazioni.

Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI (Incident Detection and Response Command Line Interface) per automatizzare questi passaggi, consulta. CLI AWS per il rilevamento e la risposta agli incidenti

Argomenti

- Fornire l'accesso per l'inserimento degli avvisi in Incident Detection and Response
- Integra il rilevamento e la risposta agli incidenti con Amazon CloudWatch
- Ingestisci allarmi APMs che hanno un'integrazione diretta con Amazon EventBridge

- Esempio: integra le notifiche di Datadog e Splunk
- Usa i webhook per inserire allarmi APMs senza integrazione diretta con Amazon EventBridge

Fornire l'accesso per l'inserimento degli avvisi in Incident Detection and Response

Per consentire ad AWS Incident Detection and Response di importare allarmi dal tuo account, installa il ruolo `AWSServiceRoleForHealth_EventProcessor` collegato al servizio (SLR).AWS presuppone che la reflex crei una regola gestita da Amazon EventBridge. La regola gestita invia notifiche dai tuoi 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.AWS Health

È possibile installare questo ruolo collegato al servizio nel proprio account seguendo le istruzioni in Creare un ruolo collegato al servizio 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

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

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

- Utilizzo di ruoli collegati ai servizi per AWS Health
- Creazione di un ruolo collegato al servizio
- AWS politica gestita: AWSHealth_EventProcessorServiceRolePolicy

Integra il rilevamento e la risposta agli incidenti con Amazon CloudWatch

AWS Incident Detection and Response utilizza il ruolo collegato al servizio (SLR) che hai attivato durante il provisioning degli accessi per creare una regola EventBridge gestita da Amazon nel tuo

account denominato.AWSAWSHealthEventProcessor-DO-NOT-DELETE Incident Detection and Response utilizza questa regola per importare gli CloudWatch allarmi Amazon dai tuoi account. Non sono necessari passaggi aggiuntivi da cui importare gli allarmi. CloudWatch

Ingestisci allarmi APMs che hanno un'integrazione diretta con Amazon EventBridge

L'illustrazione seguente mostra il processo di invio di notifiche ad AWS Incident Detection and Response da strumenti di Application Performance Monitoring (APM) che hanno un'integrazione diretta con Amazon EventBridge, come Datadog e Splunk. Per un elenco completo di APMs quelle con integrazione diretta EventBridge, consulta EventBridge le integrazioni di Amazon.

Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI (Incident Detection and Response Command Line Interface) per automatizzare questi passaggi, consulta. CLI AWS per il rilevamento e la risposta agli incidenti

Utilizza i seguenti passaggi per configurare l'integrazione con AWS Incident Detection and Response. Prima di eseguire questi passaggi, verifica che il ruolo AWS collegato al servizio (SLR) `AWSServiceRoleForHealth_EventProcessor` sia installato nei tuoi account.

Configura l'integrazione con AWS Incident Detection and Response

È necessario completare i seguenti passaggi per ogni AWS account e AWS regione. Gli avvisi devono provenire dall'AWS account e dalla AWS regione in cui risiedono le risorse dell'applicazione.

1. Configura ciascuna delle tue fonti di eventi APMs come EventBridge partner Amazon (ad esempio,`aws.partner/my_apm/integrationName`). Per linee guida sulla configurazione del tuo APM come fonte di eventi, consulta Ricezione di eventi da un partner SaaS con Amazon. EventBridge Questo crea un bus di eventi partner nel tuo account.
2. Esegui una delle seguenti operazioni:
   - (Metodo consigliato) Crea un bus di EventBridge eventi personalizzato. AWS Incident Detection and Response installa un bus managed rule (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) tramite `AWSServiceRoleForHealth_EventProcessor` SLR. L'origine della regola è il bus degli eventi personalizzato. La destinazione della regola è AWS Incident Detection and Response. La regola corrisponde allo schema per l'acquisizione di eventi APM di terze parti.

- (Metodo alternativo) Utilizzate il bus eventi predefinito anziché un bus eventi personalizzato. Il bus di eventi predefinito richiede la regola gestita per inviare avvisi APM ad AWS Incident Detection and Response.

3. Crea una AWS Lambdafunzione (ad esempio,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`) per trasformare gli eventi del bus degli eventi del tuo partner. Gli eventi trasformati corrispondono alla regola gestita`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.

   a. 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. Il modello corrisponde alla regola gestita.

   b. Imposta la destinazione della funzione Lambda sul bus eventi personalizzato creato nel passaggio 2 (metodo consigliato) 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 del partner definito nel passaggio 1 (ad esempio, aws. partner/my_apm/integrationName). L'obiettivo della regola è la funzione Lambda definita nel passaggio 3 (ad esempio,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`). Per linee guida sulla definizione della EventBridge regola, consulta EventBridge le regole di Amazon.

