AWSConcetti e procedure di rilevamento e risposta agli incidenti

AWSGuida per l'utente di rilevamento e risposta agli incidenti

Version July 3, 2024

AWSGuida per l'utente di rilevamento e risposta agli incidenti: AWSConcetti e procedure di rilevamento e risposta agli incidenti

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. Un team di Incident Management Engineer (IME) monitora i carichi di lavoro integrati 24 ore su 24, 7 giorni su 7 e ti coinvolge su un call bridge entro 5 minuti da un allarme critico.

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 IME monitorano i carichi di lavoro integrati 24 ore su 24, 7 giorni su 7 per rilevare incidenti critici. Gli IME rispondono entro 5 minuti dall'attivazione di un allarme o in risposta a un caso di supporto di importanza critica per l'azienda da te segnalato a Incident Detection and Response.
- Risoluzione più rapida: gli IME utilizzano 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. Gli IME garantiscono la gestione degli incidenti in un unico thread e vi mantengono in contatto con gli esperti giusti fino alla risoluzione dell'incidente. AWS
- Gestione degli incidenti per AWS gli eventi: poiché comprendiamo il contesto del carico di lavoro critico (ad esempio, account, servizi e istanze), possiamo rilevare e notificare in modo proattivo un potenziale impatto sul carico di lavoro durante un evento di servizio. AWS Se richiesto, gli IME coinvolgono l'utente durante gli eventi AWS di servizio e forniscono aggiornamenti sugli eventi. Sebbene Incident Detection and Response non possa dare priorità al ripristino durante un evento di servizio, Incident Detection and Response fornisce una guida di Support per aiutarti a implementare il tuo piano di mitigazione.
- Riduzione del rischio di guasto: dopo la risoluzione, gli IME forniscono una revisione post-incidente (su richiesta). Inoltre, gli AWS esperti collaborano con voi per applicare le lezioni apprese per migliorare il piano di risposta agli incidenti e i runbook. Puoi anche sfruttare AWS Resilience Hub per il monitoraggio continuo della resilienza dei tuoi carichi di lavoro.

Termini del prodotto Incident Detection and Response

- 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 annullamento devono essere inviate trenta (30) giorni prima della data di validità 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.

Disponibilità del rilevamento e della risposta agli incidenti

AWS Incident Detection and Response è attualmente disponibile in lingua inglese per gli account Enterprise Support ospitati in uno dei seguenti paesi Regioni AWS:

Nome	Regione AWS
us-east-1	Stati Uniti orientali (Virginia)
us-east-2	Stati Uniti orientali (Ohio)
us-west-1	Stati Uniti occidentali (California settentrionale)
us-west-2	US West (Oregon)

Nome	Regione AWS
ca-central-1	Canada (Centrale)
sa-east-1	Sud America (San Paolo)
eu-central-1	Europa (Francoforte)
eu-west-1	Europa (Irlanda)
eu-west-2	Europa (Londra)
eu-west-3	Europa (Parigi)
eu-north-1	Europa (Stoccolma)
ap-south-1	Asia Pacifico (Mumbai)
ap-northeast-1	Asia Pacifico (Tokyo)
ap-northeast-2	Asia Pacifico (Seoul)
ap-southeast-1	Asia Pacifico (Singapore)
ap-southeast-2	Asia Pacifico (Sydney)

Rilevamento e risposta agli incidenti AWS RACI

La tabella seguente mostra AWS Incident Detection and Response responsabile, responsabile, consultato e informato o RACI.

Attività	Cliente	Rilevamento e risposta agli incidenti
Raccolta dati		

Attività	Cliente	Rilevamento e risposta agli incidenti
Introduzione al cliente e al carico di lavoro	C	R
Architettura	R	A
Operazioni	R	A
Determina CloudWatch gli allarmi da configurare	R	A
Definisci il piano di risposta agli incidenti	R	A
Completamento del questionario di onboarding	R	A
Revisione della prontezza operativa		
Effettua una revisione ben architettata (WAR) sul carico di lavoro	C	R
Convalida la risposta agli incidenti	C	R
Convalida la matrice di allarme	C	R
Identifica AWS i servizi chiave utilizzati dal carico di lavoro	A	R
Configurazione dell'account		
Crea un ruolo IAM nell'account del cliente	R	I
Installa la EventBridge regola gestita utilizzando il ruolo creato	I	R
Prova gli CloudWatch allarmi	R	A
Verifica che gli allarmi dei clienti coinvolgano il rilevamento e la risposta agli incidenti	I	R
Aggiorna gli allarmi	R	C

Attività	Cliente	Rilevamento e risposta agli incidenti
Aggiorna i runbook	C	R
Gestione degli incidenti		
Notifica in modo proattivo gli incidenti rilevati mediante il rilevamento e la risposta agli incidenti	I	R
Fornisci una risposta agli incidenti	I	R
Fornisci la risoluzione degli incidenti e il ripristino dell'infrastruttura	R	C
Revisione successiva all'incidente		
Richiedi una revisione successiva all'incidente	R	I
Fornisci una revisione successiva all'incidente	I	R

Architettura AWS 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 ulteriori informazioni, 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 runbook specifici indicano ad AWS Incident Detection and Response chi contattare, come contattarli e quali informazioni condividere.

Inizia a usare AWS Incident Detection and Response

È possibile 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 un 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 un unico AWS account o più AWS conti.

Ad esempio, potresti avere un'applicazione monolitica ospitata in un singolo account (ad esempio, Employee Performance App in Fig.1). Oppure, potresti avere un'applicazione (ad esempio, Storefront Webapp nella Fig. 1) suddivisa in microservizi che si estendono su diversi account. Un carico di lavoro potrebbe condividere risorse, ad esempio un database, con altre applicazioni o carichi di lavoro, come illustrato nella Fig. 1.

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

Onboarding

AWS collabora con te per integrare il carico di lavoro e gli allarmi in Incident Detection and ResponseAWS. Fornisci informazioni chiave a AWS nella Questionari di onboarding del carico di lavoro e inserimento degli allarmi. È consigliabile registrare anche i carichi di lavoro. AppRegistry Per ulteriori informazioni, consulta la Guida per l'AppRegistry utente.

