aws

Guida per l'utente

Incident Manager

Incident Manager: Guida per l’utente

Table of Contents

Strumento di gestione degli incidenti AWS Systems Manager non è più aperto a nuovi clienti. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Strumento di gestione degli incidenti AWS Systems Manager la pagina Modifica della disponibilità.

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.

Che cos'è Strumento di gestione degli incidenti AWS Systems Manager?

Incident Manager, uno strumento di AWS Systems Manager, è progettato per aiutarti a mitigare e ripristinare gli incidenti che interessano le applicazioni ospitate su. AWS

Nel contesto di AWS, per incidente si intende qualsiasi interruzione o riduzione non pianificata della qualità dei servizi che può avere un impatto significativo sulle operazioni aziendali. Pertanto, è fondamentale che le organizzazioni stabiliscano una strategia di risposta per mitigare e recuperare in modo efficiente gli incidenti e implementare azioni per prevenire incidenti futuri.

Incident Manager aiuta a ridurre i tempi di risoluzione degli incidenti mediante:

- Fornire piani automatizzati per coinvolgere in modo efficiente le persone responsabili della risposta agli incidenti.
- Fornitura di dati pertinenti per la risoluzione dei problemi.
- Abilitazione di azioni di risposta automatizzate utilizzando runbook di automazione predefiniti.
- Fornire metodi per collaborare e comunicare con tutte le parti interessate.

Le funzionalità e i flussi di lavoro integrati in Incident Manager si basano sulle migliori pratiche per la risposta agli incidenti che Amazon ha sviluppato fin dalla sua nascita. Incident Manager si integra con Amazon CloudWatch, AWS CloudTrail AWS Systems Manager, e Amazon EventBridge. Servizi AWS

Componenti e funzionalità principali

Questa sezione descrive le funzionalità di Incident Manager utilizzate per configurare i piani di risposta agli incidenti.

Piano di risposta

Un piano di risposta funziona come un modello che definisce cosa deve essere messo in atto quando si verifica un incidente. Include informazioni come:

- Chi è tenuto a rispondere quando si verifica un incidente.
- La risposta automatica stabilita per mitigare l'incidente.

- Lo strumento di collaborazione che i soccorritori devono utilizzare per comunicare e ricevere notifiche automatiche sull'incidente.

Rilevamento degli incidenti

Puoi configurare Amazon CloudWatch alarms e Amazon EventBridge Events per creare incidenti quando vengono rilevate condizioni o modifiche che influiscono sulle tue AWS risorse.

Supporto per l'automazione Runbook

È possibile avviare i runbook di automazione dall'interno di Incident Manager per automatizzare la risposta critica agli incidenti e fornire passaggi dettagliati ai primi soccorritori.

Coinvolgimento ed escalation

Un piano di coinvolgimento specifica tutti coloro che devono notificare ogni singolo incidente. È possibile specificare i singoli contatti che sono stati aggiunti a Incident Manager o specificare una pianificazione delle chiamate creata in Incident Manager. I piani di coinvolgimento specificano anche un percorso di escalation per contribuire a garantire la visibilità tra le parti interessate e la partecipazione attiva durante il processo di risposta agli incidenti.

Orari di chiamata

Una pianificazione delle chiamate in Incident Manager consiste in una o più rotazioni create dall'utente per la pianificazione. Per ogni rotazione, puoi includere fino a 30 contatti. Se aggiunto a un piano di escalation o a un piano di risposta, il programma di chiamata definisce chi riceve una notifica quando si verifica un incidente che richiede l'intervento del soccorritore. Gli orari di chiamata aiutano a garantire una copertura completa e ridondante 24 ore su 24, 7 giorni su 7, in base alle esigenze di risposta agli incidenti.

Collaborazione attiva

I soccorritori rispondono attivamente agli incidenti attraverso l'integrazione con il client di applicazioni di chat Amazon Q Developer. Amazon Q Developer nelle applicazioni di chat supporta la creazione di canali di chat per Incident Manager che utilizzano Slack, Microsoft Teamso Amazon Chime. I soccorritori possono comunicare direttamente tra loro, ricevere notifiche automatiche sugli incidenti e, Slack e Microsoft Teams—esegue direttamente alcune operazioni dell'interfaccia a riga di comando (CLI) di Incident Manager.

Diagnosi degli incidenti

I soccorritori possono visualizzare up-to-date le informazioni nella console Incident Manager durante un incidente. In base alle modifiche delle informazioni, i soccorritori possono quindi creare elementi di follow-up e porvi rimedio utilizzando i runbook di automazione.

Risultati tratti da altri servizi

Per supportare la diagnosi degli incidenti da parte dei soccorritori, puoi abilitare la funzionalità Findings in Incident Manager. I risultati sono informazioni sulle AWS CodeDeploy implementazioni e sugli aggiornamenti degli AWS CloudFormation stack avvenuti nel periodo in cui si è verificato un incidente e che hanno coinvolto una o più risorse probabilmente correlate all'incidente. La disponibilità di queste informazioni riduce il tempo necessario per valutare le potenziali cause, il che può ridurre il tempo medio di ripristino (MTTR) da un incidente.

Analisi post-incidente

Dopo la risoluzione di un incidente, si utilizza un'analisi post-incidente per identificare i miglioramenti apportati alla risposta all'incidente, compresi i tempi di rilevamento e mitigazione. Un'analisi può anche aiutarti a comprendere la causa principale degli incidenti. Incident Manager crea azioni di follow-up consigliate che è possibile utilizzare per migliorare la risposta agli incidenti.

Vantaggi dell'utilizzo di Incident Manager

Scopri i vantaggi dell'utilizzo di Incident Manager nelle operazioni di rilevamento e risposta agli incidenti.

Questa sezione descrive i vantaggi che l'organizzazione può ottenere implementando un piano di risposta di Incident Manager.

Diagnostica i problemi in modo efficiente e immediato

Gli CloudWatch allarmi Amazon e EventBridge gli eventi Amazon che configuri possono creare incidenti automaticamente in caso di interruzione o riduzione non pianificata della qualità dei tuoi servizi.

CloudWatch gli allarmi rilevano e segnalano quando ci sono modifiche al valore della metrica o dell'espressione relativa a una soglia in un certo numero di periodi di tempo. EventBridge gli eventi vengono creati come risultato di modifiche in un ambiente, un'applicazione o un servizio specificato in una EventBridge regola. Quando si crea un allarme o un evento, è possibile specificare un'azione per un incidente da creare in Incident Manager e il piano di risposta appropriato per facilitare il coinvolgimento, l'intensificazione e la mitigazione dell'incidente.

Incident Manager offre la possibilità di raccogliere e tracciare automaticamente le metriche relative a un incidente, tramite l'uso di metriche. CloudWatch Oltre alle metriche automatizzate generate per

l'incidente quando viene creato tramite un CloudWatch allarme, è possibile aggiungere metriche manualmente in tempo reale, per fornire contesto e dati aggiuntivi ai soccorritori in caso di incidente.

Utilizza la cronologia degli incidenti di Incident Manager per visualizzare i punti di interesse in ordine cronologico. I soccorritori possono anche utilizzare la sequenza temporale per aggiungere eventi personalizzati per descrivere cosa hanno fatto o cosa è successo. I punti di interesse automatici includono:

- Un CloudWatch allarme o una EventBridge regola crea un incidente.
- Le metriche degli incidenti vengono segnalate a Incident Manager.
- I soccorritori sono coinvolti.
- I passaggi del Runbook sono stati completati correttamente.

Impegnati efficacemente

Incident Manager riunisce i soccorritori attraverso l'uso di contatti, pianificazioni delle chiamate, piani di intervento e canali di chat. È possibile definire i singoli contatti direttamente in Incident Manager e specificare le preferenze di contatto (e-mail, SMS o voce). I contatti vengono aggiunti alle rotazioni programmate durante le chiamate per determinare chi è incaricato di gestire gli incidenti durante un determinato periodo. Utilizzando i contatti definiti e gli orari di chiamata, si creano piani di emergenza per coinvolgere i soccorritori necessari al momento giusto durante un incidente.

Collabora in tempo reale

La comunicazione durante un incidente è la chiave per una risoluzione più rapida. Utilizzo di un Amazon Q Developer in un client di applicazioni di chat configurato per l'uso Slack, Microsoft Teams, o Amazon Chime, puoi riunire i soccorritori nel loro canale di chat connesso preferito, dove interagiscono direttamente con l'incidente e tra loro. Incident Manager mostra anche le azioni in tempo reale dei soccorritori nel canale di chat, fornendo un contesto agli altri.

Automatizza il ripristino del servizio

Incident Manager consente ai soccorritori di concentrarsi sulle attività chiave necessarie per risolvere un incidente tramite l'uso dei runbook di automazione. In Incident Manager, i runbook sono una serie predefinita di azioni intraprese per risolvere un incidente. Combinano la potenza delle attività automatizzate con i passaggi manuali in base alle necessità, lasciando i soccorritori più disponibili ad analizzare e rispondere all'impatto.

Prevenire incidenti futuri

Utilizzando l'analisi post-incidente di Incident Manager, il team può sviluppare piani di risposta più solidi e apportare modifiche alle applicazioni per prevenire incidenti e tempi di inattività futuri. L'analisi post-incidente consente inoltre l'apprendimento iterativo e il miglioramento dei runbook, dei piani di risposta e delle metriche.

Servizi correlati

Incident Manager si integra con diversi servizi Servizi AWS e strumenti di terze parti per aiutarti a rilevare e risolvere gli incidenti e a interagire indirettamente con le sue operazioni API e gestire l'infrastruttura. Per informazioni, consultare Integrazioni di prodotti e servizi con Incident Manager.

Accesso a Incident Manager

È possibile accedere a Incident Manager in uno dei seguenti modi:

- La console Incident Manager
- AWS CLI— Per informazioni generali, vedere Guida introduttiva AWS CLI alla Guida per l'AWS Command Line Interface utente. Per informazioni sui comandi CLI per Incident Manager, vedere ssm-incidents e ssm-contactsnel riferimento ai AWS CLI comandi.
- API Incident Manager: per ulteriori informazioni, consulta l'Strumento di gestione degli incidenti AWS Systems Manager API Reference.
- AWS SDKs— Per ulteriori informazioni, vedere Strumenti su cui basarsi AWS.

Regioni e quote di Incident Manager

Incident Manager non è supportato in tutti i Regioni AWS formati supportati da Systems Manager.

Per visualizzare informazioni sulle regioni e sulle quote di Incident Manager, consulta Strumento di gestione degli incidenti AWS Systems Manager endpoint e quote in. Riferimenti generali di Amazon Web Services

Prezzi per Incident Manager

L'utilizzo di Incident Manager è a pagamento. Per ulteriori informazioni, consulta la pagina AWS dei prezzi di Systems Manager.

> **Note**
>
> Altri Servizi AWS contenuti e AWS contenuti di terze parti resi disponibili in relazione a questo servizio possono essere soggetti a costi separati e regolati da condizioni aggiuntive.

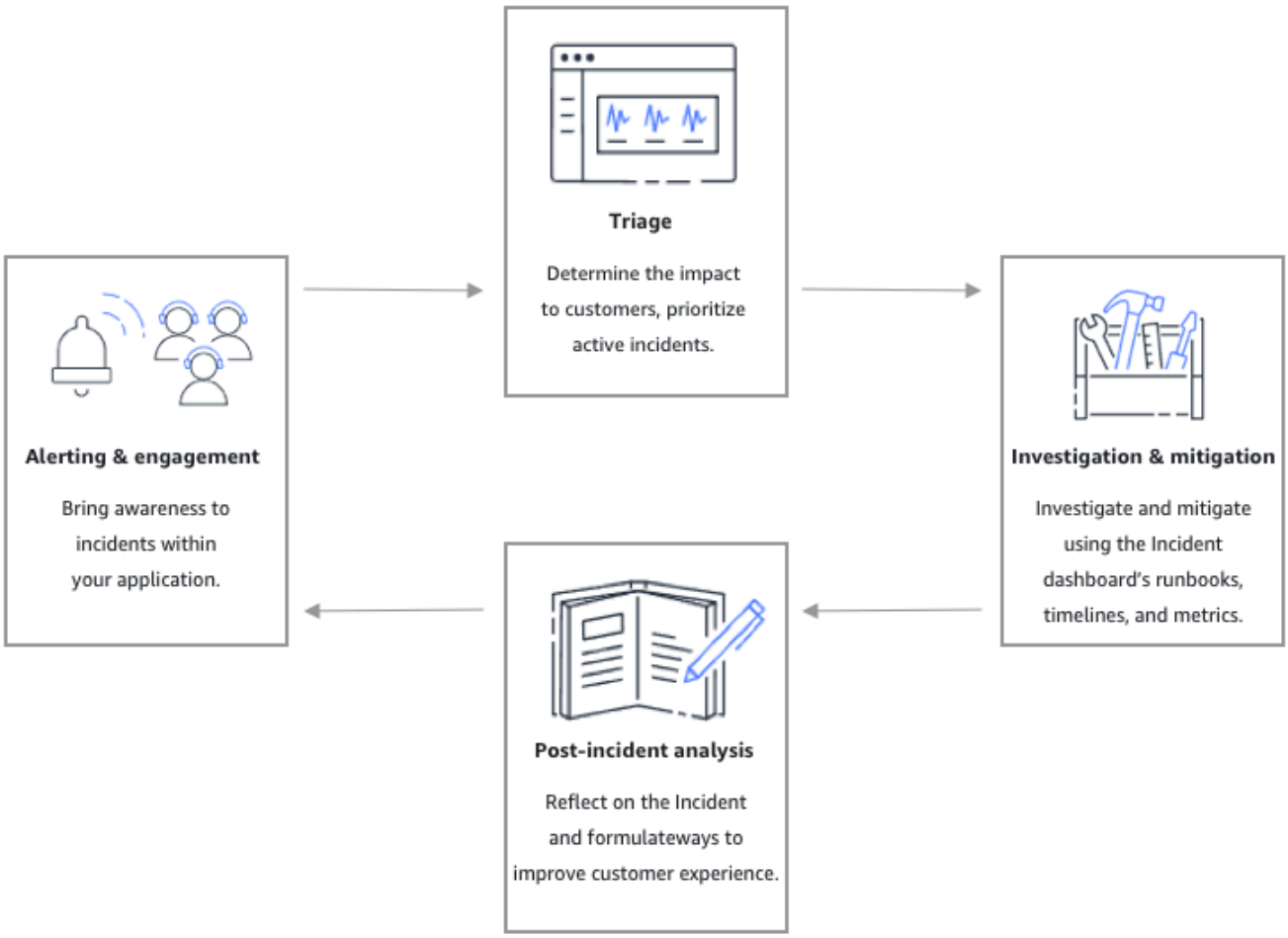
Per una panoramica di Trusted Advisor un servizio che consente di ottimizzare i costi, la sicurezza e le prestazioni dell' AWS ambiente, consulta AWS Trusted Advisorla Guida per l'Supporto AWS utente.