Per esempi su come configurare l'integrazione di un bus di eventi partner da utilizzare con AWS Incident Detection and Response, consultaEsempio: integra le notifiche di Datadog e Splunk.

Esempio: integra le notifiche di Datadog e Splunk

Questo esempio fornisce passaggi dettagliati per l'integrazione delle notifiche da Datadog e Splunk a AWS Incident Detection and Response.

Argomenti

- Fase 1: configura il tuo APM come fonte di eventi in Amazon EventBridge
- Passaggio 2: crea un bus di eventi personalizzato
- Fase 3: Creare una AWS Lambda funzione per la trasformazione
- Fase 4: Creare una EventBridge regola Amazon personalizzata

Fase 1: configura il tuo APM come fonte di eventi in Amazon EventBridge

Configura ognuno di voi APMs come fonte di eventi in Amazon EventBridge nel tuo account AWS. Per istruzioni su come configurare il tuo APM come fonte di eventi, consulta le istruzioni per la configurazione della sorgente di eventi per il tuo strumento nei EventBridge partner Amazon.

Configurando il tuo APM come fonte di eventi, puoi importare notifiche dall'APM a un bus di eventi nel tuo account AWS. Dopo la configurazione, AWS Incident Detection and Response può avviare il processo di gestione degli incidenti quando l'event bus riceve un evento. Questo processo aggiunge Amazon EventBridge come destinazione nel tuo APM.

Passaggio 2: crea un bus di eventi personalizzato

È consigliabile utilizzare un bus di eventi personalizzato. AWS Incident Detection and Response utilizza il bus di eventi personalizzato per importare eventi trasformati. Una AWS Lambda funzione trasforma l'evento del bus degli eventi partner e lo invia al bus degli eventi personalizzato. AWS Incident Detection and Response installa una regola gestita per importare eventi dal bus di eventi personalizzato.

Puoi utilizzare il bus di eventi predefinito anziché un bus di eventi personalizzato. AWS Incident Detection and Response modifica la regola gestita per importarla dal bus degli eventi predefinito anziché da uno personalizzato.

Crea un bus di eventi personalizzato nel tuo AWS account:

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/
2. Scegli Buses, Event bus.
3. In Custom event bus, scegli Crea.
4. Fornisci un nome per il bus dell'evento in Nome. Il formato consigliato è APMName-AWSIncidentDetectionResponse-EventBus.

   Ad esempio, usa uno dei seguenti se usi Datadog o Splunk:

   - Datadog: Datadog-AWSIncidentDetectionResponse-EventBus
   - Splunk: Splunk-AWSIncidentDetectionResponse-EventBus

Fase 3: Creare una AWS Lambda funzione per la trasformazione

La funzione Lambda trasforma gli eventi tra il bus eventi partner nel passaggio 1 e il bus eventi personalizzato (o predefinito) del passaggio 2. La trasformazione della funzione Lambda corrisponde alla regola gestita di AWS Incident Detection and Response.

Crea una AWS Lambda funzione nel tuo account AWS

1. Apri la pagina Funzioni sulla AWS Lambda console.
2. Scegli Crea funzione.
3. Scegli la scheda Autore da zero.
4. Per Nome della funzione, inserisci un nome utilizzando il formato`APMName-AWSIncidentDetectionResponse-LambdaFunction`.

   Di seguito sono riportati alcuni esempi per Datadog e Splunk:

   - Datadog: Datadog-AWSIncidentDetectionResponse-LambdaFunction
   - Splunk: Splunk-AWSIncidentDetectionResponse-LambdaFunction
5. Per Runtime, inserisci Python 3.10.
6. Lascia i campi rimanenti con i valori predefiniti. Scegli Crea funzione.
7. Nella pagina di modifica del codice, sostituisci il contenuto predefinito della funzione Lambda con la funzione nei seguenti esempi di codice.

   Notate i commenti che iniziano con # nei seguenti esempi di codice. Questi commenti indicano quali valori modificare.