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 voi per comprendere il vostro carico di lavoro e come supportarvi durante gli incidenti e AWS Eventi di servizio. 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
- AWS Eventi di assistenza

Ingestione degli allarmi

AWS collabora con te per integrare i tuoi allarmi. AWSIncident Detection and Response può importare allarmi da Amazon CloudWatch e dagli strumenti di monitoraggio delle prestazioni delle applicazioni di terze parti (APM) 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 integrare un carico di lavoro in Incident Detection and AWS Response. Questa tabella mostra esempi di durata di ogni attività. Le date effettive per ogni attività sono definite in base alla disponibilità del team e alla pianificazione.

Abbonamento all'account

Per sottoscrivere un carico di lavoro a 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 integrare un carico di lavoro in un'unica soluzione AWS account, crea la richiesta di assistenza dall'account del carico di lavoro o dal tuo account di pagamento.
- Per effettuare l'onboarding di un carico di lavoro che si estende su più livelli AWS account, crea la richiesta di assistenza dal tuo account di pagamento. Nel corpo della richiesta di assistenza, elenca tutti gli account IDs da inserire a bordo.

> **Important**
>
> Se crei una richiesta di supporto per sottoscrivere un carico di lavoro a Incident Detection and Response dall'account errato, potresti riscontrare ritardi e richieste di informazioni aggiuntive prima che i carichi di lavoro possano essere sottoscritti.

Per sottoscrivere un carico di lavoro

1. Vai al AWS Support Centra, quindi seleziona Crea custodia come illustrato nell'esempio seguente. È possibile sottoscrivere carichi di lavoro solo da account registrati in Enterprise Support.

2. Compila il modulo per la richiesta di assistenza:
   - 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. Per esempio:

   [A bordo] Rilevamento e risposta agli AWS incidenti - *`workload_name`*
4. Inserisci una descrizione per questa modifica. Ad esempio, inserisci «Questa richiesta riguarda l'onboarding di un carico di lavoro per il rilevamento e la risposta agli AWS incidenti». Assicurati di includere le seguenti informazioni nella tua richiesta:
   - Nome del carico di lavoro: il nome del tuo carico di lavoro.
   - ID account:ID1, ID2ID3, e così via. Questi sono gli account che desideri aggiungere a AWS Incident Detection and Response.

- Data di inizio dell'abbonamento: la data in cui desideri iniziare l'abbonamento AWS Incident Detection and Response.

5. Nella sezione Contatti aggiuntivi - facoltativa, 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. Scegli Invia.

   Dopo aver inviato la richiesta, puoi aggiungere altre email 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 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: completa tutte le informazioni del questionario relative al carico di lavoro che stai assumendo. 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**
>
> NOTAllega questi due documenti alla custodia utilizzando l'opzione Allega file. AWSIl team di Incident Detection and Response risponderà al caso con un link Amazon Simple Storage Service Uploader 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 Per informazioni su come esternalizzare un carico di lavoro, consulta. Offboard di un carico di lavoro

Individuazione del carico di lavoro

AWS collabora con voi per comprendere il più possibile il contesto del vostro carico di lavoro. AWSIncident Detection and Response utilizza queste informazioni per creare runbook di supporto durante gli incidenti e AWS Eventi di servizio. Le informazioni richieste vengono acquisite inQuestionari di onboarding del carico di lavoro e inserimento degli allarmi. È consigliabile registrare i carichi di lavoro su AppRegistry. Per ulteriori informazioni, consulta la Guida per l'AppRegistry utente.

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 sull'utilizzo del carico di lavoro AWS servizi in ciascuno AWS Regione.
- Informazioni specifiche su come AWS ti supporta durante un evento di servizio.
- Allarmi utilizzati dal team per rilevare l'impatto critico del carico di lavoro.

Configurazione degli allarmi

AWS collabora con te per definire metriche e allarmi per fornire visibilità sulle prestazioni delle tue applicazioni e su quelle sottostanti AWS infrastruttura. 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.
- Amazon CloudWatch canarini. Per ulteriori informazioni, vedere Canaries and X-Ray tracing e X-Ray.
- Allarme aggregato (monitoraggio delle dipendenze)

Esempio di allarme, il tutto utilizzando il sistema di monitoraggio CloudWatch

Nome metrico/Soglia di allarme	Allarme ARN o ID della risorsa	Se questo allarme si attiva	Se richiesto, chiudi un Premium Support Case per questi servizi
APIerrori/ numero di errori >= 10 per 10 punti dati	arn:aws:cloudwatch:us-west- 2:000000000000:alarm:e2 -Errori MPmimLambda	Ticket inviato al team dell'amministratore del	Lambda, porta API

Nome metrico/Soglia di allarme	Allarme ARN o ID della risorsa	Se questo allarme si attiva	Se richiesto, chiudi un Premium Support Case per questi servizi
		database () DBA	
ServiceUnavailable (Codice di stato Http 503) Numero di errori >=3 per 10 punti dati (client diversi) in una finestra di 5 minuti	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:http errorcode503	Ticket consegnato al team di assistenza	Lambda, porta API
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:http errorcode400	Ticket consegnato al team di assistenza	EC2, Amazon Aurora

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

Risultati chiave:

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

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.

Controlla 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:
  - HTTPCodeELB_ _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 Elastic Beanstalk, prendi WebSocket API 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' WebSocket APIesecuzione 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 DNS le query finché non viene completamente ripristinato. Per ulteriori informazioni, consulta Monitoring 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 trattare i dati mancanti come. notBreaching 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 trattare i dati mancanti in notBreachingmodo che i dati mancanti vengano trattati come «OK» e la metrica non entri nello stato «Allarme» 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.