Ciclo di vita degli incidenti in Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager fornisce un step-by-step framework basato sulle migliori pratiche per identificare e reagire agli incidenti, come interruzioni del servizio o minacce alla sicurezza. L'obiettivo principale di Incident Manager è aiutare a ripristinare i servizi o le applicazioni interessati alla normalità il più rapidamente possibile attraverso una soluzione completa di gestione del ciclo di vita degli incidenti.

Come illustrato nella figura seguente, Incident Manager fornisce strumenti e best practice per ogni fase del ciclo di vita dell'incidente:

- Avvisi e coinvolgimento
- Triage
- Indagine e mitigazione
- Analisi post-incidente



Avvisi e coinvolgimento

La fase di avviso e coinvolgimento del ciclo di vita degli incidenti si concentra sulla sensibilizzazione agli incidenti all'interno delle applicazioni e dei servizi. Questa fase inizia prima che venga rilevato un incidente e richiede una comprensione approfondita delle applicazioni. Puoi utilizzare i CloudWatchparametri di Amazon per monitorare i dati sulle prestazioni delle tue applicazioni o utilizzare Amazon EventBridge per aggregare avvisi provenienti da diverse fonti, applicazioni e servizi. Dopo aver impostato il monitoraggio delle applicazioni, puoi iniziare a inviare avvisi in caso di metriche che non rientrano nella norma storica. Per ulteriori informazioni sulle best practice di monitoraggio, consulta. Monitoraggio

Per supportare la diagnosi degli incidenti da parte dei soccorritori, puoi abilitare la funzionalità Findings in Incident Manager. I risultati sono informazioni sulle AWS CodeDeploy implementazioni e sugli aggiornamenti degli AWS CloudFormation stack avvenuti nel periodo in cui si è verificato un

incidente. La disponibilità di queste informazioni riduce il tempo necessario per valutare le potenziali cause, il che può ridurre il tempo medio di ripristino (MTTR) a seguito di un incidente.

Ora che state monitorando gli incidenti nelle vostre applicazioni, potete definire un piano di risposta agli incidenti da utilizzare durante un incidente. Per ulteriori informazioni sulla creazione di piani di risposta, consultaCreazione e configurazione dei piani di risposta in Incident Manager. Amazon EventBridge Events or CloudWatch Alarms può creare automaticamente un incidente utilizzando i piani di risposta come modello. Per ulteriori informazioni sulla creazione di incidenti, consultaCreazione automatica o manuale di incidenti in Incident Manager.

I piani di risposta lanciano piani di intensificazione e piani di coinvolgimento correlati per coinvolgere i primi soccorritori nell'incidente. Per ulteriori informazioni sulla configurazione dei piani di escalation, vedere. Crea un piano di escalation Contemporaneamente, Amazon Q Developer nelle applicazioni di chat invia notifiche ai soccorritori utilizzando un canale di chat indirizzandoli alla pagina dei dettagli dell'incidente. Utilizzando il canale di chat e i dettagli dell'incidente, il team può comunicare e valutare un incidente. Per ulteriori informazioni sulla configurazione dei canali di chat in Incident Manager, consultaAttività 2: creare un canale di chat in Amazon Q Developer nelle applicazioni di chat.

Triage

Il triage è il momento in cui i primi soccorritori cercano di determinare l'impatto sui clienti. La visualizzazione dei dettagli dell'incidente nella console Incident Manager fornisce ai soccorritori tempistiche e metriche per aiutarli a valutare l'incidente. La valutazione dell'impatto di un incidente pone anche le basi per i tempi di risposta, la risoluzione e la comunicazione dell'incidente. I soccorritori danno priorità agli incidenti utilizzando valutazioni di impatto da 1 (Critico) a 5 (Nessun impatto).

La tua organizzazione può definire l'ambito esatto di ogni valutazione di impatto come preferisci. La tabella seguente fornisce esempi di come ogni livello di impatto potrebbe essere generalmente definito.

Codice di impatto	Nome dell'impatto	Esempio di ambito definito
1	`Critical`	Errore completo dell'appl icazione che ha un impatto sulla maggior parte dei clienti.

Codice di impatto	Nome dell'impatto	Esempio di ambito definito
2	`High`	Errore completo dell'appl icazione che ha un impatto su un sottoinsieme di clienti.
3	`Medium`	Errore parziale dell'appl icazione con ripercussioni sul cliente.
4	`Low`	Guasti intermittenti che hanno un impatto limitato sui clienti.
5	`No Impact`	I clienti non sono attualmente interessati, ma è necessaria un'azione urgente per evitare l'impatto.

Indagine e mitigazione

La visualizzazione dei dettagli degli incidenti fornisce al team i runbook, le tempistiche e le metriche. Per scoprire come gestire un incidente, consulta il. Visualizzazione dei dettagli degli incidenti nella console

I runbook forniscono comunemente procedure di indagine e possono estrarre automaticamente dati o tentare soluzioni di uso comune. I runbook forniscono anche passaggi chiari e ripetibili che il team ha ritenuto utili per mitigare gli incidenti. La scheda Runbook si concentra sulla fase corrente del runbook e mostra le fasi passate e future.

Incident Manager si integra con Systems Manager Automation per creare runbook. Usa i runbook per eseguire una delle seguenti operazioni:

- Gestisci istanze e risorse AWS
- Esegui automaticamente gli script
- Gestisci le risorse CloudFormation

Per ulteriori informazioni sui tipi di azioni supportati, vedere il riferimento alle azioni di Systems Manager Automation nella Guida per l'AWS Systems Manager utente.

La scheda Cronologia mostra quali azioni sono state intraprese. La timeline registra ciascuna con un timestamp e dettagli creati automaticamente. Per aggiungere eventi personalizzati alla sequenza temporale, consulta la Sequenza temporale sezione nella pagina dei dettagli dell'incidente di questa guida per l'utente.

La scheda Diagnosi mostra le metriche compilate automaticamente e le metriche aggiunte manualmente. Questa visualizzazione fornisce informazioni preziose sulle attività dell'applicazione durante un incidente.

La scheda Impegni consente di aggiungere altri contatti all'incidente e aiuta a fornire le risorse necessarie per consentire al contatto coinvolto di mettersi rapidamente al corrente una volta coinvolto nell'incidente. I contatti vengono coinvolti attraverso piani di escalation definiti o piani di coinvolgimento personali.

Utilizzando un canale di chat, puoi interagire direttamente con il tuo incidente e con gli altri soccorritori del tuo team. Utilizzando Amazon Q Developer nelle applicazioni di chat, puoi configurare i canali di chat in. Slack, Microsoft Teamse Amazon Chime. In Slack e Microsoft Teams canali, i soccorritori possono interagire con gli incidenti direttamente dal canale di chat utilizzando una serie di comandi. `ssm-incidents` Per ulteriori informazioni, consulta Interagire tramite il canale di chat.

Analisi post-incidente

Incident Manager fornisce un framework per riflettere su un incidente, adottare le misure necessarie per evitare che l'incidente si ripeta in futuro e per migliorare le attività di risposta agli incidenti in generale. I miglioramenti possono includere:

- Modifiche alle applicazioni coinvolte in un incidente. Il tuo team può utilizzare questo tempo per migliorare il sistema e renderlo più tollerante ai guasti.
- Modifiche a un piano di risposta agli incidenti. Prenditi il tempo necessario per incorporare le lezioni apprese.
- Modifiche ai runbook. Il tuo team può approfondire i passaggi necessari per la risoluzione e i passaggi che puoi automatizzare.
- Modifiche agli avvisi. Dopo un incidente, il tuo team potrebbe aver notato dei punti critici nelle metriche che puoi utilizzare per avvisare il team prima di un incidente.

Incident Manager facilita questi potenziali miglioramenti utilizzando una serie di domande di analisi post-incidente e di azioni da intraprendere insieme alla cronologia dell'incidente. Per ulteriori informazioni sul miglioramento attraverso l'analisi, vedere. Performing a post-incident analysis in Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager modifica della disponibilità

Dopo un'attenta valutazione, AWS ha deciso di smettere di accettare nuovi clienti su AWS Systems Manager Incident Manager a partire dal 7 novembre 2025 e in futuro non aggiungerà più nuove funzionalità o funzionalità a Incident Manager. AWS continueranno a investire nella sicurezza e nella disponibilità di Incident Manager e gli attuali clienti di Incident Manager potranno continuare a utilizzare il servizio normalmente negli account in cui Incident Manager è già abilitato.

Poiché Incident Manager non aggiungerà più nuove funzionalità o funzionalità, è importante comprendere le alternative disponibili per la gestione degli incidenti. Per ulteriori informazioni sulle alternative, vedereGuide alla migrazione.

Quando si esegue la migrazione da Incident Manager a una soluzione alternativa, si consiglia di esportare i dati degli incidenti per ulteriori analisi o scopi di archiviazione. Per ulteriori informazioni, consulta Esportazione dei dati di Incident Manager.

Una volta completata la migrazione, consigliamo inoltre di ripulire le risorse rimanenti di Incident Manager per evitare addebiti continui. Per ulteriori informazioni, consulta Pulizia delle risorse di Incident Manager.

Per ulteriore assistenza, puoi contattare il tuo Technical Account Manager o creare una richiesta di supporto nel Support Center di Console di gestione AWS.

Guide alla migrazione

Poiché non Strumento di gestione degli incidenti AWS Systems Manager verranno più aggiunte nuove funzionalità o funzionalità, è importante comprendere le alternative per la gestione degli incidenti. Questa sezione fornisce guide alla migrazione per aiutarti a passare da Incident Manager a soluzioni alternative.

Per gestire i problemi operativi sulla tua AWS infrastruttura, ti consigliamo di utilizzare AWS Systems Manager OpsCenter. Per le funzionalità di paging e risposta automatizzate, consigliamo le soluzioni offerte dai nostri AWS partner Partner Network. AWS I Solution Architect e i Technical Account Manager saranno in grado di guidarvi verso l'opzione più adatta in base alle vostre esigenze specifiche.

Puoi anche consultare le seguenti guide alla migrazione per l'integrazione con le soluzioni dei partner:

- Migrazione verso AWS Systems Manager OpsCenter
- Migrazione a Jira Service Management
- Migrazione verso ServiceNow
- Migrazione verso PagerDuty

Migrazione verso AWS Systems Manager OpsCenter

AWS Systems Manager OpsCenter, una funzionalità di AWS Systems Manager, fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono visualizzare, esaminare e risolvere gli elementi di lavoro operativi (OpsItems) relativi alle AWS risorse. OpsCenter è progettato per ridurre il tempo medio di risoluzione (MTTR) dei problemi che influiscono AWS sulle risorse. OpsCenter aggrega e standardizza OpsItems tutti i servizi fornendo al contempo dati di indagine contestuali su ciascuna risorsa correlata e OpsItem correlata. OpsItems OpsCenter si integra con Systems Manager Automation, che consente di utilizzare i runbook di automazione per analizzare e risolvere i problemi. È possibile visualizzare report di riepilogo generati automaticamente suddivisi per stato e origine. OpsItems Puoi anche utilizzare la funzionalità cross-account OpsCenter di cui dispone per gestire centralmente più account. OpsItems Tieni presente che ci sono costi associati all' OpsCenter uso. Per maggiori dettagli, consulta la pagina AWS Systems Manager dei prezzi.

Simile a Incident Manager, OpsCenter ha integrazioni con Amazon CloudWatch e Amazon EventBridge. Ciò significa che è possibile configurare questi servizi per creare automaticamente un OpsItem ingresso OpsCenter quando un CloudWatch allarme entra nello `ALARM` stato o quando EventBridge elabora un evento proveniente da uno Servizio AWS che pubblica eventi. La configurazione di CloudWatch allarmi ed EventBridge eventi per la creazione automatica OpsItems consente di diagnosticare e risolvere rapidamente i problemi relativi alle AWS risorse da un'unica console. Se disponi di CloudWatch allarmi e EventBridge regole esistenti integrati con Incident Manager, ti consigliamo di aggiornare gli CloudWatch allarmi e le regole per l'integrazione con. EventBridge OpsCenter Consulta la nostra documentazione tecnica per istruzioni dettagliate sull'integrazione degli CloudWatch allarmi OpsCenter o sull'integrazione degli eventi con. EventBridge OpsCenter

Migrazione a Jira Service Management

Jira Service Management (JSM) è una soluzione di gestione dei servizi IT (ITSM) che aiuta i team a ricevere, tracciare, gestire e risolvere le richieste di dipendenti e clienti attraverso più canali, tra cui e-mail, chat, centri assistenza e widget. Basato sulla piattaforma Jira, Jira Service Management consente ai team di un'organizzazione, dallo sviluppo all'IT alle risorse umane, di ricevere richieste, rispondere ad avvisi e incidenti, implementare modifiche, tenere traccia delle risorse, far emergere le conoscenze e automatizzare i flussi di lavoro. Jira Service Management include funzionalità di gestione degli incidenti come la pianificazione delle chiamate, gli avvisi, la gestione degli incidenti gravi, la gestione delle modifiche e le funzionalità post mortem (PIR) senza colpa progettate per i DevOps flussi di lavoro, sfruttando le CI/CD pipeline e l'automazione esistenti per ridurre lo sforzo manuale.

Jira Service Management si integra con Amazon e CloudWatch Amazon EventBridge, consentendoti di creare automaticamente avvisi di Jira Service Management quando gli CloudWatch allarmi entrano `ALARM` nello stato o quando EventBridge elabora gli eventi di qualsiasi azienda che pubblica eventi. Servizio AWS La configurazione di CloudWatch allarmi ed EventBridge eventi per creare automaticamente avvisi di Jira Service Management consente di diagnosticare e risolvere rapidamente i problemi con le risorse da un'unica piattaforma. AWS Jira Service Management funge da spedizioniere, notificando le persone giuste attraverso più canali (e-mail, SMS, telefonate, notifiche push su dispositivi mobili) in base agli orari delle chiamate e alle politiche di escalation.