   Modello di codice di trasformazione Datadog:

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example 'Datadog-AWSIncidentDetectionResponse-EventBus'
EventBusName = "Datadog-AWSIncidentDetectionResponse-EventBus"
```

```
def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # Replace the dictionary path, event["detail"]["meta"]["monitor"]["name"], with
 the path to your alert name based on your APM payload.
    # This example is for finding the alert name for Datadog.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["meta"]["monitor"]["name"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
     Entries=[
              {
               'Detail': json.dumps(event["detail"], indent=2),
               'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
               'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
               'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
             }
     ]
    )
    print(response['Entries'])
```

Modello di codice di trasformazione Splunk:

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
 use your default event bus which is called 'default'.
# Example Splunk-AWSIncidentDetectionResponse-EventBus
EventBusName = "Splunk-AWSIncidentDetectionResponse-EventBus"
```

```
def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
 the name of your alert that is coming from your APM. Each APM is different and
 each unique alert will have a different name.
    # replace the dictionary path event["detail"]["ruleName"] with the path to your
 alert name based on your APM payload.
    # This example is for finding the alert name in Splunk.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["ruleName"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
    Entries=[
             {
              'Detail': json.dumps(event["detail"], indent=2),
              'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
 DetailType value is required.
              'Source': 'GenericAPMEvent', # Do not modify. This Source value is
 required.
              'EventBusName': EventBusName # Do not modify. This variable is set
 at the top of this code as a global variable. Change the variable value for your
 eventbus name at the top of this code.
           }
        ]
    )
    print(response['Entries'])
```

8. Seleziona Implementa.
9. Aggiungi l'PutEventsautorizzazione al ruolo di esecuzione Lambda per il bus di eventi a cui stai inviando i dati trasformati:
    a. Apri la pagina Funzioni sulla AWS Lambda console.
    b. Seleziona la funzione, quindi scegli Autorizzazioni nella scheda Configurazione.
    c. In Ruolo di esecuzione, seleziona il nome del ruolo per aprire il ruolo di esecuzione nella AWS Identity and Access Management console.
    d. In Criteri di autorizzazione, seleziona il nome del criterio esistente per aprire il criterio.
    e. In Autorizzazioni definite in questa politica, scegli Modifica.
    f. Nella pagina dell'editor delle politiche, seleziona Aggiungi nuova dichiarazione:
    g. L'editor delle politiche aggiunge una nuova dichiarazione vuota simile alla seguente

h. Sostituisci la nuova istruzione generata automaticamente con la seguente:

```
{
  "Sid": "AWSIncidentDetectionResponseEventBus0",
  "Effect": "Allow",
  "Action": "events:PutEvents",
  "Resource": "arn:aws:events:{region}:{accountId}:event-bus/{custom-eventbus-
name}"
}
```

i. La risorsa è l'ARN del bus eventi personalizzato che hai creato Passaggio 2: crea un bus di eventi personalizzato o l'ARN del tuo bus eventi predefinito se utilizzi il bus eventi predefinito nel tuo codice Lambda.

10. Verifica e conferma che le autorizzazioni richieste siano state aggiunte al ruolo.
11. Scegli Imposta questa nuova versione come predefinita, quindi scegli Salva modifiche.

Cosa è richiesto da una trasformazione del payload?

Le seguenti coppie chiave:valore JSON sono necessarie negli eventi del bus di 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.

```
{
    "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}
\u003c\u003d 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"
      ]
    }
}
```

Si noti che prima della trasformazione dell'evento, `detail-type` indica l'APM da cui proviene l'avviso, la fonte proviene da un APM partner e la `incident-detection-response-identifier` chiave non è presente.