Utilizzo AWS CloudFormation modelli per creare CloudWatch allarmi in Incident Detection and Response

Per accelerare l'onboarding verso il rilevamento e la risposta agli AWS incidenti e ridurre lo sforzo necessario per creare allarmi, AWS ti fornisce AWS CloudFormation modelli. 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	Compariso nOperator (Soglia)	Periodo	Datapoint sToAlarm	TreatMiss ingData	Statistic	Link al modello
Applicazi one Elastic Load Balancer	(m1+m2)/ (m1+m2+m m4) *100 m1= _Target_2 xx_Count m2= _Target_3 xx_Count m3= _Target_4 xx_Count m4= _Target_5 xx_count HTTPCode HTTPCode HTTPCode HTTPCode	LessThanT hreshold(95)	60	3 su 3	perso	Somma	Template (Modello)
Amazon CloudFron t	TotalErro rRate	GreaterTh anThresho ld(5)	60	3 su 3	notBreach ing	Media	Template (Modello)

NameSpac	Metriche	Compariso nOperator (Soglia)	Periodo	Datapoint sToAlarm	TreatMiss ingData	Statistic	Link al modello
Applicazi one Elastic Load Balancer	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3 su 3	notBreach ing	Massimo	Template (Modello)
Elastic Load Balancer di rete	UnHealthy HostCount	GreaterTh anOrEqual ToThresho ld(2)	60	3 su 3	notBreach ing	Massimo	Template (Modello)

2. Esamina il JSON file 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 AWS CloudFormation console.

   a. Apri il 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. Inserisci le seguenti informazioni obbligatorie:

      - AlarmNameConfige AlarmDescriptionConfig: Inserisci un nome e una descrizione per l'allarme.

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

- D istributionIDConfig: Assicurati che l'ID di distribuzione indichi le risorse corrette nell'account che stai creando AWS CloudFormation impilare.

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 SNS notifica. È consigliabile attivare la protezione dalla terminazione per evitare l'eliminazione 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 corretto e AWS Regione, avvisa il tuo Technical Account Manager (TAM). Il team 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

Consulta i seguenti casi d'uso per esempi di come utilizzare gli CloudWatch allarmi Amazon in Incident Detection and Response.

Esempio di utilizzo A: Application Load Balancer

Crea il seguente CloudWatch allarme che segnala il potenziale impatto sul carico di lavoro. Puoi creare una metrica matematica che avvisi 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/Applicazione ELB

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

Crea il seguente CloudWatch allarme che segnala il potenziale impatto sul carico di lavoro. Puoi creare una metrica composita che avvisi quando c'è un'elevata lantenza o un numero medio elevato di errori 4XX nel Gateway. API Per i parametri disponibili, consulta Dimensioni e metriche di Amazon API Gateway

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

NameSpace: AWS/APIGateway

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 da un database AND Amazon Simple Storage Service, il controllo dello stato deve convalidare tutti gli elementi. Un modo per farlo è creare una pagina web di monitoraggio, come / 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 avvisi in Incident Detection AWS and Response

AWSIncident 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, APMs tra cui Amazon, 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.

Argomenti

- Fornisci l'accesso per l'inserimento degli avvisi in modalità 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

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

Per consentire a AWS Incident Detection and Response di importare gli allarmi dal tuo account, installa il ruolo collegato al `AWSServiceRoleForHealth_EventProcessor` servizio (). SLR AWS presuppone la creazione SLR di una regola EventBridge gestita da Amazon. La regola gestita invia notifiche dai tuoi account a AWS Incident Detection and Response. Per informazioni al riguardoSLR, incluse le informazioni associate AWS policy gestita, vedere Utilizzo dei ruoli collegati ai servizi nella AWS Health Guida per l'utente.

Puoi installare questo ruolo collegato al servizio nel tuo account seguendo le istruzioni in Creare un ruolo collegato al servizio nella AWS Identity and Access Management Guida per l'utente. In alternativa, è possibile utilizzare il seguente AWS comando Command Line Interface (AWSCLI):

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

Uscite chiave

- Installazione riuscita del Service Linked Role nel tuo account.

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti argomenti:

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

Integra il rilevamento e la risposta agli incidenti con Amazon CloudWatch

AWSIncident Detection and Response utilizza il ruolo collegato al servizio (SLR) che hai attivato durante il provisioning degli accessi per creare una regola gestita da Amazon EventBridge nel tuo AWS account denominato. `AWSHealthEventProcessor-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

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

Utilizza i seguenti passaggi per configurare l'integrazione con AWS Incident Detection and Response. Prima di eseguire questi passaggi, verificate che AWS service-linked role (SLR)`AWSServiceRoleForHealth_EventProcessor`, è installato nei tuoi account.

Configura l'integrazione con AWS Incident Detection and Response

È necessario completare i seguenti passaggi per ciascuno AWS account e AWS Regione. Gli avvisi devono provenire dal AWS account e 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 della tua APM come fonte di eventi, consulta Ricezione di eventi da un partner SaaS con Amazon. EventBridge In questo modo viene creato un bus di eventi partner nel tuo account.
2. Esegui una di queste operazioni:
   - (Metodo consigliato) Crea un bus di EventBridge eventi personalizzato. AWSIncident Detection and Response installa un bus rule (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) gestito 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 di terze partiAPM.
   - (Metodo alternativo) Utilizzate il bus eventi predefinito anziché un bus eventi personalizzato. Il bus di eventi predefinito richiede la regola gestita per inviare APM avvisi a AWS Incident Detection and Response.
3. Creazione di un AWS Lambdafunzione (ad esempio,`My_APM-AWSIncidentDetectionResponse-LambdaFunction`) per trasformare gli eventi del bus degli eventi partner. Gli eventi trasformati corrispondono alla regola gestita`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
   a. Gli eventi trasformati includono un identificatore univoco di rilevamento e risposta agli AWS incidenti 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 a AWS Incident Detection and Response. L'origine della regola è il bus degli eventi partner definito nel passaggio 1 (ad esempio, integrationName aws.partner/my_apm/). 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 di Datadog e Splunk con Incident Detection and Response. AWS

1. Configura la tua APM come fonte di eventi in Amazon EventBridge nel tuo AWS account.
2. Crea un bus di eventi personalizzato.
3. Crea un AWS Lambda funzione di trasformazione.
4. Crea la tua EventBridge regola personalizzata.

Passaggio 1: configura la tua APM come fonte di eventi in Amazon EventBridge

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

Configurando la tua APM come fonte di eventi, puoi inserire le notifiche dal tuo APM a un event bus nel tuo AWS account. 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 tuoAPM.