Se hai già integrato CloudWatch allarmi e EventBridge regole con Strumento di gestione degli incidenti AWS Systems Manager, ti consigliamo di aggiornare tali integrazioni per utilizzare invece Jira Service Management. La documentazione ufficiale di Atlassian fornisce istruzioni dettagliate per l'integrazione di Jira Service Management con e l'integrazione di Jira Service Management con CloudWatch. EventBridge

Oltre alla creazione automatica di avvisi, Jira Service Management offre una gamma di funzionalità per semplificare la gestione degli incidenti, come la pianificazione delle chiamate, le politiche di escalation e le regole di automazione. I clienti possono fare riferimento alla seguente documentazione Atlassian per i dettagli sulla configurazione di queste funzionalità:

- Scopri gli avvisi e il servizio di chiamata
- Crea orari di chiamata
- Crea politiche di escalation
- Configura team e persone

- Imposta i metodi di contatto
- Configura le regole di notifica
- Configura notifiche vocali e SMS
- Imposta le regole di automazione
- Imposta e gestisci le parti interessate all'incidente

Per ulteriore assistenza, puoi contattare il tuo Technical Account Manager o un rappresentante di vendita Atlassian per ulteriori informazioni.

Migrazione verso ServiceNow

ServiceNow Incident Management è un modulo ITSM di base progettato per ripristinare le normali operazioni di servizio dopo interruzioni non pianificate, riducendo al minimo l'impatto aziendale. Analogamente a ServiceNow Incident Manager, Incident Management fornisce un sistema strutturato e automatizzato per visualizzare, indagare e risolvere gli incidenti IT, con funzionalità come l'assegnazione automatica delle priorità e processi di escalation integrati.

Il modulo ServiceNow Service Operations with Incident Management and Event management si integra con Amazon CloudWatch, consentendoti di creare automaticamente ServiceNow eventi/avvisi e incidenti quando CloudWatch gli allarmi entrano nello stato. `ALARM` La configurazione degli CloudWatch allarmi per creare automaticamente ServiceNow gli incidenti con webhook to AIOps event management consente di diagnosticare e risolvere rapidamente i problemi con risorse da un'unica piattaforma. AWS

Se disponi di CloudWatch allarmi esistenti integrati con Strumento di gestione degli incidenti AWS Systems Manager, ti consigliamo di aggiornare tali integrazioni per utilizzare ServiceNow invece la gestione degli incidenti e la piattaforma di intelligence degli eventi. AIOps La ServiceNow documentazione ufficiale fornisce istruzioni dettagliate per l'integrazione ServiceNow con Amazon CloudWatch.

Oltre alla creazione automatizzata degli ServiceNow incidenti, Incident Management offre una serie di funzionalità per migliorare la gestione degli incidenti, come la gestione delle comunicazioni degli incidenti, la pianificazione delle chiamate, le politiche di escalation e altro ancora. I clienti possono fare riferimento alla seguente ServiceNow documentazione per i dettagli sulla configurazione di queste funzionalità:

- Documentazione sulla gestione degli incidenti

- Gestione dell'affidabilità del servizio
- Gestione e contatti delle comunicazioni relative agli incidenti
- Orari di chiamata
- Processo di intensificazione

Per ulteriore assistenza, puoi contattare il tuo Technical Account Manager o un rappresentante di ServiceNow vendita per ulteriori informazioni.

Migrazione verso PagerDuty

PagerDutyè una piattaforma di gestione degli incidenti che aiuta le organizzazioni a rilevare, rispondere e persino prevenire gli incidenti. Come Incident Manager, PagerDuty fornisce una posizione centrale in cui i team operativi affrontano il lavoro critico relativo alle AWS risorse, riducendo l'impatto sui clienti.

PagerDuty si integra con Amazon CloudWatch e Amazon EventBridge, consentendoti di creare automaticamente PagerDuty incidenti quando gli CloudWatch allarmi entrano nello `ALARM` stato o quando EventBridge elabora eventi da qualsiasi azienda Servizio AWS che pubblica eventi. Configurando CloudWatch allarmi ed EventBridge eventi per creare automaticamente PagerDuty incidenti, puoi diagnosticare e risolvere rapidamente i problemi relativi alle risorse da un'unica piattaforma. AWS

Se hai già integrato CloudWatch allarmi e EventBridge regole con Strumento di gestione degli incidenti AWS Systems Manager, ti consigliamo di aggiornare tali integrazioni per utilizzarle al loro posto. PagerDuty La PagerDuty documentazione ufficiale fornisce istruzioni dettagliate per l'integrazione CloudWatch e l'integrazione PagerDuty con. PagerDuty EventBridge

Oltre alla creazione automatizzata degli incidenti, PagerDuty offre una gamma di funzionalità per migliorare la gestione degli incidenti, come la pianificazione su chiamata, le politiche di escalation e oltre 700 integrazioni di piattaforme. out-of-box Puoi anche personalizzare le regole di notifica, configurare le superfici di chat e sfruttare l'intelligenza artificiale e l'automazione all'interno della piattaforma per accelerare la risoluzione degli incidenti. PagerDuty

- Gestisci gli utenti
- Crea squadre
- Imposta i metodi di contatto
- Configura le regole di notifica

- Imposta una rotazione in caso di chiamata
- Crea politiche di escalation
- Configura l'integrazione con Slack
- Imposta le azioni di automazione

Per ulteriore assistenza, puoi contattare il tuo Technical Account Manager o AWS-IM-help@pagerduty.com per ulteriori informazioni.

Esportazione dei dati di Incident Manager

Questo argomento descrive come utilizzare uno script Python per esportare i record degli incidenti e le analisi post-incidenti da. Strumento di gestione degli incidenti AWS Systems Manager Lo script esporta i dati in file JSON strutturati per ulteriori analisi o scopi di archiviazione.

Cosa puoi esportare

Lo script esporta i seguenti dati:

- Registrazioni complete degli incidenti, tra cui:
  - Eventi cronologici
  - Voci correlate
  - Impegni
  - Esecuzioni di automazione
  - Risultati relativi alla sicurezza
  - Tag
- Documenti di analisi post-incidente forniti da Systems Manager

Prerequisiti

Prima di iniziare, assicuratevi di avere:

- Python 3.7 o successivo installato
- AWS CLI configurato con le credenziali appropriate
- Sono installati i seguenti pacchetti Python:

```
pip install boto3 python-dateutil
```

Autorizzazioni IAM richieste

Per utilizzare questo script, assicurati di disporre delle seguenti autorizzazioni:

Autorizzazioni Systems Manager Incidents

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:ListEngagements",
                "ssm-incidents:GetEngagement",
                "ssm-incidents:BatchGetIncidentFindings",
                "ssm-incidents:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorizzazioni Systems Manager

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocuments",
                "ssm:GetDocument",
                "ssm:GetAutomationExecution"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Struttura di esportazione

Lo script crea la seguente struttura di directory per i dati esportati:

```
incident_manager_export_YYYYMMDD_HHMMSS/
### incident_records/
#   ### 20250309_102129_IAD_Service_A_Lambda_High_Latency.json
#   ### 20250314_114820_SecurityFinding_SecurityHubFindings.json
#   ### ...
### post_incident_analyses/
    ### 20250310_143022_Root_Cause_Analysis_Service_A.json
    ### 20250315_091545_Security_Incident_Review.json
    ### ...
```

Esecuzione dello script di esportazione

Utilizzo di base

Viene fornito lo script di esportazione dei dati di Incident Manager`here`. Scarica lo script e utilizza le seguenti istruzioni per eseguirlo.

Per eseguire lo script con le impostazioni predefinite:

```
python3 export-incident-manager-data.py
```

Opzioni disponibili

È possibile personalizzare l'esportazione utilizzando queste opzioni della riga di comando:

Opzione	Description	Default
`--region`	AWS Regione	`us-east-1`

Opzione	Description	Default
`--profile`	AWS nome del profilo	profilo predefinito
`--verbose` , `-v`	Abilita la registrazione dettagliata	FALSE
`--limit`	Numero massimo di incidenti da esportare	Nessun limite
`--timeline-events-limit`	Cronologia massima degli eventi per incidente	100
`--timeline-details-limit`	Cronologia massima dei dettagli degli eventi per incidente	100
`--related-items-limit`	Numero massimo di articoli correlati per incidente	50
`--engagements-limit`	Numero massimo di impegni per incidente	20
`--analysis-docs-limit`	Numero massimo di documenti di analisi da esportare	50

Esempi

Esporta da una regione specifica utilizzando un profilo personalizzato:

```
python3 export-incident-manager-data.py --region us-east-1 --profile my-aws-profile
```

Esportazione con registrazione dettagliata e limiti per i test:

```
python3 export-incident-manager-data.py --verbose --limit 5 --timeline-events-limit 10
```

Esportazione con limiti conservativi per set di dati di grandi dimensioni:

```
python3 export-incident-manager-data.py --timeline-events-limit 50 --timeline-details-
limit 25
```

Struttura del file di output

Struttura JSON del record degli incidenti

Ogni file di registrazione degli incidenti contiene la seguente struttura:

```
{
    "incident_record": {
        // Complete incident record from get-incident-record
    },
    "incident_summary": {
        // Incident summary from list-incident-records
    },
    "incident_source_details": {
        "from_incident_record": {},
        "from_incident_summary": {},
        "enhanced_details": {
            "created_by": "arn:aws:sts::...",
            "source": "aws.ssm-incidents.custom",
            "source_analysis": {
                "source_type": "manual",
                "creation_method": "human_via_console",
                "automation_involved": false,
                "human_created": true
            }
        }
    },
    "timeline_events": {
        "detailed_events": [
            {
                "summary": {}, // From list-timeline-events
                "details": {}  // From get-timeline-event
            }
        ],
        "summary_only_events": [],
        "metadata": {
            "total_events_found": 45,
            "events_with_details": 25,
            "limits_applied": {}
        }
```

```
    },
    "related_items": {
        "items": [],
        "metadata": {}
    },
    "engagements": {
        "engagements": [],
        "metadata": {}
    },
    "automation_executions": [],
    "findings": [],
    "tags": [],
    "post_incident_analysis": {
        "analysis_reference": {},
        "metadata": {}
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
        "incident_arn": "arn:aws:ssm-incidents::..."
    }
}
```

Struttura JSON di analisi post-incidente

Ogni file di documento di analisi contiene:

```
{
    "document_metadata": {
        // Document metadata from list-documents
    },
    "document_details": {
        "Name": "037fc5dd-cd86-49bb-9c3d-15720e78798e",
        "Content": "...", // Full JSON content
        "DocumentType": "ProblemAnalysis",
        "CreatedDate": 1234567890,
        "ReviewStatus": "APPROVED",
        "AttachmentsContent": [],
        // ... other fields from get-document
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
```

```
        "document_name": "..."
    }
}
```

Pulizia delle risorse di Incident Manager

Se non le utilizzi più Strumento di gestione degli incidenti AWS Systems Manager, ti consigliamo di ripulire le risorse rimanenti di Incident Manager. In questo modo sarai completamente esonerato dal servizio ed eviterai eventuali addebiti in corso. Per maggiori dettagli, consulta la pagina AWS Systems Manager dei prezzi.

Eliminazione del set di replica

Il Replication Set è un componente chiave di Incident Manager che facilita la replica dei dati relativi agli incidenti in più regioni. AWS Se non è più necessario Incident Manager, è necessario eliminare il Replication Set.

Per eliminare il set di repliche:

1. Aprire la console AWS Systems Manager
2. Nel riquadro di navigazione, scegli Incident Manager
3. In «Replication Sets», individua il Replication Set che desideri eliminare
4. Fate clic sul nome del Replication Set per aprire la pagina dei dettagli
5. Nella pagina dei dettagli del Replication Set, fate clic sul pulsante «Elimina»
6. Nella finestra di dialogo di conferma, esaminate le informazioni e fate clic su «Elimina set di replica» per procedere con l'eliminazione

> **Note**
>
> L'eliminazione del Replication Set rimuoverà definitivamente tutti i dati sugli incidenti memorizzati in Incident Manager. Assicuratevi di non aver più bisogno dell'accesso alle informazioni storiche sugli incidenti prima di procedere con l'eliminazione.

Eliminazione delle risorse relative a Incident Manager

Oltre al Replication Set, potrebbero essere disponibili altre risorse relative a Incident Manager, come piani di risposta, contatti e runbook. Se non hai più bisogno di queste risorse, puoi prendere in considerazione la possibilità di eliminarle completamente da Incident Manager.

Per eliminare le risorse relative a Incident Manager:

1. Apri la console AWS Systems Manager
2. Nel riquadro di navigazione, scegli Incident Manager
3. Vai alla sezione appropriata (ad esempio, «Piani di risposta», «Contatti», «Runbooks») e individua le risorse che desideri eliminare
4. Seleziona le risorse e fai clic sul pulsante «Elimina» per rimuoverle

Configurazione di AWS Systems Manager Incident Manager

Ti consigliamo di configurare AWS Systems Manager Incident Manager nell'account che utilizzi per gestire le tue operazioni. Prima di utilizzare Incident Manager per la prima volta, completa le seguenti attività:

Argomenti

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire le attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi Console di gestione AWScome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Concessione dell'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS Console di gestione AWS esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Consigliato) Utilizza le credenziali della console come credenziali temporanee per firmare le richieste programmatiche a,, o. AWS CLI AWS SDKs AWS APIs	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Login for AWS local development nella Guida per l'AWS Command Line Interface utente. • Per AWS SDKs, consulta Login for AWS local development nella AWS SDKs and Tools Reference Guide.
Identità della forza lavoro	Utilizza credenziali temporanee per firmare le richieste	Segui le istruzioni per l'interfaccia che desideri utilizzare.

Quale utente necessita dell'accesso programmatico?	Per	Come
(Utenti gestiti nel centro identità IAM)	programmatiche a AWS CLI, AWS SDKs, o. AWS APIs	• Per la AWS CLI, vedere Configurazione dell'uso AWS IAM Identity Center nella AWS CLI Guida per l'utente.AWS Command Line Interface • Per AWS SDKs gli strumenti e AWS APIs, consulta l'autenticazione di IAM Identity Center nella Guida di riferimento AWS SDKs and Tools.
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche a AWS CLI, AWS SDKs, o. AWS APIs	Seguendo le istruzioni riportate in Utilizzo delle credenziali temporanee con le AWS risorse nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche a AWS CLI,, AWS SDKs o. AWS APIs	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli strumenti AWS SDKs e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli strumenti e agli AWS SDKs strumenti. • Per AWS APIs, consulta la sezione Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Ruolo richiesto per la configurazione di Incident Manager

Prima di iniziare, il tuo account deve disporre dell'autorizzazione IAM`iam:CreateServiceLinkedRole`. Incident Manager utilizza questa autorizzazione per `AWSServiceRoleforIncidentManager` crearla nel tuo account. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Incident Manager.