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

```
{
    "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}
 \u003c\u003d 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 ora `detail-type` è adesso`ams.monitoring/generic-apm`, la fonte è ora`GenericAPMEvent`, e sotto i dettagli c'è una nuova coppia chiave:valore:. `incident-detection-response-identifier`

Nell'esempio precedente, il `incident-detection-response-identifier` valore viene preso dal nome dell'avviso sotto il percorso. `$.detail.meta.monitor.name` I percorsi dei nomi degli avvisi APM sono diversi da un APM all'altro. La funzione Lambda deve essere modificata per

prendere il nome dell'allarme dal percorso JSON dell'evento partner corretto e utilizzarlo per il valore. `incident-detection-response-identifier`

Ogni nome univoco impostato su `incident-detection-response-identifier` viene fornito al team di AWS Incident Detection and Response durante l'onboarding. Gli eventi con un nome sconosciuto `incident-detection-response-identifier` non vengono elaborati.

Fase 4: Creare una EventBridge regola Amazon personalizzata

Il bus degli eventi partner creato nella Fase 1 richiede una EventBridge regola da te creata. La regola invia gli eventi desiderati dal bus eventi partner alla funzione Lambda creata nel passaggio 3.

Per linee guida sulla definizione della EventBridge regola, consulta EventBridge le regole di Amazon.

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/
2. Scegli Regole, quindi seleziona il bus degli eventi partner associato al tuo APM. Di seguito sono riportati alcuni esempi di bus per eventi partner:
   - Datadog: aws. partner/datadog.com/eventbus-nome
   - Splunk: aws. partner/signalfx.com/RandomString
3. Scegli Crea regola per creare una nuova EventBridge regola.
4. Per il nome della regola, inserisci un nome nel formato seguente`APMName-AWS Incident Detection and Response-EventBridgeRule`, quindi scegli Avanti. Di seguito sono riportati alcuni esempi di nomi:
   - Datadog: Datadog-AWSIncidentDetectionResponse-EventBridgeRule
   - Splunk: Splunk-AWSIncidentDetectionResponse-EventBridgeRule
5. Per Event source, seleziona AWS events o EventBridge partner events.
6. Lascia Sample event e Creation method come valori predefiniti.
7. Per Event pattern, scegliete quanto segue:
   a. Fonte dell'evento: EventBridge partner.
   b. Partner: seleziona il tuo partner APM.
   c. Tipo di evento: tutti gli eventi.

   Di seguito sono riportati esempi di modelli di eventi:

Esempio di pattern di eventi Datadog

Esempio di pattern di eventi Splunk

8. Per Targets, scegli quanto segue:
   a. Tipi di target:AWS servizio
   b. Seleziona un obiettivo: scegli la funzione Lambda.
   c. Funzione: il nome della funzione Lambda creata nel passaggio 2.
9. Scegliete Avanti, Salva regola.

Usa i webhook per inserire allarmi APMs senza integrazione diretta con Amazon EventBridge

AWS Incident Detection and Response supporta l'utilizzo di webhook per l'inserimento di allarmi da terze parti APMs che non hanno un'integrazione diretta con Amazon. EventBridge Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI (Incident Detection and Response Command Line Interface) per automatizzare questi passaggi, consulta. CLI AWS per il rilevamento e la risposta agli incidenti

Per un elenco delle integrazioni dirette APMs con Amazon EventBridge, consulta Amazon EventBridge integrazioni.

Utilizza i seguenti passaggi per configurare l'integrazione con AWS Incident Detection and Response. Prima di eseguire questi passaggi, verifica che la AWS Managed Rule, AWSHealthEventProcessorEventSource-DO-NOT-DELETE, sia installata nei tuoi account

Inserisci eventi utilizzando webhook

1. Definisci un Amazon API Gateway per accettare il payload dal tuo APM.
2. Definisci una AWS Lambda funzione per l'autorizzazione utilizzando un token di autenticazione, come mostrato nella figura precedente.

3. Definisci una seconda funzione Lambda per trasformare e 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.
4. Configura il tuo APM per inviare notifiche all'URL generato dall'API Gateway.

CLI AWS per il rilevamento e la risposta agli incidenti

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

L'Incident Detection and Response CLI viene utilizzata AWS CloudShell per raccogliere informazioni sull'onboarding, raccogliere dati sulle risorse tramite l'API AWS Resource Groups Tagging e gestire i casi di supporto. La CLI può creare nuovi Amazon CloudWatch allarmi o inserire quelli esistenti, nonché implementare e testare l'infrastruttura per consentire a strumenti di terze parti di inviare avvisi AWS CloudFormation a Incident Detection and Response. Puoi eseguire la CLI in modalità interattiva per guidarti attraverso le fasi di onboarding o in modalità offline per casi collettivi o d'uso. DevOps

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

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 dei nuovi carichi di lavoro prima dell'onboarding, 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

Incident Detection and Response utilizza le informazioni raccolte dal questionario di onboarding per sviluppare runbook e piani di risposta per la gestione degli incidenti che influiscono sui carichi di lavoro. I runbook documentano le fasi adottate dagli Incident Manager per rispondere 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'individuazione del carico di lavoro. I piani di risposta sono modelli di documenti AWS Systems Manager(SSM) utilizzati per innescare incidenti. Per ulteriori informazioni sui documenti SSM, consulta Documenti.AWS Systems Manager Per ulteriori informazioni su Incident Manager, consulta What Is?Strumento di gestione degli incidenti AWS Systems Manager

Risultati chiave:

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

- Completamento degli allarmi, dei runbook e della definizione del piano di risposta 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:

```
Runbook template for AWS Incident Detection and Response
# Description
This document is intended for [CustomerName] [WorkloadName].

[Insert short description of what the workload is intended for].