Passaggio 2: crea un bus di eventi personalizzato

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

È possibile utilizzare il bus eventi predefinito anziché un bus eventi personalizzato. AWSIncident Detection and Response modifica la regola gestita in modo da importarla dal bus degli eventi predefinito anziché da uno personalizzato.

Crea un bus di eventi personalizzato nel tuo AWS conto:

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 un AWS Lambda funzione di 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 AWS Incident Detection and Response.

Crea un AWS Lambda funzione nel tuo AWS account

1. Apri la pagina Funzioni sul 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 Deploy (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 sul AWS Lambda console.
    b. Seleziona la funzione, quindi scegli Autorizzazioni nella scheda Configurazione.

c. In Ruolo di esecuzione, selezionate 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 il ARN bus degli eventi personalizzato che hai creato Passaggio 2: crea un bus di eventi personalizzato o il bus ARN degli eventi predefinito se utilizzi il bus eventi predefinito nel tuo codice Lambda.

10. Verifica e conferma che l'autorizzazione richiesta sia stata aggiunta 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 JSON chiave:valore sono necessarie negli eventi del bus degli eventi inseriti 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 event bus 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 la APM provenienza dell'avviso, la fonte proviene da un partner APM 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`aams.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` APMi percorsi dei nomi degli avvisi sono diversi da uno APM all'altro. La funzione Lambda deve essere modificata per prendere il nome dell'allarme dal JSON percorso corretto dell'evento partner e utilizzarlo per il `incident-detection-response-identifier` valore.

Ogni nome univoco impostato su `incident-detection-response-identifier` viene fornito al team di rilevamento e risposta agli AWS incidenti durante l'onboarding. Gli eventi a cui è stato assegnato 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 per eventi partner associato al tuoAPM. Di seguito sono riportati alcuni esempi di bus per eventi partner:
   - Datadog: aws.partner/datadog.com/eventbus-name
   - Splunk: aws.partner/signalfx.com/ RandomString
3. Scegli Crea regola per creare una nuova regola. EventBridge
4. Per il nome della regola, inserisci un nome nel formato seguenteAPMName-`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 Origine dell'evento, seleziona AWSeventi o eventi EventBridge partner.
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 APM partner.

    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 bersagli: AWS service

    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

AWSIncident 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 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 regola AWS gestita, AWSHealthEventProcessorEventSource-DO- NOT - DELETE, sia installata nei tuoi account

Inserisci eventi utilizzando i webhook

1. Definisci un Amazon API Gateway per accettare il payload dal tuoAPM.

2. Definisci un AWS Lambda funzione per l'autorizzazione mediante un token di autenticazione, come illustrato nella figura precedente.
3. Definite una seconda funzione Lambda per trasformare e aggiungere l'identificatore AWS Incident Detection and Response al payload. È inoltre possibile utilizzare questa funzione per filtrare gli eventi che si desidera inviare a AWS Incident Detection and Response.
4. Configura il tuo APM per inviare notifiche agli utenti URL generati dal API Gateway.

Sviluppa runbook per il rilevamento e la risposta AWS agli incidenti

È possibile scaricare un esempio di runbook di Incident Detection and Response: aws-idr-runbook-example .zip.

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, descritte in precedenza. I piani di risposta sono AWS Systems Manager (SSM) modelli di documento utilizzati per innescare incidenti. Per ulteriori informazioni sui SSM documenti, consulta AWS Systems Manager Documenti, per ulteriori informazioni su Incident Manager, vedi Cos'è AWS Systems Manager Incident Manager?

Risultati chiave:

- Completamento della definizione del carico di lavoro sul rilevamento e la AWS risposta agli incidenti.
- Completamento degli allarmi, dei runbook e della definizione del piano di risposta sul rilevamento e la risposta AWS agli incidenti.

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

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

> **Note**
>
> Il AWS Identity and Access Management l'utente o il ruolo utilizzato per il test degli allarmi deve disporre `cloudwatch:SetAlarmState` dell'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 dell'allarme, 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. AWSIncident Detection and Response segue i passaggi prescritti dal manuale per darti un'idea di 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

AWSIncident Detection and Response verifica 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 a AWS CLI from AWS CloudShell. AWSIncident Detection and Response fornisce un elenco di AWS CLI comandi da utilizzare durante i test.

Esempio AWS CLI comando 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 necessarie per le CloudWatch API operazioni, consulta Amazon CloudWatch permissions reference.

Allarmi di terze parti APM

I carichi di lavoro che utilizzano uno strumento di monitoraggio delle prestazioni delle applicazioni (APM) di terze parti DataDog, come Splunk o Dynatrace NewRelic, richiedono istruzioni diverse per simulare un allarme. All'inizio di GameDay, AWS Incident Detection and Response richiede di modificare temporaneamente le soglie di allarme o gli operatori di confronto per forzare lo stato dell'allarme. ALARM Questo stato attiva un payload per AWS Incident Detection and Response.

Uscite chiave

Risultati chiave:

- L'inserimento degli allarmi ha avuto esito positivo 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.
- AWSIncident Detection and Response può contattarti tramite i mezzi di conferenza prescritti.
- Tutti gli allarmi e i casi di assistenza generati nell'ambito del Gameday sono stati risolti.
- Viene inviata un'e-mail Go-Live per confermare che il carico di lavoro è ora monitorato da Incident Detection and Response. AWS

Questionari di onboarding del carico di lavoro e inserimento degli allarmi

Scarica il questionario di onboarding del 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)	Operazioni di vendita al dettaglio su Amazon (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 di conformità e/o normativi applicabili per questo carico di lavoro e qualsiasi azione richiesta da 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 AWS tag di 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 per accelerare il supporto durante gli incidenti. **Note** I tag rispettano la distinzione tra maiuscole e minuscole. Se fornisci più tag, tutte le risorse utilizzate da questo	appName: Optimax ambiente: Produzione

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

Domanda	Risposta di esempio
Un elenco di AWS Servizi utilizzati da questo carico di lavoro e da AWS Account e 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
Descrivi in dettaglio eventuali component i upstream/downstream non integrati che potrebbero 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.
Ce ne sono di locali o non AWS componenti per questo carico di lavoro? In caso affermati vo, quali sono e quali funzioni vengono eseguite?	Tutto il traffico basato su Internet in entrata/in uscita da AWS viene instradato tramite il nostro servizio proxy locale.
Fornisci dettagli su eventuali piani di failover/ disaster recovery manuali o automatizzati a livello di zona di disponibilità e regionale.	Standby a caldo. Failover automatico verso WEST US-2 durante un calo prolungato della percentuale di successo.