Guida introduttiva a Incident Manager

Questa sezione illustra come prepararsi nella console Incident Manager. È necessario completare la procedura Get prepare in the console prima di poterla utilizzare per la gestione degli incidenti. La procedura guidata illustra la configurazione del set di replica, almeno un piano di contatto e un piano di escalation e il primo piano di risposta. Le seguenti guide ti aiuteranno a comprendere Incident Manager e il ciclo di vita degli incidenti:

- Che cos'è Strumento di gestione degli incidenti AWS Systems Manager?
- Ciclo di vita degli incidenti in Incident Manager

Prerequisiti

Se utilizzi Incident Manager per la prima volta, consulta il. Configurazione di AWS Systems Manager Incident Manager Ti consigliamo di configurare Incident Manager nell'account che utilizzi per gestire le tue operazioni.

Si consiglia di completare la configurazione rapida di Systems Manager prima di iniziare la procedura guidata di preparazione di Incident Manager. Utilizzate Systems Manager Quick Setup per configurare AWS i servizi e le funzionalità utilizzati di frequente con le best practice consigliate. Incident Manager utilizza le funzionalità di Systems Manager per gestire gli incidenti associati all'utente Account AWS e trae vantaggio dalla configurazione preliminare di Systems Manager.

Preparati alla procedura guidata

La prima volta che usi Incident Manager, puoi accedere alla procedura guidata Get prepared dalla home page del servizio Incident Manager. Per accedere alla procedura guidata Get ready dopo aver completato la prima configurazione, scegli Prepara nella pagina dell'elenco degli Incidenti.

1. Apri la console Incident Manager.
2. Nella home page del servizio Incident Manager, scegli Preparati.

Impostazioni generali

1. In Impostazioni generali, scegli Configura.

2. Leggi i termini e le condizioni. Se accetti i termini e le condizioni di Incident Manager, seleziona Ho letto e accetto i termini e le condizioni di Incident Manager, quindi scegli Avanti.
3. Nell'area Regioni, la regione corrente Regione AWS appare come la prima regione del set di repliche. Per aggiungere altre regioni al set di replica, selezionale dall'elenco delle regioni.

   Si consiglia di includere almeno due regioni. Nel caso in cui una regione non sia temporaneamente disponibile, le attività relative agli incidenti possono comunque essere indirizzate all'altra regione.

   > **Note**
   >
   > La creazione del set di replica crea il ruolo collegato al `AWSServiceRoleforIncidentManager` servizio nell'account. Per ulteriori informazioni su questo ruolo, consulta. Utilizzo di ruoli collegati ai servizi per Incident Manager

4. Per configurare la crittografia per il set di replica, effettuate una delle seguenti operazioni:

   > **Note**
   >
   > Tutte le risorse di Incident Manager sono crittografate. Per ulteriori informazioni su come vengono crittografati i dati, consultaProtezione dei dati in Incident Manager. Per ulteriori informazioni sul set di repliche di Incident Manager, vedereConfigurazione del set di repliche di Incident Manager.

   - Per utilizzare una chiave AWS proprietaria, scegli Usa chiave AWS proprietaria.
   - Per usare la tua AWS KMS chiave, scegli Scegli una chiave esistente AWS KMS key. Per ogni regione selezionata nel passaggio 3, scegli una AWS KMS chiave o inserisci un AWS KMS Amazon Resource Name (ARN).

     > **Tip**
     >
     > Se non ne hai uno disponibile AWS KMS key, scegli Crea un AWS KMS key.

5. (Facoltativo) Nell'area Tag, aggiungete uno o più tag al set di replica. Un tag include una chiave e, facoltativamente, un valore.

I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Per ulteriori informazioni, consulta Etichettatura delle risorse in Incident Manager.

6. (Facoltativo) Nell'area di accesso al servizio, per attivare la funzione Findings, seleziona la casella di controllo Crea ruolo di servizio per i risultati in questo account.

   Un risultato è un'informazione sulla distribuzione del codice o sulla modifica dell'infrastruttura avvenuta più o meno nello stesso periodo in cui è stato creato un incidente. Un risultato può essere esaminato come causa potenziale dell'incidente. Le informazioni su queste potenziali cause vengono aggiunte alla pagina dei dettagli dell'incidente relativa all'incidente. Con le informazioni su queste implementazioni e modifiche a portata di mano, i soccorritori non devono cercare manualmente queste informazioni.

   > **Tip**
   >
   > Per visualizzare le informazioni sul ruolo da creare, scegli Visualizza i dettagli delle autorizzazioni.

7. Scegli Create (Crea).

   Per ulteriori informazioni sui set di replica e sulla resilienza, consulta. Resilienza in Strumento di gestione degli incidenti AWS Systems Manager

Contatti (facoltativo durante la fase Get prepare)

Incident Manager coinvolge i contatti durante un incidente. Per ulteriori informazioni sui contatti, vedereCreazione e configurazione dei contatti in Incident Manager.

1. Scegli Crea contatto.
2. Per Nome, inserisci il nome del contatto.
3. Per Alias univoco, inserisci un alias per identificare questo contatto.
4. Nella sezione Canale di contatto, procedi come segue per definire il modo in cui il contatto viene coinvolto durante gli incidenti:

   a. Per Tipo, scegli Email, SMS o Voce.
   b. Per Nome del canale, inserisci un nome univoco per aiutarti a identificare il canale.
   c. Per Dettagli, inserisci l'indirizzo email o il numero di telefono del contatto.

I numeri di telefono devono contenere da 9 a 15 caratteri e iniziare con + il prefisso internazionale e il numero dell'abbonato.

d. Per creare un altro canale di contatto, scegli Aggiungi canale di contatto. Ti consigliamo di definire almeno due canali per ogni contatto.

5. Nell'area Piano di coinvolgimento, procedi come segue per definire tramite quali canali notificare il contatto e per quanto tempo attendere la conferma su ciascun canale.

> **Note**
>
> Ti consigliamo di definire almeno due canali nel piano di coinvolgimento.

a. Per il nome del canale di contatto, scegli un canale specificato nell'area Canale di contatto.

b. Per Tempo di coinvolgimento (min), inserisci il numero di minuti di attesa prima di entrare in contatto con il canale di contatto.

   Ti consigliamo di selezionare almeno un dispositivo per interagire all'inizio di un coinvolgimento, specificando **0** (zero) minuti di attesa.

c. Per aggiungere altri canali di contatto al piano di coinvolgimento, scegli Aggiungi coinvolgimento.

6. (Facoltativo) Nell'area Tag, aggiungi uno o più tag al contatto. Un tag include una chiave e, facoltativamente, un valore.

   I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Per ulteriori informazioni, consulta Etichettatura delle risorse in Incident Manager.

7. Per creare il record del contatto e inviare i codici di attivazione ai canali di contatto definiti, scegli Crea.

8. (Facoltativo) Nella pagina di attivazione del canale di contatto, inserisci il codice di attivazione inviato a ciascun canale.

   Puoi generare nuovi codici di attivazione in un secondo momento se non riesci a inserirli ora.

9. Per aggiungere altri contatti, scegli Crea contatto e ripeti i passaggi precedenti.

(Facoltativo durante Get prepared) Piani di escalation

1. Scegli Crea un piano di escalation.

   Un piano di escalation passa attraverso i tuoi contatti durante un incidente, garantendo che Incident Manager coinvolga i soccorritori corretti durante un incidente. Per ulteriori informazioni sui piani di escalation, vedere. Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager
2. In Nome, inserisci un nome univoco per il piano di escalation.
3. Per Alias, inserisci un alias univoco per aiutarti a identificare il piano di escalation.
4. Nell'area Fase 1, effettuate le seguenti operazioni:

   a. Per i canali Escalation, scegliete i canali di contatto con cui interagire.
   b. Se desideri che un contatto sia in grado di interrompere la progressione delle fasi del piano di escalation, seleziona Accogngment interrompe la progressione del piano.
   c. Per aggiungere altri canali a una fase, scegli Aggiungi canale di escalation.
5. Per creare una nuova fase nel piano di escalation, scegli Aggiungi fase e aggiungi i dettagli della fase.
6. (Facoltativo) Nell'area Tag, aggiungi uno o più tag al piano di escalation. Un tag include una chiave e, facoltativamente, un valore.

   I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Per ulteriori informazioni, consulta Etichettatura delle risorse in Incident Manager.
7. Scegli Crea un piano di escalation.

Piano di risposta

> **Note**
>
> Potrebbe essere necessario tornare alla pagina iniziale di Incident Manager e scegliere Prepara per continuare.

1. Scegli Crea piano di risposta.

   Usa il piano di risposta per mettere insieme i contatti e i piani di escalation che hai creato.

Durante questa procedura guidata introduttiva, le seguenti sezioni sono facoltative, soprattutto se è la prima volta che configuri un piano di risposta:

- Canale di chat
- Runbook
- Impegni
- Integrazioni di terze parti

Per informazioni sull'aggiunta di questi elementi ai piani di risposta in un secondo momento, consultaPreparazione agli incidenti in Incident Manager.

2. In Nome, inserisci un nome univoco e identificabile per il piano di risposta. Il nome viene utilizzato per creare l'ARN del piano di risposta o nei piani di risposta senza nome visualizzato.
3. (Facoltativo) In Nome visualizzato, inserisci un nome per aiutarti a identificare questo piano di risposta durante la creazione di incidenti.
4. Per Titolo, inserisci un titolo che aiuti a identificare il tipo di incidente correlato a questo piano di risposta.

   Il valore specificato è incluso nel titolo di ogni incidente. Al titolo viene aggiunto anche l'allarme o l'evento che ha dato inizio all'incidente.
5. In Impatto, seleziona il livello di impatto previsto per gli incidenti relativi a questo piano di risposta, ad esempio **`Critical`** o**`Low`**.
6. (Facoltativo) In Riepilogo, inserisci una breve descrizione che viene utilizzata per fornire una panoramica dell'incidente. Incident Manager inserisce automaticamente le informazioni pertinenti nel riepilogo durante un incidente.
7. (Facoltativo) Per la stringa di deduplicazione, immettere una stringa di deduplicazione. Incident Manager utilizza questa stringa per impedire che la stessa causa principale crei più incidenti nello stesso account.

   Una stringa di deduplicazione è un termine o una frase che il sistema utilizza per verificare la presenza di incidenti duplicati. Se si specifica una stringa di deduplicazione, Incident Manager cerca gli incidenti aperti che contengono la stessa stringa nel campo al momento della creazione dell'incidente. `dedupeString` Se viene rilevato un duplicato, Incident Manager deduplica l'incidente più recente nell'incidente esistente.

> **Note**
>
> Per impostazione predefinita, Incident Manager deduplica automaticamente più incidenti creati dallo stesso allarme Amazon CloudWatch o evento Amazon. EventBridge Non è necessario inserire la propria stringa di deduplicazione per impedire la duplicazione di questi tipi di risorse.

8. (Facoltativo) Nell'area Tag degli incidenti, aggiungi uno o più tag al piano di risposta. Un tag include una chiave e, facoltativamente, un valore.

   I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Per ulteriori informazioni, consulta Etichettatura delle risorse in Incident Manager.
9. Seleziona i contatti e i piani di escalation da applicare all'incidente dal menu a discesa Impegni.
10. Scegli Crea piano di risposta.

Dopo aver creato un piano di risposta, puoi associare Amazon CloudWatch alarms o Amazon EventBridge Events al piano di risposta. Questo creerà automaticamente un incidente basato su un allarme o un evento. Per ulteriori informazioni, consulta Creazione automatica o manuale di incidenti in Incident Manager.

Gestione degli incidenti in tutte Account AWS le regioni in Incident Manager

È possibile configurare Incident Manager, uno strumento di AWS Systems Manager, per lavorare con più Regioni AWS account e. Questa sezione descrive le best practice interregionali e interaccount, i passaggi di configurazione e le limitazioni note.

Argomenti

Gestione degli incidenti tra regioni

Incident Manager supporta la creazione automatica e manuale di incidenti in diversi Regioni AWS modi. Quando si esegue inizialmente l'onboarding con Incident Manager utilizzando la procedura guidata Get prepared, è possibile specificarne fino a tre Regioni AWS per il set di replica. Per gli incidenti creati automaticamente da Amazon CloudWatch alarms o Amazon EventBridge events, Incident Manager tenta di creare un incidente uguale alla Regione AWS regola dell'evento o all'allarme. Se Incident Manager presenta un'interruzione in quella regione, crea CloudWatch o crea EventBridge automaticamente l'incidente in un'altra regione in cui vengono replicati i dati.

> **Important**
>
> Tieni presenti queste importanti informazioni.
>
> - Si consiglia di specificarne almeno due Regioni AWS nel set di replica. Se non si specificano almeno due regioni, il sistema non riuscirà a creare incidenti durante il periodo in cui Incident Manager non è disponibile.
> - Gli incidenti creati da un failover tra regioni non richiamano i runbook specificati nei piani di risposta.

Per ulteriori informazioni sull'onboarding con Incident Manager e sulla specifica di regioni aggiuntive, consulta. Guida introduttiva a Incident Manager

Gestione degli incidenti su più account

Incident Manager utilizza AWS Resource Access Manager (AWS RAM) per condividere le risorse di Incident Manager tra account di gestione e applicazioni. Questa sezione descrive le migliori pratiche tra account, come configurare la funzionalità tra account per Incident Manager e le limitazioni note della funzionalità tra account in Incident Manager.

Un account di gestione è l'account da cui si esegue la gestione delle operazioni. In una configurazione organizzativa, l'account di gestione possiede i piani di risposta, i contatti, i piani di escalation, i runbook e altre risorse. AWS Systems Manager

Un account di applicazione è l'account che possiede le risorse che compongono le applicazioni. Queste risorse possono essere EC2 istanze Amazon, tabelle Amazon DynamoDB o qualsiasi altra risorsa utilizzata per creare applicazioni in. Cloud AWS Gli account delle applicazioni possiedono anche gli CloudWatch allarmi Amazon e EventBridge gli eventi Amazon che creano incidenti in Incident Manager.

AWS RAM utilizza le condivisioni di risorse per condividere risorse tra account. È possibile condividere il piano di risposta e contattare le risorse tra account in AWS RAM. Condividendo queste risorse, gli account delle applicazioni e gli account di gestione possono interagire con interventi e incidenti. La condivisione di un piano di risposta consente di condividere tutti gli incidenti passati e futuri creati utilizzando tale piano di risposta. La condivisione di un contatto consente di condividere tutti gli impegni passati e futuri del contatto o del piano di risposta.