## Step: Priority
**Priority actions**
1. When a case is created with Incident Detection and Response, lock the case to
 yourself, verify the Customer Stakeholders in the Case from *Engagement Plans -
 Initial Engagement*.
2. Send the first correspondence on the support case to the customer as below. If
 there is no support case or if it is not possible to use the support case then backup
 communication details are listed in the steps that follow.

```
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 after I have finished initial investigation.

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
```


Compliance and regulatory requirements for the workload
<<e.g. The workload deals with patient health records which must be kept secured and
 confidential. Information not to be shared with any third parties.>>

Actions required from Incident Detection and Response in complying
<<e.g Incident Management Engineers must not shared data with third parties.>>

Step: Information
Review of common information
```

```
* This section provides a space for defining common information which may be needed
 through the life of the incident.
* The target user of this information is the Incident Management Engineer and
 Operations Engineer.
* The following steps may reference this information to complete an action (for
 example, execute the "Initial Engagement" plan).

---
**Engagement plans**

Describe the engagement plans applicable to this runbook. This section contains
 only contact details. Engagement plans will be referenced in the step by step
 **Communication Plans**.

* **Initial engagement**

AWS Incident Detection and Response Team will add customer stakeholder addresses below
 to the Support Case. AWS Stakeholders are for additional stakeholders that may need to
 be made aware of any issues.
When updating customer stakeholders details in this plan also update the Backup Mailto
 links.
  * ***Customer Stakeholders***:  customeremail1; customeremail2; etc
  * ***AWS Stakeholders***: aws-idr-oncall@amazon.com; tam-team-email; etc.
  * ***One Time Only Contacts***: [These are email contacts that are included on only
 the first communication. Remove these contacts after the first communication has gone
 out. These could be customer paging email addresses such as pager-duty that must not
 be paged for every correspondence]
  * ***Backup Mailto Impact Template***: <*Insert Impact Template Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.
  * ***Backup Mailto No Impact Template***: <*Insert No Impact Mailto Link here*>
    * Use the backup Mailto when communication over cases is not possible.


* **Engagement Escalation**

AWS Incident Detection and Response will reach out to the following contacts when the
 contacts from the **Initial engagement** plan do not respond to incidents.
For each Escalation Contact indicate if they must be added to the support case, phoned
 or both.
  * ***First Escalation Contact***: [escalationEmailAddress#1] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
```

```
  * ***Second Escalation Contact***: [escalationEmailAddress#2] / [PhoneNumber] - Wait
 XX Minutes before escalating to this contact.
    * [add Contact to Case / phone] this contact.
  * Etc;
---
**Communication plans**

Describe how Incident Management Engineer communicates with designated stakeholders
 outside the incident call and communication channels.

* **Impact Communication plan**
This plan is initiated when Incident Detection and Response have determined from step
 **Triage** that an alert indicates potential impact to a customer.
Incident Detection and Response will request the customer to join the predetermined
 bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated
 in **Engagement plans - Incident call setup**.
All backup email templates for use when cases can't be used are in **Engagement plans -
 Initial engagement**.
  * 1 – Before sending the impact notification, verify then remove and/or add customer
 contacts from the Support Case CC based on the contacts listed in the **Initial
 engagement** Engagement plan.
  * 2 – Send the engagement notification to the customer based the following Template:

    (choose one and remove the rest)
    ***Impact Template - 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 2023, 3:30 PM UTC>
    Please join the Chime Bridge below so we can start the steps outlined in your
 Runbook:
        <insert Chime Meeting ID>
        <insert Link to Chime Bridge>
        International dial-in numbers: https://chime.aws/dialinnumbers/
    ```


    ***Impact Template - Customer Provided Bridge***
    ```
    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 2023 3:30 PM UTC>
    Please respond with your internal bridge details so we can join and start the steps
 outlined in your Runbook.
    ```
    Impact Template - 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 2023, 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 bridgeURL>
    ```
  * 3 - Set the Case to Pending Customer Action
  * 4 - Follow **Engagement Escalation** plan as mentioned above.
  * 5 - If the customer does not respond within 30 minutes, disengage and continue to
 monitor until the alarm recovers.