Questionario di onboarding sul carico di lavoro - AWS Domande relative agli eventi di assistenza

AWS Domande sugli eventi di servizio

Domanda	Risposta di esempio
Fornite i dati di contatto (nome/e-mail/telefono) del team interno di gestione degli incidenti gravi e delle crisi informatiche della vostra azienda.	Team di gestione degli incidenti principali mim@example.com +61 2 3456 7890

Domanda	Risposta di esempio
Fornite i dettagli di qualsiasi ponte statico di gestione degli incidenti/crisi stabilito dalla vostra azienda. Se utilizzate ponti non statici, specificate l'applicazione preferita e AWS richiederà questi dettagli durante un incidente. **Note** Se non ne viene fornito uno, allora AWS ti contatterà durante un incidente e ti fornirà un bridge Chime a cui unirti.	Amazon Chime https://chime.aws/1234567890

Questionario sull'ingestione di allarmi

Domande sul runbook

Domanda	Risposta di esempio
AWS coinvolgerà i contatti del carico di lavoro tramite AWS Support Caso. Chi è il contatto principale quando si attiva un allarme per questo carico di lavoro? Specificate l'applicazione di conferenza preferita e AWS richiederà questi dettagli durante un incidente. **Note** Se non viene fornita un'applicazione di conferenza preferita, allora AWS ti contatterà durante un incidente e ti fornirà un bridge Chime a cui unirti.	Team di candidatura app@example.com +61 2 3456 7890

Domanda	Risposta di esempio
Se il contatto principale non è disponibile 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
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

Matrice di allarme

Fornisci le seguenti informazioni per identificare la serie di allarmi che attiveranno il rilevamento e la risposta agli AWS incidenti per creare incidenti per conto del tuo carico di lavoro. Una volta che gli ingegneri di AWS Incident Detection and Response avranno esaminato gli allarmi, verranno fornite ulteriori fasi di onboarding.

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

- AWSGli allarmi di rilevamento e risposta agli incidenti devono entrare nello stato «Allarme» solo in caso di impatto aziendale significativo sul carico di lavoro monitorato (perdita di entrate/peggioramento dell'esperienza del cliente) che richiede l'attenzione immediata dell'operatore.

- AWSGli allarmi di rilevamento e risposta agli incidenti devono inoltre coinvolgere i resolver per il carico di lavoro contemporaneamente o prima dell'attivazione. AWS Gli Incident Manager collaborano con i vostri resolver nel processo di mitigazione e non fungono da soccorritori di prima linea che poi passano a voi.
- AWSLe soglie di allarme di rilevamento e risposta agli incidenti 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 si sposta tra lo stato «Allarme» e «OK», si verifica un impatto sufficiente a giustificare la risposta e l'attenzione dell'operatore.

AWSPolitica di rilevamento e risposta agli incidenti 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 team di ingegneria dell'affidabilità del sito (SRE) se desideri che il team di rilevamento e risposta AWS agli incidenti li chiami dopo aver inviato un'e-mail di coinvolgimento iniziale.

Tabella Alarm Matrix

Nome della metrica/ARN/Threshold	Descrizione	Note	Azioni richieste
Volume del carico di lavoro/ *CW Alarm ARN* / CallCount < 100000 per 5 punti dati entro	Questa metrica rappresenta il numero di richieste in entrata che arrivano al carico di lavoro, misurato a	L'allarme è entrato nello stato «Allarme» 10 volte nell'ultima settimana. Questo allarme è a rischio di falsi positivi. È	Coinvolgi il team di Site Reliability Engineering inviando un'e-mail a *SRE@xyz.com*

Nome della metrica/ARN/Threshold	Descrizione	Note	Azioni richieste
5 minuti, considera i dati mancanti come mancanti	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 DNS implementazione che impediscono agli utenti di accedere al carico di lavoro.	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 dell'affidabilità del sito	Crea un caso AWS Premium Support per i nostri servizi ELB e Route 53. Se è necessari a IMMEDIATE un'azione: controlla Memoria/spazio EC2 libero su disco e informa il *XYZ* Invia un team via e-mail per riavviare l'istanza o esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)

Nome della metrica/ARN/Threshold	Descrizione	Note	Azioni richieste
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 che devono essere soddisfatte dal carico di lavoro. HTTP 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'esecuzi one di un particolare processo in batch. Risolutori: tecnici dell'affidabilità del sito	Coinvolgi il team di Site Reliabili ty Engineering inviando un'e-mail a *SRE@xyz.com* Crea un caso AWS Premium Support per i nostri ECW servizi. RDS Se è necessari a IMMEDIATE un'azione: controlla Memoria/spazio EC2 libero su disco e informa il *XYZ* Invia un team via e-mail per riavviare l'istanza o esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)

Nome della metrica/ARN/Threshold	Descrizione	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 HTTP richieste 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 dell'affidabilità del sito	Coinvolgi il team di Site Reliability Engineering inviando un'e-mail a *SRE@xyz.com* Crea un caso AWS Premium Support per i nostri servizi ELB e Route 53. Se è necessaria a IMMEDIATE un'azione: controlla Memoria/spazio EC2 libero su disco e informa il *XYZ* Invia un team via e-mail per riavviare l'istanza o esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)
Esempio di New Relic Alarm			

Nome della metrica/ARN/Threshold	Descrizione	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: Flusso di lavoro end-to-end del test, AWS regione: EAST US-1, ID AWS account: 012345678910	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 dell'affidabilità del sito	Coinvolgi il team di Site Reliability Engineering inviando un'e-mail a *SRE@xyz.com* Crea un caso AWS Premium Support per i nostri ECS servizi e DynamoDB. Se è necessaria IMMEDIATE un'azione: controlla Memoria/spazio EC2 libero su disco e informa il *XYZ* Invia un team via e-mail per riavviare l'istanza o esegui un log flush. (se non è necessaria un'azione immediata, lascia vuoto)

Richiedi modifiche a un carico di lavoro integrato

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 AWS Support Centra, quindi seleziona Crea caso, come illustrato 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. Per esempio:

   AWSRilevamento e risposta agli incidenti - *workload_name*
7. Inserisci una descrizione per questa modifica. Ad esempio, inserisci «Questa richiesta riguarda le modifiche a un carico di lavoro esistente inserite in Incident Detection and AWS 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, ID2ID3, e così via.
   - Dettagli della modifica: inserisci i dettagli della modifica richiesta.
8. Nella sezione Contatti aggiuntivi - facoltativa, 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. Scegli 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 altri messaggi di posta elettronica.