Best practice

Segui queste best practice quando condividi le tue risorse di Incident Manager tra più account:

- Aggiorna regolarmente la condivisione delle risorse con i piani di risposta e i contatti.
- Rivedi regolarmente i principi di condivisione delle risorse.
- Configura Incident Manager, runbook e canali di chat nel tuo account di gestione.

Imposta e configura la gestione degli incidenti tra account

I passaggi seguenti descrivono come impostare e configurare le risorse di Incident Manager e utilizzarle per la funzionalità tra account. In passato potresti aver configurato alcuni servizi e risorse per la funzionalità tra account. Utilizza questi passaggi come elenco di controllo dei requisiti prima di iniziare il primo incidente utilizzando risorse su più account.

1. (Facoltativo) Crea organizzazioni e unità organizzative utilizzando. AWS Organizations Segui i passaggi del Tutorial: Creazione e configurazione di un'organizzazione nella Guida per l'AWS Organizations utente.
2. (Facoltativo) Utilizzate Quick Setup, uno degli strumenti di cui disponete AWS Systems Manager, per impostare i AWS Identity and Access Management ruoli corretti da utilizzare durante la configurazione dei runbook tra più account. Per ulteriori informazioni, consulta Quick Setup nella Guida per l'utente di AWS Systems Manager .
3. Segui i passaggi elencati in Esecuzione di automazioni in più Regioni AWS account nella Guida per l'AWS Systems Manager utente per creare runbook nei documenti di automazione di Systems Manager. Un runbook può essere eseguito da un account di gestione o da uno degli account dell'applicazione. A seconda del caso d'uso, sarà necessario installare il AWS CloudFormation modello appropriato per i ruoli necessari per creare e visualizzare i runbook durante un incidente.
   - Esecuzione di un runbook nell'account di gestione. L'account di gestione deve scaricare e installare il AWS-SystemsManager-AutomationReadOnlyRole CloudFormation modello. Durante l'installazione AWS-SystemsManager-AutomationReadOnlyRole, specifica l'account IDs di tutti gli account dell'applicazione. Questo ruolo consentirà agli account dell'applicazione di leggere lo stato del runbook dalla pagina dei dettagli dell'incidente. L'account dell'applicazione deve installare il AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation modello. La pagina dei dettagli dell'incidente utilizza questo ruolo per ottenere lo stato di automazione dall'account di gestione.
   - Esecuzione di un runbook in un account dell'applicazione. L'account di gestione deve scaricare e installare il AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation modello. Questo ruolo consente all'account di gestione di leggere lo stato del runbook nell'account dell'applicazione. L'account dell'applicazione deve scaricare e installare il AWS-SystemsManager-AutomationReadOnlyRole CloudFormation modello. Durante l'installazione`AWS-SystemsManager-AutomationReadOnlyRole`, specificare l'ID dell'account di gestione e degli altri account dell'applicazione. L'account di gestione e gli altri account delle applicazioni assumono questo ruolo per leggere lo stato del runbook.
4. (Facoltativo) In ogni account dell'applicazione dell'organizzazione, scaricate e installate il AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation modello. Durante l'installazione AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole, specifica l'ID dell'account di gestione. Questo ruolo fornisce le autorizzazioni necessarie a Incident Manager per accedere alle informazioni sulle AWS CodeDeploy distribuzioni e CloudFormation sugli

aggiornamenti dello stack. Queste informazioni vengono riportate come risultati di un incidente se la funzionalità Findings è abilitata. Per ulteriori informazioni, consulta Identificazione delle potenziali cause di incidenti derivanti da altri servizi come «risultati» in Incident Manager.

5. Per configurare e creare contatti, piani di escalation, canali di chat e piani di risposta, segui i passaggi descritti in. Preparazione agli incidenti in Incident Manager
6. Aggiungi i contatti e le risorse del piano di risposta alla condivisione di risorse esistente o a una nuova condivisione di risorse in. AWS RAM Per ulteriori informazioni, consulta Nozioni di base su AWS RAM nella Guida per l'utente di AWS RAM . L'aggiunta di piani di risposta AWS RAM consente agli account delle applicazioni di accedere agli incidenti e ai dashboard degli incidenti creati utilizzando i piani di risposta. Gli account delle applicazioni acquisiscono inoltre la capacità di associare CloudWatch allarmi ed EventBridge eventi a un piano di risposta. L'aggiunta dei contatti e dei piani di escalation AWS RAM consente agli account delle applicazioni di visualizzare le interazioni e coinvolgere i contatti dalla dashboard degli incidenti.
7. Aggiungi funzionalità multiaccount e interregionali alla tua console. CloudWatch Per i passaggi e le informazioni, consulta la CloudWatch console interregionale per più account nella Amazon CloudWatch User Guide. L'aggiunta di questa funzionalità garantisce che gli account dell'applicazione e l'account di gestione che hai creato possano visualizzare e modificare le metriche dai dashboard degli incidenti e delle analisi.
8. Crea un bus di EventBridge eventi Amazon per più account. Per passaggi e informazioni, consulta Invio e ricezione di EventBridge eventi Amazon tra AWS account. Puoi quindi utilizzare questo bus di eventi per creare regole di evento che rilevano gli incidenti negli account delle applicazioni e li creano nell'account di gestione.

Limitazioni

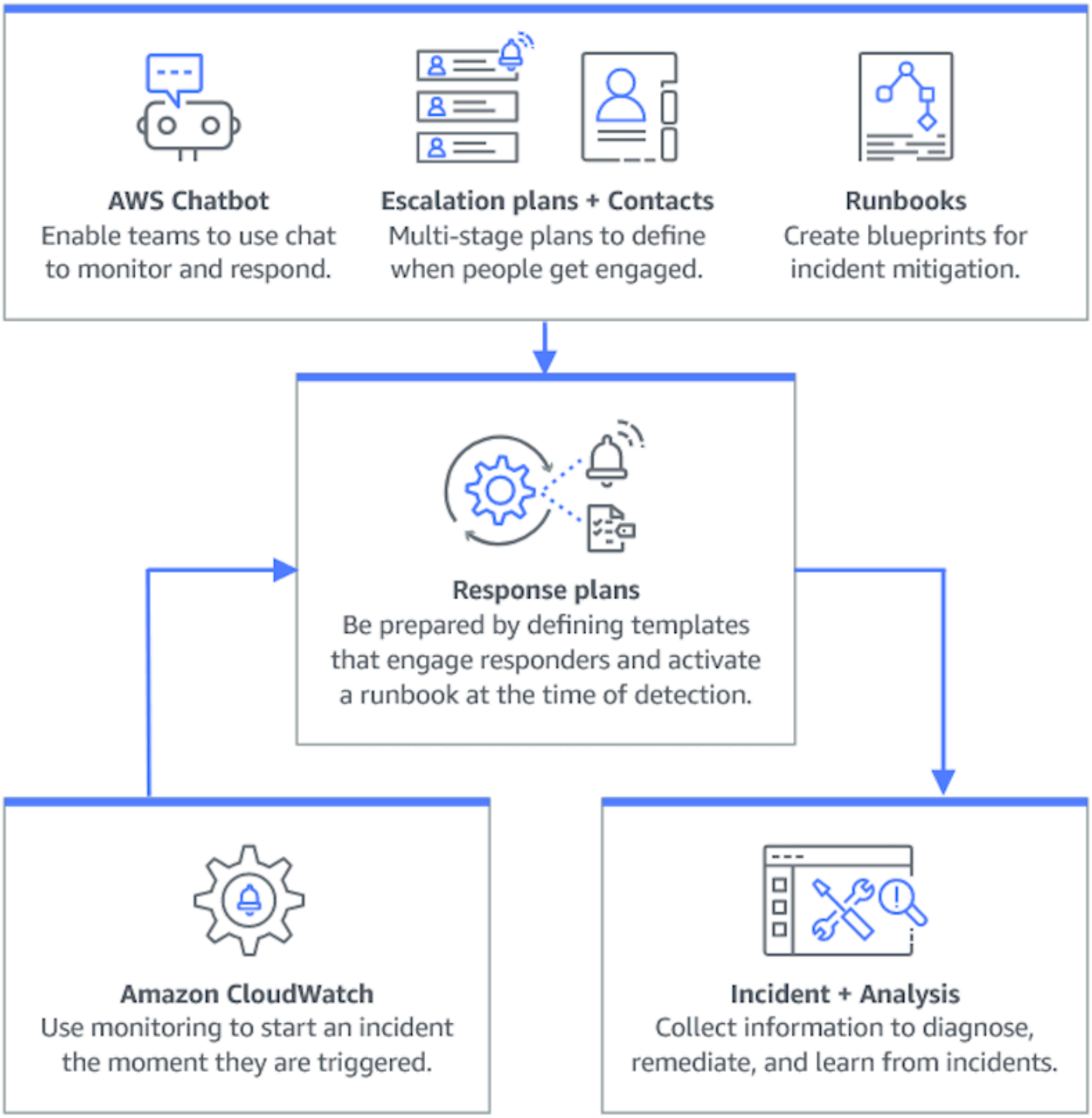
Di seguito sono riportate le limitazioni note della funzionalità cross-account di Incident Manager:

- L'account che crea un'analisi post-incidente è l'unico account che può visualizzarla e modificarla. Se si utilizza un account di applicazione per creare un'analisi post-incidente, solo i membri di tale account possono visualizzarla e modificarla. Lo stesso vale se si utilizza un account di gestione per creare un'analisi post-incidente.
- Gli eventi della sequenza temporale non vengono compilati per i documenti di automazione eseguiti negli account delle applicazioni. Gli aggiornamenti dei documenti di automazione eseguiti negli account delle applicazioni sono visibili nella scheda Runbook dell'incidente.

- Gli argomenti di Amazon Simple Notification Service non possono essere utilizzati su più account. Gli argomenti di Amazon SNS devono essere creati nella stessa regione e nello stesso account del piano di risposta in cui vengono utilizzati. Ti consigliamo di utilizzare l'account di gestione per creare tutti gli argomenti e i piani di risposta SNS.
- I piani di escalation possono essere creati solo utilizzando i contatti dello stesso account. Un contatto che è stato condiviso con te non può essere aggiunto a un piano di escalation del tuo account.
- I tag applicati ai piani di risposta, ai record degli incidenti e ai contatti possono essere visualizzati e modificati solo dall'account del proprietario della risorsa.

Preparazione agli incidenti in Incident Manager

La pianificazione di un incidente inizia molto prima del ciclo di vita dell'incidente. Come illustrato nella figura seguente, prima di iniziare a rispondere agli incidenti, è necessario prepararsi impostando i canali di chat, creando piani di escalation, specificando i contatti e determinando i runbook di automazione da utilizzare nella risposta agli incidenti. Quindi, utilizzate un piano di risposta che specifichi come avviene il monitoraggio e se le risposte sono automatizzate. Una volta completata la riparazione, è possibile analizzare l'incidente e la risposta all'incidente per affinare ulteriormente il piano di risposta per gli incidenti futuri.



Argomenti

- Monitoraggio
- Configurazione dei set di replica e dei risultati in Incident Manager
- Creazione e configurazione dei contatti in Incident Manager

- Gestione delle rotazioni dei soccorritori con pianificazioni di chiamata in Incident Manager
- Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager
- Creazione e integrazione di canali di chat per i soccorritori in Incident Manager
- Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti
- Creazione e configurazione dei piani di risposta in Incident Manager
- Identificazione delle potenziali cause di incidenti derivanti da altri servizi come «risultati» in Incident Manager

Monitoraggio

Il monitoraggio dello stato delle applicazioni AWS ospitate è fondamentale per garantire l'operatività e le prestazioni delle applicazioni. Nel determinare le soluzioni di monitoraggio, tenete presente quanto segue:

- Criticità della funzionalità: in caso di guasto del sistema, quanto sarebbe importante l'impatto sugli utenti a valle.
- Punti comuni di errore: con quale frequenza si verifica un guasto del sistema; i sistemi che richiedono un intervento frequente devono essere monitorati attentamente.
- Aumento della latenza: quanto è aumentato o diminuito il tempo necessario per completare un'attività.
- Metriche lato client e lato server: se esiste una discrepanza tra le metriche correlate sul client e sul server.
- Fallimenti legati alle dipendenze: errori a cui il team può e deve prepararsi.

Dopo aver creato i piani di risposta, puoi utilizzare le tue soluzioni di monitoraggio per tracciare automaticamente gli incidenti nel momento in cui si verificano nel tuo ambiente. Per ulteriori informazioni sul tracciamento e la creazione degli incidenti, vedereVisualizzazione dei dettagli dell'incidente nella console Incident Manager.

Per ulteriori informazioni sull'architettura di applicazioni e carichi di lavoro infrastrutturali sicuri, ad alte prestazioni, resilienti ed efficienti, consulta Well-Architected.AWS

Configurazione dei set di replica e dei risultati in Incident Manager

Dopo aver completato la procedura guidata Get prepare di Incident Manager, è possibile gestire determinate opzioni nella pagina Impostazioni. Queste opzioni includono il set di replica, i tag applicati al set di replica e la funzione Findings.

Argomenti

Configurazione del set di repliche di Incident Manager

Il set di repliche di Incident Manager replica i dati su molti utenti Regioni AWS per eseguire le seguenti operazioni:

- Aumentare la ridondanza tra le regioni
- Consenti a Incident Manager di accedere alle risorse in diverse regioni e riduci la latenza per i tuoi utenti.
- Crittografa i tuoi dati con una chiave Chiave gestita da AWS o con la tua chiave gestita dal cliente.

  Tutte le risorse di Incident Manager sono crittografate per impostazione predefinita. Per ulteriori informazioni su come vengono crittografate le risorse, consultaProtezione dei dati in Incident Manager.

Per iniziare a usare Incident Manager, crea innanzitutto il set di replica utilizzando la procedura guidata Get prepared. Per ulteriori informazioni su come prepararsi in Incident Manager, consulta il. Preparati alla procedura guidata

Modifica del set di replica

Utilizzando la pagina delle impostazioni di Incident Manager, è possibile modificare il set di replica. È possibile aggiungere regioni, eliminare regioni e abilitare o disabilitare la protezione dall'eliminazione dei set di replica. Non è possibile modificare la chiave utilizzata per crittografare i dati. Per modificare la chiave, elimina e ricrea il set di replica.