* **No Impact Communication plan**
This plan is initiated when an alarm recovers before Incident Detection and Response
 have completed initial **Triage**.
  * 1 - Before sending the no impact notification, verify then remove and/or add
 customer contacts from the Support Case CC based on the contacts listed in the
 Engagement plans - Initial engagement Engagement plan.
  * 2 - Send a no engagement notification to the customer based on the below template:

  No Impact Template
  ```
  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 2023, 3:30 PM UTC>
      Alarm End Time -  <Example: 1 January 2023, 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 - Put the case in to Pending Customer Action.
  * 4 - If the customer does not respond within 30 minutes Resolve the case.
```
```

```
* **Updates**
If AWS Incident Detection and Response is expected to provide regular updates to
 customer stakeholders, list those stakeholders here. Updates must be sent via the same
 support case.
Remove this section if not needed.
  * Update Cadence: Every XX minutes
  * External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc
  * Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

---
**Application architecture overview**

This section provides an overview of the application/workload architecture for Incident
 Management Engineer and Operations Engineer awareness.

* **AWS Accounts and Regions with key services** - list of AWS accounts with regions
 supporting this application. Assists Engineers in assessing underlying infrastructure
 supporting the application.
    * 123456789012
      * US-EAST-1 - brief desc as appropriate
        * EC2 - brief desc as appropriate
        * DynamoDB - brief desc as appropriate
        * etc.
      * US-WEST-1 - brief desc as appropriate
      * etc.
    * another-account-etc.

* **Resource identification** - describe how engineers determine resource association
 with application
    * Resource groups: etc.
    * Tag key/value: AppId=123456

* **CloudWatch Dashboards** - list dashboards relevant to key metrics and services
  * 123456789012
    * us-east-1
      * some-dashboard-name
      * etc.
  * some-other-dashboard-name-in-current-acct

## Step: Triage
**Evaluate incident and impact**
This section provides instructions for triaging of the incident to determine correct
 impact, description, and overall correct runbook being executed.
```

```
* **Evaluation of initial incident information**
  * 1 - Review Incident Alarm, noting time of first detected impact as well as the
 alarm start time.
  * 2 - Identify which service(s) in the customer application is seeing impact.
  * 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions
 with key services**.
  * 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

---
* **Impact**
Impact is determined when either the customer's metrics do not recover, appear to be
 trending worse or if there is indication of AWS Service Impact.
  * 1 – Start **Communication plans - Impact Communication plan**
  * 2 - Start **Engagement plans - Engagement Escalation** if no response is received
 from the **Initial Engagement** contacts.
  * 3 - Start **Communication plans - Updates** if specified in **Communication plans**

* **No Impact**
No Impact is determined when the customer's alarm recovers before Triage is complete
 and there are no indications of AWS service impact or sustained impact on the
 customer's CloudWatch Dashboards.
  * 1 - Start **Communication plans - No Impact Communication plan**

## Step: Investigate
**Investigation**

  This section describes performing investigation of known and unknown symptoms.

**Known issue**
  * *List all known issues with the application and their standard actions here*

**Unknown issues**
  * Investigate with the customer and AWS Premium Support.
  * Escalate internally as required.

## Step: Mitigation
**Collaborate**
* Communicate any changes or important information from the **Investigate** step to the
 members of the incident call.

**Implement mitigation**
```

```
* ***List customer failover plans / Disaster Recovery plans / etc here for implementing
 mitigation.

## Step: Recovery
**Monitor customer impact**
* Review metrics to confirm recovery.
* Ensure recovery is across all Availability Zones / Regions / Services
* Get confirmation from the customer that impact is over and the application has
 recovered.