Offboard di un carico di lavoro

Per eliminare 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 esternalizzare un carico di lavoro racchiuso in un'unica soluzione AWS account, crea la richiesta di assistenza dall'account del carico di lavoro o dal tuo account di pagamento.
- Per esternalizzare un carico di lavoro che si estende su più livelli AWS account, quindi crea la richiesta di assistenza dal tuo account di pagamento. Nel corpo della richiesta di assistenza, elenca tutti gli account IDs da sbloccare.

> **Important**
>
> Se crei una richiesta di assistenza per trasferire un carico di lavoro dall'account errato, potrebbero verificarsi 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 AWS Support Centra, quindi seleziona Crea custodia.
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. Per esempio:

   [Offboard] Rilevamento e risposta agli AWS incidenti - *`workload_name`*
7. Inserisci una descrizione per questa modifica. Ad esempio, inserisci «Questa richiesta riguarda l'offboarding di un carico di lavoro esistente integrato 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, ID2ID3, 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. Scegli Invia.

Monitoraggio e osservabilità di AWS Incident Detection and Response

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

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

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

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

Implementazione dell'osservabilità su AWS Incident Detection and Response

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

- Fase di onboarding: l'osservabilità durante l'onboarding si concentra sul rilevamento di quando i risultati aziendali dell'applicazione sono compromessi. A tal fine, l'osservabilità durante la fase di onboarding si concentra sulla definizione delle metriche chiave dei risultati aziendali a livello di applicazione per notificare le interruzioni dei carichi di lavoro. AWS In questo modo è AWS possibile rispondere prontamente a queste interruzioni e fornire assistenza per il ripristino.
- Fase successiva all'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 Technical Account Manager (TAM).

Gestione degli incidenti con AWS Incident Detection and Response

AWSIncident Detection and Response offre un monitoraggio e una gestione proattivi degli incidenti 24 ore su 24, 7 giorni su 7, forniti da un team designato di responsabili degli incidenti.

1. Generazione di allarmi: gli allarmi attivati sui tuoi carichi di lavoro vengono inviati tramite EventBridge Amazon AWS a Incident Detection and Response. AWSIncident Detection and Response richiama automaticamente il runbook associato all'allarme e avvisa un responsabile degli incidenti. Se sul tuo carico di lavoro si verifica un incidente critico che non viene rilevato dagli allarmi monitorati da AWS Incident Detection and Response, puoi creare un caso di supporto per richiedere una risposta agli incidenti. Per ulteriori informazioni sulla richiesta di un Incident Response, consulta. Richiesta di risposta all'incidente
2. AWS Incident Manager Engagement: L'Incident Manager risponde all'allarme e coinvolge l'utente in una teleconferenza o come diversamente specificato nel runbook. Il responsabile dell'incidente verifica lo stato del Servizi AWS per determinare se l'allarme è correlato a problemi con Servizi AWS viene utilizzato dal carico di lavoro e fornisce consulenza sullo stato dei servizi sottostanti. Se necessario, il responsabile dell'incidente crea quindi un caso per vostro conto e si occupa del diritto AWS esperti per il supporto.

   Perché AWS Incident Detection and Response monitora Servizi AWS specificamente per le vostre applicazioni, AWS Incident Detection and Response potrebbe determinare che l'incidente è correlato a un Servizio AWS problema anche prima di un Servizio AWS l'evento è dichiarato. In questo scenario, il responsabile dell'incidente fornisce informazioni sullo stato del Servizio AWS, attiva il AWS Flusso di Service Event Incident Management e segue il team di assistenza in caso di risoluzione. Le informazioni fornite offrono l'opportunità di implementare tempestivamente i piani o le soluzioni alternative di ripristino per mitigare l'impatto del AWS Evento di servizio. Per ulteriori informazioni, consulta Gestione degli incidenti per gli eventi di servizio.
3. Risoluzione dell'incidente: il responsabile dell'incidente coordina l'incidente in base alle esigenze AWS collabora e si assicura che tu rimanga coinvolto con il diritto AWS esperti fino a quando l'incidente non sarà mitigato o risolto.
4. Revisione successiva all'incidente (se richiesta): dopo un AWS incidente, Incident Detection and Response può eseguire una revisione successiva all'incidente su richiesta dell'utente e generare un rapporto successivo all'incidente. Il rapporto successivo all'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 della causa principale (). RCA Puoi richiederne un'aggiunta RCA 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
AWS Support 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 AWS Support support case on
 behalf of the customer.
```