Aggiungere una regione

1. Apri la console Incident Manager, quindi scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Scegli Aggiungi regione.
3. Seleziona la Regione.
4. Scegliere Aggiungi.

Eliminare una regione

1. Apri la console Incident Manager, quindi scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Seleziona la regione che desideri eliminare.
3. Scegli Elimina.
4. Inserisci delete nella casella di testo e scegli Elimina.

Eliminazione del set di replica

L'eliminazione dell'ultima regione del set di replica comporta l'eliminazione dell'intero set di replica. Prima di poter eliminare l'ultima regione, disattivate la protezione da eliminazione disattivando la protezione da eliminazione nella pagina Impostazioni. Dopo aver eliminato il set di replica, è possibile creare un nuovo set di replica utilizzando la procedura guidata Get prepared.

Per eliminare una regione dal set di replica, attendi 24 ore dopo averla creata. Se si tenta di eliminare una regione dal set di replica prima di 24 ore dalla creazione, l'eliminazione non riesce.

L'eliminazione del set di replica comporta l'eliminazione di tutti i dati di Incident Manager.

Eliminare il set di replica

1. Apri la console Incident Manager, quindi scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Seleziona l'ultima regione del set di replica.
3. Scegli Elimina.
4. Immettete delete nella casella di testo e scegliete Elimina.

Gestione dei tag per un set di replica

I tag sono metadati facoltativi assegnati a una risorsa. Utilizza i tag per classificare una risorsa in diversi modi, ad esempio per scopo, proprietario o ambiente.

Per gestire i tag per un set di replica

1. Apri la console Incident Manager, quindi scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nell'area Tag, scegli Modifica.
3. Per aggiungere un tag, procedere come segue:
   a. Scegli Aggiungi nuovo tag.
   b. Immettete una chiave e un valore opzionale per il tag.
   c. Scegli Save (Salva).
4. Per eliminare un tag, procedi come segue:
   a. Sotto il tag che desideri eliminare, scegli Rimuovi.
   b. Scegli Save (Salva).

Gestione della funzione Findings

La funzione Findings aiuta i soccorritori dell'organizzazione a identificare le potenziali cause alla radice degli incidenti subito dopo l'inizio degli incidenti. Attualmente, Incident Manager fornisce risultati per le AWS CodeDeploy implementazioni e gli aggiornamenti dello stack. AWS CloudFormation

Per il supporto dei risultati su più account, dopo aver abilitato la funzionalità, è necessario completare un passaggio di configurazione aggiuntivo in ogni account dell'applicazione dell'organizzazione.

Per utilizzare la funzionalità, consenti a Incident Manager di creare un ruolo di servizio che include le autorizzazioni necessarie per accedere ai dati per tuo conto.

Per abilitare la funzione Findings

1. Apri la console Incident Manager, quindi scegli Impostazioni nel riquadro di navigazione a sinistra.
2. Nell'area Risultati, scegli Crea ruolo di servizio.

3. Esamina le informazioni sul ruolo di servizio da creare, quindi scegli Crea.

Per disabilitare la funzione Findings

Per smettere di usare la funzione Findings, elimina il `IncidentManagerIncidentAccessServiceRole` ruolo da ogni account in cui è stato creato.

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione a sinistra, seleziona Ruoli.
3. Nella casella di ricerca immetti **`IncidentManagerIncidentAccessServiceRole`**.
4. Scegli il nome del ruolo, quindi scegli Elimina.
5. Immettete il nome del ruolo nella finestra di dialogo per confermare che desiderate eliminare il ruolo, quindi scegliete Elimina.

Creazione e configurazione dei contatti in Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager i contatti rispondono agli incidenti. Un contatto può disporre di più canali che Incident Manager può utilizzare durante un incidente. È possibile definire il piano di coinvolgimento di un contatto per descrivere come e quando Incident Manager coinvolge il contatto.

Argomenti

Canali di contatto

I canali di contatto sono i vari metodi utilizzati da Incident Manager per coinvolgere un contatto.

Incident Manager supporta i seguenti canali di contatto:

- E-mail
- Short Message Service (SMS)

- Voce

Attivazione del canale di contatto

Per proteggere la tua privacy e la tua sicurezza, Incident Manager ti invia un codice di attivazione del dispositivo quando crei contatti. Per attivare i dispositivi durante un incidente, è necessario prima attivarli. A tale scopo, inserisci il codice di attivazione del dispositivo nella pagina di creazione dei contatti.

Alcune funzionalità di Incident Manager includono funzionalità che inviano notifiche a un canale di contatto. Utilizzando queste funzionalità, acconsenti all'invio da parte del servizio di notifiche relative a interruzioni del servizio o altri eventi ai canali di contatto inclusi nel flusso di lavoro specificato. Ciò include le notifiche inviate a un contatto come parte di una rotazione del programma di chiamata. Le notifiche possono essere inviate tramite e-mail, SMS o chiamata vocale come specificato nei dettagli di un contatto. Utilizzando queste funzionalità, confermi di essere autorizzato ad aggiungere i canali di contatto che fornisci a Incident Manager.

Impostazioni di opt-out

Puoi annullare queste notifiche in qualsiasi momento rimuovendo un dispositivo mobile come canale di contatto. I singoli destinatari delle notifiche possono inoltre annullare le notifiche in qualsiasi momento rimuovendo il dispositivo dal loro contatto.

Per rimuovere un canale di contatto da un contatto

1. Vai alla console Incident Manager e scegli Contatti dalla barra di navigazione a sinistra.
2. Seleziona il contatto con il canale di contatto che stai rimuovendo e scegli Modifica.
3. Scegli Rimuovi accanto al canale di contatto che desideri rimuovere.
4. Scegli Aggiorna.

Disattivazione del canale di contatto

Per disattivare un dispositivo, rispondi ANNULLA L'ISCRIZIONE. La risposta UNSUBSCRIBE impedisce a Incident Manager di interagire con il tuo dispositivo.

Riattivazione del canale di contatto

1. Rispondi START al messaggio di Incident Manager.

2. Vai alla console Incident Manager e scegli Contatti dalla barra di navigazione a sinistra.
3. Seleziona il contatto con il canale di contatto che stai rimuovendo e scegli Modifica.
4. Scegli Attiva dispositivi.
5. Inserisci il codice di attivazione inviato al dispositivo da Incident Manager.
6. Seleziona Activate (Attiva).

Piani di coinvolgimento

I piani di coinvolgimento definiscono quando Incident Manager interagisce con i canali di contatto. È possibile coinvolgere i canali di contatto più volte in fasi diverse dall'inizio di un coinvolgimento. Puoi utilizzare i piani di coinvolgimento in un piano di escalation o in un piano di risposta. Per ulteriori informazioni sui piani di escalation, consulta. Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager

Creazione di un contatto

Per creare un contatto, usa i seguenti passaggi.

1. Apri la console Incident Manager e scegli Contatti dalla barra di navigazione a sinistra.
2. Scegli Crea contatto.
3. Digita il nome completo del contatto e fornisci un alias univoco e identificabile.
4. Definisci un canale di contatto. Ti consigliamo di avere due o più tipi diversi di canali di contatto.
    a. Scegli il tipo: e-mail, SMS o voce.
    b. Inserisci un nome identificabile per il canale di contatto.
    c. Fornisci i dettagli del canale di contatto, ad esempio e-mail: arosalez@example.com
5. Per definire più di un canale di contatto, scegli Aggiungi canale di contatto. Ripeti il passaggio 4 per ogni nuovo canale di contatto aggiunto.
6. Definisci un piano di coinvolgimento.

> **Important**
>
> Per coinvolgere un contatto, è necessario definire un piano di coinvolgimento.

    a. Scegli il nome del canale di contatto.

b. Definisci quanti minuti dall'inizio del coinvolgimento devi attendere prima che Incident Manager attivi questo canale di contatto.

c. Per aggiungere un altro canale di contatto, scegli Aggiungi coinvolgimento.

7. Dopo aver definito il tuo piano di coinvolgimento, scegli Crea. Incident Manager invia un codice di attivazione a ciascuno dei canali di contatto definiti.
8. (Facoltativo) Per attivare i canali di contatto, inserisci il codice di attivazione che Incident Manager ha inviato a ciascun canale di contatto definito.
9. (Facoltativo) Per inviare un nuovo codice di attivazione, scegli Invia nuovo codice.
10. Scegli Fine.

Dopo aver definito un contatto e attivato i relativi canali di contatto, puoi aggiungere contatti ai piani di escalation per formare una catena di escalation. Per ulteriori informazioni sui piani di escalation, consulta. Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager Puoi aggiungere contatti a un piano di risposta per un coinvolgimento diretto. Per ulteriori informazioni sulla creazione di piani di risposta, consultaCreazione e configurazione dei piani di risposta in Incident Manager.

Importa i dati di contatto nella tua rubrica

Quando viene creato un incidente, Incident Manager può avvisare i soccorritori utilizzando notifiche vocali o SMS. Per garantire che i soccorritori vedano che la chiamata o la notifica SMS proviene da Incident Manager, consigliamo a tutti i soccorritori di scaricare il file in formato scheda virtuale (.vcf) di Incident Manager nella rubrica dei propri dispositivi mobili. Il file è ospitato su Amazon CloudFront ed è disponibile nella partizione AWS commerciale.

Per scaricare il file.vcf di Incident Manager

1. Sul tuo dispositivo mobile, scegli o inserisci il seguente URL: https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .vcf.
2. Salva o importa il file nella rubrica del tuo dispositivo mobile.

Gestione delle rotazioni dei soccorritori con pianificazioni di chiamata in Incident Manager

Una pianificazione delle chiamate in Incident Manager definisce chi riceve una notifica quando si verifica un incidente che richiede l'intervento dell'operatore. Una pianificazione di chiamata consiste in una o più rotazioni create dall'utente per la pianificazione. Ogni rotazione può includere fino a 30 contatti.

Dopo aver creato un programma di chiamata, puoi includerlo come intensificazione nel tuo piano di escalation. Quando si verifica un incidente associato a quel piano di escalation, Incident Manager avvisa l'operatore (o gli operatori) che sono in servizio in base alla pianificazione. Questo contatto può quindi confermare l'impegno. Nel piano di escalation, puoi designare uno o più orari di chiamata, nonché uno o più contatti individuali, in più fasi dell'escalation. Per ulteriori informazioni, consulta Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager.

> **Tip**
>
> Come best practice, consigliamo di aggiungere contatti e orari di chiamata come canali di escalation in un piano di escalation. Dovresti quindi scegliere un piano di escalation come impegno in un piano di risposta. Questo approccio offre la copertura più completa per la risposta agli incidenti nell'organizzazione.

Ogni programma di chiamata supporta fino a otto rotazioni. Le rotazioni possono sovrapporsi o essere eseguite contemporaneamente. Ciò aumenta il numero di operatori incaricati di rispondere quando si verifica un incidente. È inoltre possibile creare rotazioni che vengono eseguite consecutivamente. Ciò supporta scenari come la gestione degli incidenti «follow the sun» in cui esistono gruppi in tutto il mondo che supportano lo stesso servizio.

Utilizza gli argomenti di questa sezione per aiutarti a creare e gestire pianificazioni di chiamata per le operazioni di risposta agli incidenti.

Argomenti

- Creazione di una pianificazione e di una rotazione delle chiamate in Incident Manager
- Gestione di una pianificazione delle chiamate esistente in Incident Manager

Creazione di una pianificazione e di una rotazione delle chiamate in Incident Manager

Crea un programma di chiamata con una o più rotazioni di contatti da coinvolgere per rispondere agli incidenti durante i loro turni.

Prima di iniziare

Prima di creare una pianificazione delle chiamate, assicurati di aver creato in precedenza i contatti che desideri aggiungere alle rotazioni della pianificazione. Per informazioni, consulta Creazione e configurazione dei contatti in Incident Manager.

Contabilità delle modifiche all'ora legale (DST)

Quando si crea una rotazione, si specifica il fuso orario globale che funge da base per gli orari e le date di copertura dei turni specificati per questa rotazione. È possibile utilizzare qualsiasi fuso orario definito dalla Internet Assigned Numbers Authority (IANA). For example: `America/Los_Angeles`, `UTC` e `Asia/Seoul`. È possibile aggiungere più di una rotazione a un programma di chiamata. Tuttavia, quando i soccorritori di ogni rotazione si trovano geograficamente in fusi orari diversi, tieni presente le eventuali modifiche all'ora legale a cui ogni rotazione potrebbe essere soggetta.

Ad esempio, `America/Los_Angeles` e `Europe/Dublin` osserva diversi orari dell'ora legale. Di conseguenza, la differenza di orario tra le due zone può variare da 6 a 8 ore, a seconda del periodo dell'anno. Ad esempio, un follow-the-sun programma di chiamata prevede una rotazione nel fuso `America/Los_Angeles` orario e una rotazione in `Europe/Dublin` entrata. In questo esempio, la pianificazione può contenere un intervallo di turni di un'ora o una sovrapposizione dei turni di un'ora a causa delle modifiche dell'ora legale.

Per evitare queste situazioni, consigliamo il seguente approccio:

1. Utilizza un unico fuso orario per tutte le rotazioni in un programma di chiamata.
2. Calcola l'ora locale quando assegni i soccorritori al di fuori di quel particolare fuso orario.

Se decidi di assegnare ogni rotazione al relativo fuso orario locale, rivedi la pianificazione prima di qualsiasi ora legale. Quindi, modifica gli orari dei turni di rotazione in base alle esigenze per assicurarti di evitare interruzioni o sovrapposizioni involontarie nella copertura di chiamata prima che le modifiche all'ora legale abbiano effetto.

Per creare un programma di chiamata

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.
3. Scegli Crea pianificazione delle chiamate.
4. Per Nome del programma, inserisci un nome per aiutarti a identificare la pianificazione, ad esempio**`MyApp Primary On-call Schedule`**.
5. Per Schedule alias, inserisci un alias per questa pianificazione che sia unico nella versione corrente Regione AWS, ad esempio. **`my-app-primary-on-call-schedule`**
6. (Facoltativo) Nell'area Tag, applicate una o più coppie di tag (nome chiave e valore) alla pianificazione delle chiamate.

   I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, puoi etichettare una pianificazione per identificare il periodo di tempo in cui viene eseguita, i tipi di operatori che contiene o il piano di escalation che supporta. Per ulteriori informazioni sull'etichettatura delle risorse di Incident Manager, vedere. Etichettatura delle risorse in Incident Manager
7. Continua aggiungendo una o più rotazioni alla pianificazione delle chiamate.