**Identify action items**
* Record key decisions and actions taken, including temporary mitigation that might
 have been implemented.
* Ensure outstanding action items have assigned owners.
* Close out any Communication plans that were opened during the incident with a final
 confirmation of recovery notification.
```

Testa i carichi di lavoro integrati in Incident Detection and Response

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

L'ultimo passaggio del processo di onboarding consiste nell'organizzare una giornata di gioco per il nuovo carico di lavoro. Al termine dell'inserimento degli allarmi, AWS Incident Detection and Response conferma una data e un'ora a tua scelta per iniziare la giornata di gioco.

La tua giornata di gioco ha due scopi principali:

- Convalida funzionale: conferma che AWS Incident Detection and Response è in grado di ricevere correttamente gli eventi di allarme. Inoltre, la convalida funzionale conferma che gli eventi di allarme attivano i runbook appropriati e qualsiasi altra azione desiderata, come la creazione automatica dei casi, se selezionata durante l'inserimento dell'allarme.
- Simulazione: il gameday è una simulazione completa 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. Il gameday è un'opportunità per porre domande o perfezionare le istruzioni per migliorare il coinvolgimento.

Durante il test degli allarmi, AWS Incident Detection and Response collabora con te per risolvere eventuali problemi identificati.

CloudWatch allarmi

AWS Incident Detection and Response testa i tuoi CloudWatch allarmi Amazon monitorando il cambio di stato dell'allarme. Per fare ciò, imposta manualmente l'allarme allo stato di allarme utilizzando il AWS Command Line Interface. Puoi anche accedere al AWS CLI modulo AWS CloudShell. AWS Incident Detection and Response ti fornisce un elenco di AWS CLI comandi da utilizzare durante i test.

AWS CLI Comando di esempio per impostare uno stato di allarme:

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

Per ulteriori informazioni sulla modifica manuale dello stato degli CloudWatch allarmi, consulta SetAlarmState.

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

Allarmi APM di terze parti

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. All'inizio della giornata di gioco, AWS Incident Detection and Response richiede di modificare temporaneamente le soglie di allarme o gli operatori di confronto per forzare l'allarme allo stato ALARM. Questo stato attiva un payload per AWS Incident Detection and Response.

Risultati chiave

Risultati chiave:

- L'inserimento dell'allarme è riuscito e la configurazione dell'allarme è corretta.

- Gli allarmi vengono creati e ricevuti con successo da AWS Incident Detection and Response.
- Viene creato un caso di supporto per il tuo coinvolgimento e i contatti prescritti vengono avvisati.
- AWS Incident Detection and Response può interagire con te tramite i mezzi di conferenza prescritti.
- Tutti gli allarmi e i casi di assistenza generati durante la giornata di gioco sono stati risolti.
- Viene inviata un'e-mail Go-Live per confermare che il carico di lavoro è ora monitorato da AWS 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 - opzionale, inserisci l'e-mail a IDs cui desideri ricevere la corrispondenza relativa a questa modifica.

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

> **Important**
>
> La mancata aggiunta di e-mail IDs 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 l'e-mail IDs 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

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. Nella sezione matematica metrica, scegli Modifica.
4. Scegli Aggiungi matematica, Inizia con un'espressione vuota.
5. Inserisci la tua espressione matematica, quindi scegli Applica.

6. Deseleziona la metrica esistente monitorata dall'allarme.
7. Seleziona l'espressione che hai appena creato, quindi scegli Seleziona metrica.
8. Scegliete Salta all'anteprima e create.
9. 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. • IF (condition, value_if_true, value_if_false): restituisce 0 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), 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).
`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'interva llo 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).

Funzione matematica metrica	Caso d'uso	Spiegazione
`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 intervall o.
`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 l'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 Vai 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 il riavvio dell'istanza 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 piùAWS account, crea la richiesta di assistenza dal tuo account di pagamento. Nel corpo della richiesta di assistenza, elenca tutti gli account da eliminare. IDs

> **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 cui il carico di lavoro è stato ritirato.
8. Nella sezione Contatti aggiuntivi - opzionale, inserisci l'e-mail a IDs 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 èAWS possibile rispondere prontamente a queste interruzioni e fornire assistenza per il ripristino. Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI (Incident Detection and Response Command Line Interface) per automatizzare questi passaggi, consulta. CLI AWS per il rilevamento e la risposta agli incidenti
- Fase post-onboarding: 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 l'impostazione 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 account manager tecnici (). TAMs

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
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 successivo all'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

- Fornisci l'accesso AWS Support Center Console ai team delle applicazioni
- Richiedi una risposta all'incidente

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

Fornisci l'accesso AWS Support Center Console ai team delle applicazioni

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 AWSAWS Support App in Slack

Il diagramma seguente illustra il end-to-end flusso di lavoro di 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 una conferenza con gli AWS esperti necessari per accelerare il recupero del tuo carico di lavoro.