```
 At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and AWS Support 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 a 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 an 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 AWS Support and TAM team to ensure newly created ALBs are pre-scaled to
 accommodate expected spikes in workload traffic.
```

Fornisci l'accesso ai team delle applicazioni

AWSIncident Detection and Response comunica con l'utente tramite AWS Support casi durante il ciclo di vita di un incidente. Per corrispondere con gli Incident Manager, i team devono avere accesso a AWS Support Centro.

Per ulteriori informazioni sulla fornitura dell'accesso, consulta Gestire l'accesso a AWS Support Centro in AWS Support Guida per l'utente.

Gestione degli incidenti per gli eventi di servizio

AWSIncident Detection and Response ti avvisa di un evento di assistenza in corso nel tuo AWS Regioni, indipendentemente dal fatto che il carico di lavoro ne risenta o meno. Durante un AWS evento di servizio, AWS Incident Detection and Response crea un AWS Support case, si unisce al tuo bridge di teleconferenza per ricevere feedback sull'impatto e sul sentimento e fornisce indicazioni per invocare i tuoi piani di ripristino durante l'evento. Riceverai anche una notifica tramite AWS Health contenente i dettagli dell'evento. Clienti che non sono interessati dal AWS evento di servizio di proprietà (ad esempio, che opera in un altro AWS Regione, non utilizzare il AWS servizio compromesso e così via) continua a essere supportato dal servizio standard. Per ulteriori informazioni sull' AWS Health, vedi Cos'è AWS Health?.

Rapporto post-incidente per eventi di servizio (se richiesto): se un evento di servizio causa un incidente, è possibile richiedere AWS Incident Detection and Response per eseguire una revisione successiva all'incidente e generare un rapporto successivo all'incidente. Il rapporto post-incidente per gli eventi di servizio include quanto segue:

- Una descrizione del problema
- L'impatto dell'incidente
- Informazioni condivise su AWS Health pannello di controllo
- Le squadre impegnate durante l'incidente
- Soluzioni alternative e azioni intraprese per mitigare o risolvere l'incidente

Il rapporto post-incidente per gli eventi di servizio potrebbe contenere informazioni che possono essere utilizzate per ridurre la probabilità che l'incidente si ripeta o per migliorare la gestione delle future occorrenze di un incidente simile. Il rapporto post incidente per gli eventi di servizio non è un'analisi della causa principale (). RCA È possibile richiedere un aggiornamento RCA aggiuntivo al Post Incident Report per gli eventi di servizio.

Di seguito è riportato un esempio di evento Post Incident Report per un evento di servizio:

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

Post Incident Report - LSE000123
Customer: Example Customer
AWS Support Case ID(s): 0000000000
Incident Start: Example: 1 January 2024, 3:30 PM UTC
Incident Resolved: Example: 1 January 2024, 3:30 PM UTC
Incident Duration: 1:02:00
Service(s) Impacted: Lists the impacted services such as EC2, ALB
Region(s): Lists the impacted AWS Regions, such as US-EAST-1
Alarm Identifiers: Lists any customer alarms that triggered during the Service Level Event

Problem Statement:
Outlines impact to end users and operational infrastructure impact during the Service Level Event.
Starting at 2023-02-04T03:25:00 UTC, the customer experienced a service outage...

Impact Summary for Service Level Event:
(This section is limited to approved messaging available on the AWS Health Dashboard)
Outline approved customer messaging as provided on the AWS Health Dashboard.
Between 1:14 PM and 4:33 PM UTC, we experienced increased error rates for the Amazon SNS Publish, Subscribe, Unsubscribe, Create Topic, and Delete Topic APIs in the EU-WEST-1 Region. The issue has been resolved and the service is operating normally.

Incident Summary:
Summary of the incident in chronological order and steps taken by AWS Incident Managers during the Service Level Event to direct the incident to a path to mitigation.
At 2024-01-04T01:25:00 UTC, the workload alarm triggered a critical incident...
At 2024-01-04T01:27:00 UTC, customer was notified via case 000000000 about the triggered alarm
At 2024-01-04T01:30:00 UTC, IDR team identified an ongoing service event which was related to the customer triggered alarm
At 2024-01-04T01:32:00 UTC, IDR team sent an impact case correspondence requesting for the incident bridge details
At 2024-01-04T01:32:00 UTC, customer provided the incident bridge details
At 2024-01-04T01:32:00 UTC, IDR team joined the incident bridge and provided information about the ongoing service outage
By 2024-01-04T02:35:00 UTC, customer failed over to the secondary region (EU-WEST-1) to mitigate impact...
At 2024-01-04T03:27:00 UTC, customer confirmed recovery, the call was spun down...

Mitigation:

```
Describes what was done to mitigate the issue. NOTE: this is not an Root Cause Analysis
 (RCA).
Back-off and retries yielded mild recovery. Full mitigation happened ...

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 ...
Work with AWS Support and TAM team to ensure ...
```

Richiesta di risposta all'incidente

Se sul tuo carico di lavoro si verifica un incidente critico che non viene rilevato dagli allarmi monitorati da AWS Incident Detection and Response, puoi creare un caso di supporto per richiedere una risposta agli incidenti. Puoi richiedere un Incident Response per qualsiasi carico di lavoro sottoscritto a AWS Incident Detection and Response, compresi i carichi di lavoro in fase di onboarding.

Per richiedere una risposta agli incidenti per un incidente che ha un impatto attivo sul tuo carico di lavoro, crea un AWS Support Caso. Una volta sollevata la richiesta di assistenza, AWS Incident Detection and Response vi coinvolgerà in un conference bridge con il AWS esperti necessari per accelerare il recupero del carico di lavoro.

Richiedi una risposta agli incidenti utilizzando il AWS Support Center Console

1. Aprire 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. Per esempio:

   AWSRilevamento e risposta agli incidenti - Incidente attivo - workload_name
7. Inserire 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:

8. 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.

9. Scegli 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.

10. AWSIncident Detection and Response riconosce il vostro caso entro cinque minuti e vi coinvolge in una conferenza telefonica con i responsabili AWS esperti.

Richiedi una risposta all'incidente utilizzando il AWS Support API

I casi di supporto possono essere creati programmaticamente utilizzando il AWS Support API.

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

1. Apri il canale Slack che hai configurato AWS Support App in Slack nel.

2. Immetti il comando seguente:

```
/awssupport create
```

3. Inserisci un oggetto per questo incidente. Ad esempio, inserisci AWSIncident Detection and Response - Active Incident - workload_name.
4. Inserite 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. Per Metodo di contatto, scegli Email e Notifiche Slack.

> **Note**
>
> AWSIncident Detection and Response non supporta la chat dal vivo in Slack. Se selezioni questa opzione, noterai un ritardo nelle risposte alla tua Incident Response Request.

11. Puoi configurare altri contatti affinché ricevano copie della corrispondenza e-mail relativa a questo incidente.

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

14. L'ID del tuo caso viene fornito in un nuovo messaggio dal AWS Support App in Slack.
15. Incident Detection and Response riconosce il vostro caso entro cinque minuti e vi coinvolge in una conferenza telefonica con le autorità competenti AWS esperti.
16. La corrispondenza di Incident Detection and Response viene aggiornata nel thread del caso.

AWSApp di supporto in Slack

AWS i clienti possono utilizzare il AWS Support App in Slackper gestire i propri AWS Support casi in Slack.

AWS I clienti di Incident Detection and Response possono utilizzare il AWS Support App in Slack per ricevere notifiche relative a nuovi incidenti provocati da allarmi sul proprio carico di lavoro o per creare una richiesta di risposta agli incidenti.

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

Important

- Quando aggiorni o crei un caso Support con AWS Rilevamento e risposta agli incidenti tramite AWS Support App in Slack, devi scegliere il metodo di contatto Email and Slack Notifications.

  AWS Incident Detection and Response supporta solo la corrispondenza e-mail nei casi di assistenza. La chat dal vivo non è supportata.

- Per assicurarti di ricevere notifiche in Slack per tutti gli incidenti provocati da allarmi sul tuo carico di lavoro, devi configurare AWS Support App in Slack per tutti gli account del tuo carico di lavoro su cui hai effettuato l'onboarding AWS Rilevamento e risposta agli incidenti. I casi di supporto vengono creati nell'account da cui ha avuto origine l'allarme del carico di lavoro.
- Durante un incidente, è possibile avviare più casi di supporto ad alta gravità per conto dell'utente e intervenire AWS Support resolver. Ricevi notifiche in Slack per tutti i casi di assistenza aperti durante un incidente che corrispondono alla configurazione delle notifiche per il canale Slack.
- Notifiche che ricevi tramite AWS Support App in Slack non sostituite i contatti iniziali e crescenti del vostro carico di lavoro che vengono contattati via e-mail o telefonata con AWS Rilevamento e risposta agli incidenti durante un incidente.

Notifiche di incidenti avviati da un allarme in Slack

Quando l'app AWS Support in Slack è configurata nel tuo canale Slack, ricevi una notifica 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 dall'allarme viene riconosciuto da AWS Incident Detection and Response, in Slack verrà generata una notifica simile alla seguente:

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

Ulteriori aggiornamenti relativi a 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.

Richieste di risposta agli incidenti in Slack

Per istruzioni su come creare una richiesta di risposta agli incidenti tramite l'app AWS Support in Slack, consulta Incident Response Requests.

Reportistica di AWS Incident Detection and Response

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.

Dati di configurazione

- Tutti gli account sono stati 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 responsabilità condivisa di AWS si applica alla protezione dei dati in AWS Support. 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 le risorse. AWS 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, consulta AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi. Per informazioni, consulta Servizi e strumenti di AWS crittografia.
- 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 l'accesso 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 AWS Support o Servizi AWS utilizzi la console, l'API, la AWS CLI o AWS gli SDK. 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 IDR guida.

- Ultimo aggiornamento della documentazione: 12 giugno 2024

Modifica	Descrizione	Data
È stata aggiunta una nuova pagina AWS Support App in Slack Gestione degli incidenti aggiornata 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 il 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: Abbonamento all'account	12 giugno 2024
Post Incident Report per gli eventi di assistenza è ora disponibile	È stata aggiornata la sezione Gestione degli incidenti per gli eventi di servizio per includere informazioni sul rapporto post-incidente per gli eventi di servizio. Sezione aggiornata: Gestione degli incidenti per gli eventi di servizio	8 maggio 2024
Aggiunta una nuova sezione: Offboard a workload	È stata aggiunta la sezione Offload a workload in Guida introduttiva per includere informazioni sui carichi di lavoro di offboarding	28 marzo 2024

Modifica	Descrizione	Data
	Per ulteriori informazioni, consulta Offboard di un carico di lavoro.	
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	29 febbraio 2024
Aggiornato Cos'è il rilevamento e la risposta agli AWS incidenti	È stata aggiornata la sezione Cos'è il rilevamento e la risposta agli AWS incidenti. Sezione aggiornata: Cos'è AWS Incident Detection and Response?	19 febbraio 2024
Sezione Questionario aggiornata	È stato aggiornato il questionario di onboarding del carico di lavoro e aggiunto il questionario di inserimento degli allarmi. La sezione è stata rinominata da Questionario di onboarding a Questionari di onboarding del carico di lavoro e Alarm ingestion. Sezione aggiornata: Questionari di onboarding del carico di lavoro e inserimento degli allarmi	2 febbraio 2024

Modifica	Descrizione	Data
Aggiornato AWS Informazioni sull'evento di servizio e sull'onboarding	Sono state aggiornate diverse sezioni con nuove informazioni per l'onboarding. Sezioni aggiornate: • Gestione degli incidenti per gli eventi di servizio • Individuazione del carico di lavoro • Onboarding • Abbonamento all'account Nuove sezioni • Fornisci l'accesso 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: Fornisci l'accesso per l'inserimento degli avvisi in modalità Incident Detection and Response	17 gennaio 2024
Passaggi di esempio aggiornati	È stata aggiornata la procedura per i passaggi 2,3 e 4 in Esempio: integrazione delle notifiche da Datadog e Splunk. Sezione aggiornata: Esempio: 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 per il rilevamento e la risposta AWS agli incidenti	21 dicembre 2023

Modifica	Descrizione	Data
Modello di runbook aggiornato	Aggiornato il modello di runbook in Sviluppo di runbook per il rilevamento e la risposta AWS agli incidenti. Sezione aggiornata: Sviluppa runbook per il rilevamento e la risposta AWS agli incidenti	4 dicembre 2023
Configurazioni di allarme aggiornate	Configurazioni di allarme aggiornate con informazioni dettagliate sulla configurazione degli CloudWatch allarmi. Nuova sezione: Crea CloudWatch allarmi adatti alle tue esigenze aziendali in Incident Detection and Response Nuova sezione: Utilizzo AWS CloudFormation modelli per creare CloudWatch allarmi in Incident Detection and Response 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 Sezione aggiornata: Abbonamento all'account	05 settembre 2023
Nuova sezione in Guida introduttiva	Aggiunti avvisi di inserimento in Inserisci avvisi in Incident Detection AWS and Response Incident Detection and AWS Response.	30 giugno 2023
Documento originale	AWSRilevamento e risposta agli incidenti pubblicati per la prima volta	15 marzo 2023

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

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.