Creazione di una rotazione per un programma di chiamata in Incident Manager

Una rotazione in un programma di guardia specifica quando il turno è in vigore. Inoltre specifica i contatti attraverso i quali ruotano i turni. È possibile includere fino a otto rotazioni in un unico programma di chiamata.

È possibile aggiungere a una rotazione qualsiasi persona creata come contatto in Incident Manager. Per informazioni sulla gestione dei contatti, consultaCreazione e configurazione dei contatti in Incident Manager.

Mentre configuri la rotazione, puoi vedere l'aspetto della pianificazione generale in un calendario di anteprima sul lato destro della pagina.

Per creare una rotazione per un programma di chiamata

1. Nella sezione Rotazione 1 della pagina Crea pianificazione delle chiamate, per Nome della rotazione, immettete un nome che identifichi la rotazione, ad **`00:00 - 7:59 Support`** esempio, o. **`Dublin Support Group`**
2. Per Data di inizio, inserisci la data in cui questa rotazione diventa attiva in un `YYYY/MM/DD` formato, ad esempio. `2023/07/14`
3. Per Fuso orario, selezionate il fuso orario globale che funge da base per gli orari e le date di copertura dei turni specificati per questa rotazione.

   È possibile utilizzare qualsiasi fuso orario definito dalla Internet Assigned Numbers Authority (IANA). Ad esempio: "America/Los_Angeles", "UTC", "Asia/Seoul». Per ulteriori informazioni, consulta Time Zone Database nel sito Web IANA.

   > **Warning**
   >
   > È possibile basare ogni rotazione sul proprio fuso orario. Tuttavia, qualsiasi modifica dell'ora legale nei fusi orari selezionati può influire sulle finestre di copertura previste. Per ulteriori informazioni, consulta la sezione Contabilizzazione delle modifiche all'ora legale (DST) più avanti in questo argomento.

4. Per Ora di inizio della rotazione, inserisci l'ora in cui inizia il turno di rotazione nel `hh:mm` formato di 24 ore, ad `16:00` esempio.

   Nota le differenze nell'ora locale per i contatti con fusi orari diversi da quello specificato. Ad esempio, se scegli `America/Los_Angeles` come fuso orario e `00:00` come ora di inizio della rotazione, questo equivale alle 08:00 a Dublino, in Irlanda, e alle 13:30 a Mumbai, in India.
5. Per Ora di fine della rotazione, inserisci l'ora in cui termina il turno di questo turno di rotazione nel formato di 24 orehh`:mm`, ad esempio. `23:59`

   > **Note**
   >
   > L'intervallo di tempo tra l'inizio e la fine di una rotazione deve essere di almeno 30 minuti.

6. (Facoltativo) Per impostare la durata della rotazione su 24 ore, selezionate la copertura di 24 ore e inserite l'ora di inizio di questa rotazione nel campo Ora di inizio della rotazione. Il valore dell'ora di fine della rotazione si aggiorna automaticamente.

Ad esempio, se desideri che il servizio di guardia abbia una copertura di 24 ore con cambio turno alle 11:00, scegli una copertura di 24 ore e inserisci **`11:00`** come ora di inizio.

7. Per Giorni attivi, seleziona i giorni della settimana in cui è attiva questa rotazione. Se il tuo piano di assistenza telefonica esclude la copertura del fine settimana, ad esempio, seleziona tutti i giorni tranne la domenica e il sabato.
8. Continua aggiungendo contatti alla rotazione.

Aggiungere contatti a una rotazione in una pianificazione delle chiamate in Incident Manager

Per ogni rotazione nella pianificazione delle chiamate, puoi aggiungere uno o più contatti, fino a un totale di 30. Puoi scegliere tra i contatti configurati nella configurazione di Incident Manager.

Quando aggiungi un contatto a una rotazione, il contatto potrebbe ricevere notifiche nell'ambito delle sue mansioni di guardia. Le notifiche possono essere inviate tramite e-mail, SMS o chiamata vocale come specificato nei dettagli di un contatto.

Per informazioni sulla gestione dei contatti e sulle opzioni di notifica dei contatti, consultaCreazione e configurazione dei contatti in Incident Manager.

Per aggiungere contatti a una rotazione in un programma di chiamata

1. Nella pagina Crea pianificazione delle chiamate, nella sezione Contatti relativa alla rotazione, scegli Aggiungi o rimuovi contatti.
2. Nella finestra di dialogo Aggiungi o rimuovi contatti, seleziona gli alias dei contatti da includere nella rotazione.

   L'ordine in cui selezionate i contatti corrisponde all'ordine in cui vengono elencati per primi nella pianificazione di rotazione. Puoi modificare l'ordine dopo aver aggiunto i contatti.
3. Scegli Conferma.
4. Per modificare la posizione di un contatto nell'ordine, seleziona il pulsante di opzione per quell'utente e usa i pulsanti Su
   ()
   e Giù
   ()
   per aggiornare l'ordine dei contatti.

5. Continuate specificando la ricorrenza e la durata della rotazione dei singoli turni.

Specificazione della ricorrenza e della durata dello spostamento e aggiunta di tag a una rotazione in Incident Manager

Shift recurrence specifica la frequenza con cui i contatti in una rotazione ruotano dentro e fuori dalla chiamata. La durata della ricorrenza può essere specificata in un numero di giorni, settimane o mesi.

Per specificare la ricorrenza e la durata dello spostamento e aggiungere tag a una rotazione

1. Nella pagina Crea pianificazione delle chiamate, nella sezione Impostazioni di ricorrenza per la rotazione, procedi come segue:

   - Per il tipo di ricorrenza Turno, specifica se ogni turno di chiamata dura un certo numero di giorni, settimane o mesi scegliendo tra, e. `Daily` `Weekly` `Monthly`
   - Per Durata del turno, inserisci quanti giorni, settimane o mesi dura un turno.

     Ad esempio, se hai scelto `Daily` e inserisci**1**, il turno di reperibilità di ogni contatto dura un giorno. Se hai scelto `Weekly` e inserito**3**, il turno di chiamata di ogni contatto dura tre settimane.
2. (Facoltativo) Nell'area Tag, applicate una o più coppie di nomi chiave e valori dei tag alla rotazione.

   I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, puoi etichettare una rotazione per identificare la posizione dei contatti ad essa assegnati, il tipo di copertura che dovrebbe fornire o il piano di escalation che supporterà. Per ulteriori informazioni sull'etichettatura delle risorse di Incident Manager, consulta. Etichettatura delle risorse in Incident Manager
3. (Consigliato) Utilizza l'anteprima del calendario per assicurarti che non vi siano interruzioni involontarie nella copertura della programmazione delle chiamate.
4. Scegli Create (Crea) .

Ora puoi aggiungere la programmazione delle chiamate come canale di escalation in un piano di intensificazione. Per informazioni, consultare Crea un piano di escalation.

Gestione di una pianificazione delle chiamate esistente in Incident Manager

Utilizza il contenuto di questa sezione per aiutarti a lavorare con gli orari di chiamata che hai già creato.

Argomenti

Visualizzazione dei dettagli degli orari delle chiamate

È possibile accedere a un at-a-glance riepilogo della pianificazione delle chiamate nella pagina Visualizza i dettagli della pianificazione delle chiamate. Questa pagina contiene anche informazioni su chi è attualmente reperibile e chi lo sarà successivamente. La pagina include una visualizzazione del calendario che mostra quali contatti sono disponibili in qualsiasi momento.

Per visualizzare i dettagli della pianificazione delle chiamate

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.
3. Nella riga relativa alla programmazione delle chiamate da visualizzare, esegui una delle seguenti operazioni:

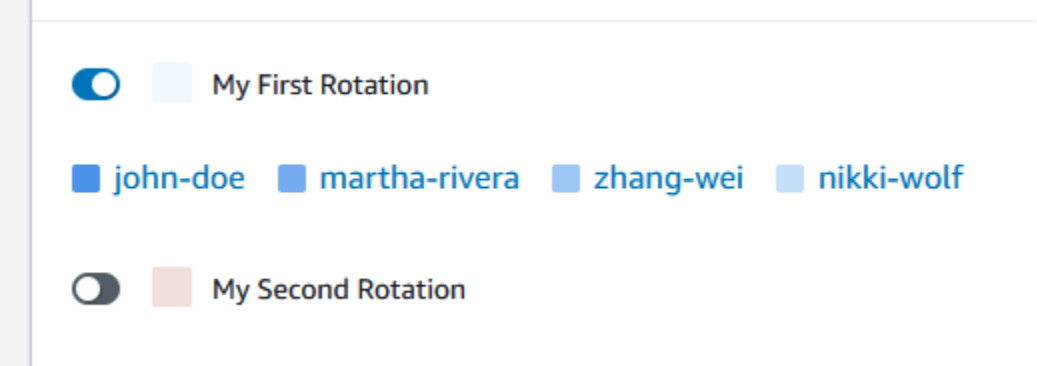
   - Per aprire una visualizzazione riepilogativa del calendario, scegli l'alias di pianificazione.

     oppure

     Seleziona il pulsante di opzione per la riga, quindi scegli Visualizza.
   - Per aprire una visualizzazione del calendario, scegli Visualizza calendario
     

     Nella visualizzazione calendario, scegli il nome di un contatto in una data specifica della pianificazione per visualizzare i dettagli sul turno assegnato o creare un'eccezione,.

- Per attivare o disattivare la visualizzazione di una rotazione specifica nel calendario, scegli l'interruttore accanto al nome della rotazione.



Modifica di un programma di chiamata

È possibile aggiornare la configurazione per una pianificazione delle chiamate e le relative rotazioni, ad eccezione dei seguenti dettagli:

- L'alias di pianificazione
- Nomi di rotazione
- Date di inizio della rotazione

Per utilizzare un calendario esistente come base per un nuovo calendario con la possibilità di modificare questi valori, puoi invece copiare il calendario. Per informazioni, consultare Copiare un programma di chiamata.

Per modificare un programma di chiamata

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.
3. Esegui una di queste operazioni:
   - Seleziona il pulsante di opzione nella riga per modificare la programmazione delle chiamate, quindi scegli Modifica.
   - Scegli l'alias di pianificazione per la pianificazione delle chiamate per aprire la pagina Visualizza i dettagli della pianificazione delle chiamate, quindi scegli Modifica.
4. Apporta le modifiche necessarie alla pianificazione delle chiamate e alle relative rotazioni. È possibile modificare le opzioni di configurazione della rotazione, ad esempio l'ora di inizio e di

fine, i contatti e la ricorrenza. È possibile aggiungere o rimuovere le rotazioni dalla pianificazione in base alle esigenze. L'anteprima del calendario riflette le modifiche apportate man mano che le apporti.

Per informazioni sull'utilizzo delle opzioni della pagina, consultaCreazione di una pianificazione e di una rotazione delle chiamate in Incident Manager.

5. Scegli Aggiorna.

> **Important**
>
> Se modifichi una pianificazione che contiene sostituzioni, le modifiche possono influire sulle sostituzioni. Per garantire che le sostituzioni rimangano configurate come previsto, ti consigliamo di rivedere attentamente le sostituzioni dei turni dopo aver aggiornato la pianificazione.

Copiare un programma di chiamata

Per utilizzare la configurazione di una pianificazione delle chiamate esistente come punto di partenza per una nuova pianificazione, è possibile creare una copia del calendario e modificarlo secondo necessità.

Per copiare una pianificazione delle chiamate

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.
3. Seleziona il pulsante radio nella riga per copiare il programma delle chiamate.
4. Scegli Copia.
5. Apporta le modifiche necessarie al calendario e alle sue rotazioni. È possibile modificare, aggiungere o rimuovere le rotazioni in base alle esigenze.

> **Note**
>
> Quando copi una pianificazione esistente, devi specificare nuove date di inizio per ogni rotazione. Le pianificazioni copiate non supportano rotazioni con date di inizio precedenti.

Per informazioni sull'utilizzo delle opzioni della pagina, consulta. Creazione di una pianificazione e di una rotazione delle chiamate in Incident Manager

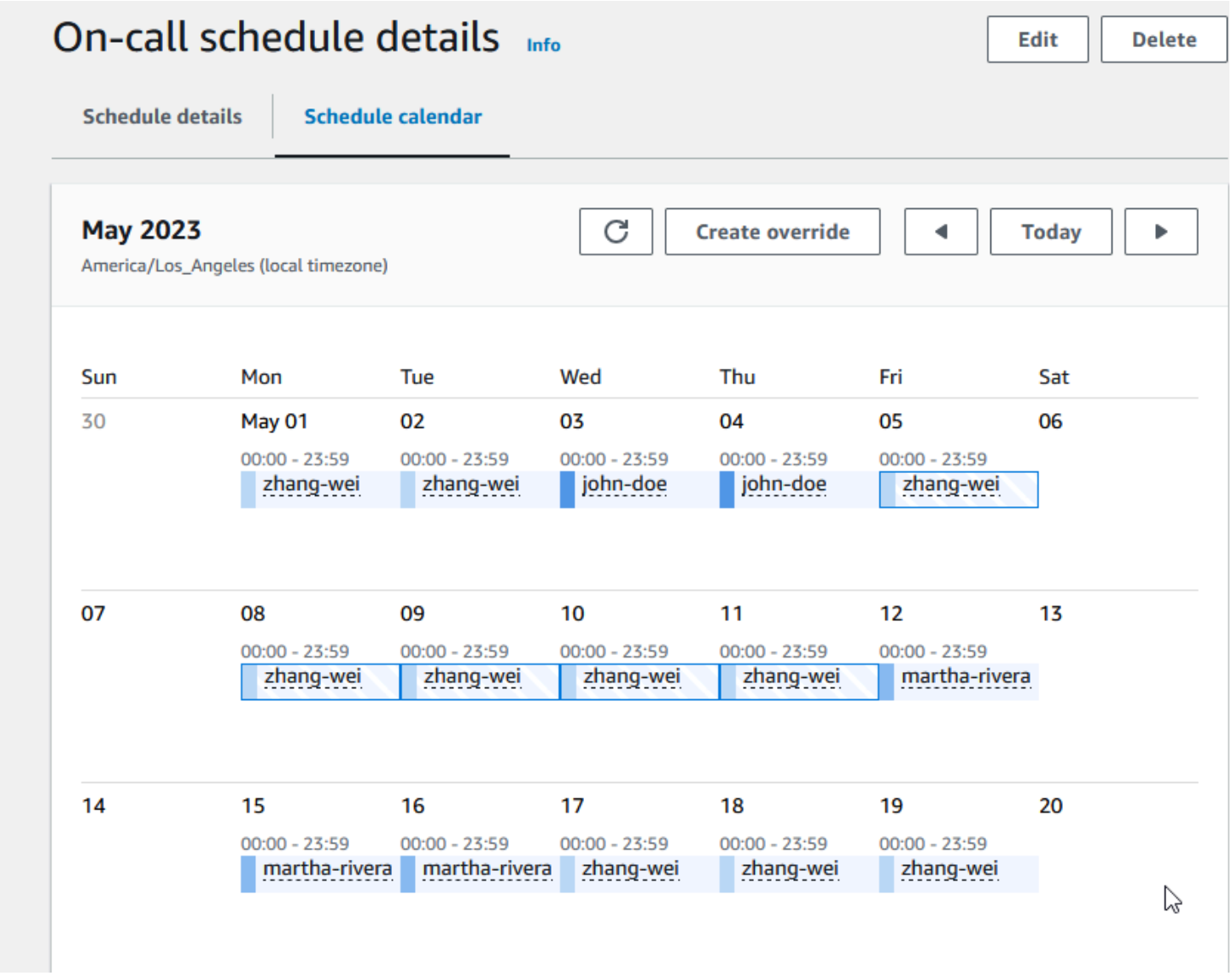
6. Scegli Crea copia.