Richiedi un Incident Response utilizzando il AWS Support Center Console

1. Apri AWS Support Center Console, quindi scegli Crea caso.
2. Scegli Tecnico.
3. Per Assistenza, scegli Incident Detection and Response.
4. Per Categoria, scegli Active Incident.

5. Per Severità, scegli Business-critical system down.
6. Inserisci un oggetto per questo incidente. Esempio:

   Rilevamento e risposta agli incidenti AWS - Active Incident - workload_name
7. Inserisci la descrizione del problema per questo incidente. Aggiungi i seguenti dettagli:
   - Informazioni tecniche:

     Nome del carico di lavoro

     ARN della AWS risorsa interessata
   - Informazioni aziendali:

     Descrizione dell'impatto sull'attività

     [Facoltativo] Dettagli di Customer Bridge
8. Per aiutarci a coinvolgere più rapidamente AWS gli esperti, fornisci i seguenti dettagli:
   - Impatto Servizio AWS
   - Servizio/i aggiunti/Altri interessati
   - Impattato Regione AWS
9. Nella sezione Contatti aggiuntivi, inserisci gli indirizzi e-mail a cui desideri ricevere la corrispondenza relativa a questo incidente.

   La figura seguente mostra la schermata della console con il campo Contatti aggiuntivi evidenziato.

10. Seleziona Invia.

    Dopo aver inviato una richiesta di Incident Response, puoi aggiungere altri indirizzi email della tua organizzazione. Per aggiungere altri indirizzi, rispondi al caso, quindi aggiungi gli indirizzi e-mail nella sezione Contatti aggiuntivi.

    L'illustrazione seguente mostra la schermata dei dettagli del caso con il pulsante Rispondi evidenziato.

    L'illustrazione seguente mostra il caso Rispondi con il campo Contatti aggiuntivi e il pulsante Invia evidenziati.

11 AWS Incident Detection and Response riconosce il tuo caso entro cinque minuti e ti coinvolge in una conferenza con gli esperti appropriati AWS.

Richiedi una risposta agli incidenti utilizzando l'API Supporto AWS

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

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 account manager tecnico 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
Aggiunta una nuova sezione: Incident Detection and Response Customer Command Line Interface (CLI)	È stata aggiunta la sezione Incident Detection and Response Customer Command Line Interface (CLI) e aggiornato il capitolo Guida introduttiva per includere informazioni sull'interfaccia CLI (Incident Detection and Response Customer Command Line Interface). Per ulteriori informazioni, consulta CLI AWS per il rilevamento e la risposta agli incidenti.	8 dicembre 2025
Diverse sezioni aggiornate: questionari sull'onboarding del carico di lavoro e sull'inserimento degli allarmi in Incident Detection and Response e Guida introduttiva 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 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
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 riflettere questa modifica. Continuerai a ricevere notifiche sugli eventi di servizio tramite AWS	14 ottobre 2025

Modifica	Descrizione	Data
	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.	
Sezione aggiornata: disponibilità regionale per il rilevamento e la risposta agli incidenti	AWS Incident Detection and Response è ora disponibile negli AWS GovCloud Stati Uniti orientali e AWS GovCloud negli Stati Uniti occidentali. Per ulteriori informazioni, consulta Disponibilità regionale per il rilevamento e la risposta agli incidenti	5 ottobre 2025
Sezione aggiornata: questionari 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. Per ulteriori informazioni, consulta Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response	26 agosto 2025
Sezione aggiornata: sottoscrivi 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: Abbonati un carico di lavoro a Incident Detection and Response	4 agosto 2025
Nuova funzione: sopprime gli allarmi attivando 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

Modifica	Descrizione	Data
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
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: Abbonati un carico di lavoro a Incident Detection and Response	12 giugno 2024

Modifica	Descrizione	Data
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 relativi all'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 Abbonamento all'account	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 onboardin g del carico di lavoro e aggiunto il questiona rio di inserimento degli allarmi. La sezione è stata rinominata da Questionario di onboarding a Questionari di onboarding del carico di lavoro e Alarm ingestion. Sezione aggiornata: Questionari di onboarding del carico di lavoro e inserimento degli allarmi in Incident Detection and Response	2 febbraio 2024
Informazioni aggiornate AWS sugli eventi di assistenza e sull'onboarding	Sono state aggiornate diverse sezioni con nuove informazioni per l'onboarding. Sezioni aggiornate: • Individuazione del carico di lavoro nel rilevamento e nella risposta agli incidenti • Introduzione al rilevamento e alla risposta agli incidenti • Abbonati un carico di lavoro a Incident Detection and Response Nuove sezioni • Fornisci l'accesso AWS Support Center Console ai team delle applicazioni	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: Fornire l'accesso per l'inserimento degli avvisi in Incident Detection and Response	17 gennaio 2024

Modifica	Descrizione	Data
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: integra le notifiche di Datadog e Splunk	21 dicembre 2023
Grafica e testo introduttivi aggiornati	Grafica aggiornata negli allarmi Ingest APMs 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

Modifica	Descrizione	Data
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 Incident Detection and Response Nuova sezione: Crea CloudWatch allarmi in Incident Detection and Response con modelli CloudFormation Nuova sezione: Esempi di casi d'uso degli CloudWatch allarmi in Incident Detection and Response	28 settembre 2023
Guida introduttiva aggiornata	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: Abbonati un carico di lavoro a Incident Detection and Response	05 settembre 2023
Nuova sezione in Guida introduttiva	Aggiunti avvisi di Inserisci allarmi in AWS Incident Detection and Response 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.