Creazione di un override per una rotazione del programma di chiamata

Se è necessario apportare modifiche una tantum a un programma di rotazione esistente, è possibile creare un'eccezione. Un override consente di sostituire tutto o parte del turno di un contatto con un altro contatto. Puoi anche creare un override che si estenda su più turni.

È possibile assegnare a un override solo i contatti già assegnati alla rotazione.

Nell'anteprima del calendario, i turni sostituiti vengono visualizzati con uno sfondo a strisce anziché uno sfondo a tinta unita. L'immagine seguente mostra che il contatto di nome Zhang Wei è interpellato in modalità alternativa. L'override include parti dei turni di John Doe e Martha Rivera, che iniziano il 5 maggio e terminano l'11 maggio.



Per creare un'eccezione per un programma di chiamata

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.
3. Nella riga relativa alla programmazione delle chiamate da visualizzare, esegui una delle seguenti operazioni:
   - Scegli l'alias di pianificazione, quindi scegli la scheda Calendario Pianifica.
   - Scegli Visualizza calendario
4. Esegui una di queste operazioni:
   - Scegli Crea override.

- Scegli il nome di un contatto nell'anteprima del calendario, quindi scegli Sostituisci spostamento.

5. Nella finestra di dialogo Create shift override, procedi come segue:

> **Note**
>
> L'override deve avere una durata di almeno 30 minuti. È possibile specificare un'eccezione solo per i turni che si verificano non più di sei mesi nel futuro.

   a. Per Seleziona rotazione, seleziona il nome della rotazione in cui creare una sostituzione.
   b. Per Data di inizio, selezionate o immettete la data di inizio dell'override.
   c. Per Ora di inizio, inserisci l'ora in cui inizia l'override nel `hh:mm` formato.
   d. Per Data di fine, seleziona o inserisci la data di fine dell'override.
   e. Per Ora di fine, inserisci l'ora in cui termina l'override, nel `hh:mm` formato.
   f. Per Seleziona un contatto sostitutivo, seleziona il nome del contatto di rotazione che è in chiamata durante il periodo di sostituzione.

6. Scegli Crea override.

Dopo aver creato una sovrascrittura, puoi identificarla in base allo sfondo a strisce. Quando scegli il nome del contatto per un turno sostituito, una casella informativa lo identifica come spostamento sostituito. Puoi scegliere Elimina sostituisci per rimuoverlo e ripristinare l'assegnazione originale durante la chiamata.

Eliminazione di un programma di chiamata

Quando non è più necessario un particolare orario di chiamata, è possibile eliminarlo da Incident Manager.

Se alcuni piani di intensificazione o piani di risposta attualmente utilizzano la pianificazione delle chiamate come canale di escalation, è necessario rimuoverla da tali piani prima di eliminare la pianificazione.

Per eliminare un programma di chiamata

1. Apri la console Incident Manager.
2. Nella barra di navigazione a sinistra, scegli Orari di chiamata.

3. Seleziona il pulsante radio nella riga per eliminare la programmazione delle chiamate.
4. Scegli Elimina.
5. Nella sezione Eliminare la pianificazione delle chiamate? finestra di dialogo, inserisci **`confirm`** nella casella di testo.
6. Scegli Delete (Elimina).

Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager fornisce percorsi di escalation attraverso contatti definiti o orari di chiamata, noti collettivamente come canali di escalation. È possibile inserire più canali di escalation in un incidente contemporaneamente. Se i contatti designati nel canale di segnalazione non rispondono, Incident Manager passa al gruppo di contatti successivo. Puoi anche scegliere se interrompere l'intensificazione del piano una volta che un utente riconosce il coinvolgimento. È possibile aggiungere piani di escalation a un piano di risposta in modo che l'escalation inizi automaticamente all'inizio di un incidente. È inoltre possibile aggiungere piani di escalation a un incidente attivo.

Argomenti

Stage

I piani di escalation utilizzano fasi in cui ogni fase dura un numero definito di minuti. Ogni fase contiene le seguenti informazioni:

- Durata: il periodo di attesa del piano prima dell'inizio della fase successiva. La prima fase del piano di escalation inizia all'inizio dell'impegno.
- Canale di escalation: un canale di escalation è un singolo contatto o un programma di chiamata composto da più contatti che ruotano le responsabilità in base a una pianificazione definita. Il piano di escalation coinvolge ogni canale utilizzando il relativo piano di coinvolgimento definito. È possibile configurare ciascun canale di escalation per interrompere la progressione del piano di escalation prima che passi alla fase successiva. Ogni fase può avere più canali di escalation.

Per informazioni sulla configurazione dei singoli contatti, vedere. Creazione e configurazione dei contatti in Incident Manager Per informazioni sulla creazione di orari di chiamata, vedereGestione delle rotazioni dei soccorritori con pianificazioni di chiamata in Incident Manager.

Crea un piano di escalation

1. Apri la console Incident Manager e scegli i piani Escalation dalla barra di navigazione a sinistra.
2. Scegli Crea piano di escalation.
3. In Nome, inserisci un nome univoco per il piano di escalation, ad esempio. **`My Escalation Plan`**
4. Per Alias, inserisci un alias per aiutarti a identificare il piano, ad esempio. **`my-escalation-plan`**
5. Per la durata della Fase, immettete il numero di minuti in cui Incident Manager deve attendere fino al passaggio alla fase successiva.
6. Per il canale Escalation, scegli uno o più contatti o orari di chiamata con cui interagire durante questa fase.
7. (Facoltativo) Per consentire a un contatto di interrompere il piano di escalation una volta confermato il coinvolgimento, seleziona Riconoscimento interrompe la progressione del piano.
8. Per aggiungere un altro canale a questa fase, scegli Aggiungi canale di escalation.
9. Per aggiungere un'altra fase al piano di escalation, scegli Aggiungi fase.
10. Ripeti i passaggi da 5 a 9 fino a completare l'aggiunta dei canali di escalation e degli stadi desiderati per questo piano di escalation.
11. (Facoltativo) Nell'area Tag, applicate una o più coppie di nomi chiave e valori dei tag al piano di escalation.

    I tag sono metadati facoltativi assegnati a una risorsa. Consentono di categorizzare una risorsa in diversi modi, ad esempio in base allo scopo, al proprietario o all'ambiente. Ad esempio, è possibile etichettare un piano di escalation per identificare il tipo di incidenti per cui utilizzarlo, i tipi di canali di escalation che contiene o il piano di escalation supportato. Per ulteriori informazioni sull'etichettatura delle risorse di Incident Manager, vedere. Etichettatura delle risorse in Incident Manager
12. Scegli Crea piano di escalation.

Creazione e integrazione di canali di chat per i soccorritori in Incident Manager

Incident Manager, uno strumento che offre ai soccorritori la possibilità di comunicare direttamente attraverso i canali di chat durante un incidente. AWS Systems Manager Un canale di chat è una chat room che configuri in Amazon Q Developer nelle applicazioni di chat. Quindi connetti questo canale a un piano di risposta in Incident Manager.

Durante un incidente, i soccorritori utilizzano il canale di chat per comunicare tra loro in merito all'incidente. Incident Manager invia inoltre eventuali aggiornamenti e notifiche sull'incidente direttamente al canale di chat. Invia queste notifiche utilizzando uno o più argomenti di Amazon Simple Notification Service (Amazon SNS) specificati nella configurazione della chat room.

Amazon Q Developer nelle applicazioni di chat e Incident Manager supportano i canali di chat nelle seguenti applicazioni:

- Slack
- Microsoft Teams
- Amazon Chime

Il processo di configurazione di un canale di chat da utilizzare negli incidenti consiste in attività in tre diversi servizi Amazon Web Services.

Attività

- Attività 1: creare o aggiornare argomenti Amazon SNS per il tuo canale di chat
- Attività 2: creare un canale di chat in Amazon Q Developer nelle applicazioni di chat
- Attività 3: aggiungi il canale di chat a un piano di risposta in Incident Manager
- Interagire tramite il canale di chat

Attività 1: creare o aggiornare argomenti Amazon SNS per il tuo canale di chat

Amazon SNS è un servizio gestito che fornisce il recapito dei messaggi dagli editori agli abbonati (noti anche come produttori e consumatori). Gli editori comunicano in modo asincrono con gli abbonati creando e inviando messaggi a un argomento, che rappresenta un punto di accesso logico

e un canale di comunicazione. Incident Manager utilizza uno o più argomenti associati a un piano di risposta per inviare notifiche relative a un incidente ai soccorritori.

In un piano di risposta, puoi includere uno o più argomenti di Amazon SNS nelle notifiche degli incidenti. Come best practice, dovresti creare un argomento SNS in ognuno dei temi Regione AWS che hai aggiunto al tuo set di replica.

> **Tip**
>
> Per un flusso di lavoro di configurazione più lineare, ti consigliamo di configurare prima gli argomenti di Amazon SNS da utilizzare con Incident Manager. Una volta configurato, puoi creare il canale di chat.

Per creare o aggiornare argomenti di Amazon SNS per il tuo canale di chat

1. Segui i passaggi indicati nell'argomento Creazione di un Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service.

   > **Note**
   >
   > Dopo aver creato l'argomento, lo modifichi per aggiornarne la politica di accesso.

2. Seleziona l'argomento che hai creato e annota o copia l'Amazon Resource Name (ARN) dell'argomento, in un formato come. `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`
3. Scegli Modifica, quindi espandi la sezione Politica di accesso per configurare autorizzazioni di accesso aggiuntive oltre a quelle predefinite.
4. Aggiungi la seguente dichiarazione all'array Statement della policy:

```
{
    "Sid": "IncidentManagerSNSPublishingPermissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
```

```
        "StringEqualsIfExists": {
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

Sostituisci *placeholder values* come segue:

- *sns-topic-arn*è l'Amazon Resource Name (ARN) dell'argomento che hai creato per questa regione, nel formato. `arn:aws:sns:us-east-2:111122223333:My_SNS_topic`
- *account-id*è l'ID dell'ambiente in Account AWS cui stai lavorando, ad esempio`111122223333`.

5. Scegli Save changes (Salva modifiche).
6. Ripetere il processo in ogni regione inclusa nel set di replica.

Attività 2: creare un canale di chat in Amazon Q Developer nelle applicazioni di chat

Puoi creare un canale di chat in Slack, Microsoft Teamso Amazon Chime. È necessario un solo canale di chat per ogni piano di risposta.

Per i tuoi canali di chat, ti consigliamo di seguire il principio del privilegio minimo (non fornire agli utenti più autorizzazioni di quelle necessarie per completare le loro attività). Inoltre, dovresti controllare regolarmente l'iscrizione del tuo sviluppatore Amazon Q nei canali di chat delle applicazioni di chat. Le recensioni aiutano a verificare che solo i rispondenti appropriati e le altre parti interessate abbiano accesso ai tuoi canali di chat.

In Slack canali e Microsoft Teams canali creati in Amazon Q Developer nelle applicazioni di chat, i soccorritori possono eseguire una serie di comandi CLI di Incident Manager direttamente dal Slack oppure Microsoft Teams applicazione. Per ulteriori informazioni, consulta Interagire tramite il canale di chat.

> **Important**
>
> Gli utenti che aggiungi al tuo canale di chat devono essere gli stessi contatti elencati nel tuo piano di escalation o di risposta. Puoi anche aggiungere altri utenti ai canali di chat, come le parti interessate e gli osservatori degli incidenti.

Per informazioni generali su Amazon Q Developer nelle applicazioni di chat, consulta What is Amazon Q Developer in chat applications nella Amazon Q Developer in chat applications Administrator Guide.

Scegli tra le seguenti applicazioni in cui creare il tuo canale:

Slack

I passaggi di questa procedura forniscono le impostazioni di autorizzazione consigliate per consentire a tutti gli utenti del canale di utilizzare i comandi di chat con Incident Manager. Utilizzando i comandi di chat supportati, i soccorritori possono aggiornare l'incidente e interagire con esso direttamente dal Slack canale di chat. Per informazioni, consultare Interagire tramite il canale di chat.

Per creare un canale di chat in Slack

- Segui i passaggi del Tutorial: Inizia con Slacknella Guida per amministratori delle applicazioni Amazon Q Developer in chat e includi quanto segue nella configurazione.
  - Nel passaggio 10, per le impostazioni del ruolo, scegli il ruolo del canale.
  - Nel passaggio 10d, per i modelli di policy, seleziona Autorizzazioni di Incident Manager.
  - Nel passaggio 11, per le politiche di Channel Guardrail, per il nome della politica, scegli. `AWSIncidentManagerResolverAccess`
  - Nel passaggio 12, nella sezione Argomenti SNS, procedi come segue:
    - Per la Regione 1, selezionane Regione AWS una inclusa nel set di replica.
    - Per gli argomenti 1, seleziona l'argomento SNS che hai creato in quella regione da utilizzare per inviare notifiche di incidenti al canale di chat.
    - Per ogni regione aggiuntiva del set di replica, scegli Aggiungi un'altra regione e aggiungi gli argomenti aggiuntivi su Regioni e SNS.

Microsoft Teams

I passaggi di questa procedura forniscono le impostazioni di autorizzazione consigliate per consentire a tutti gli utenti del canale di utilizzare i comandi di chat con Incident Manager. Utilizzando i comandi di chat supportati, i soccorritori possono aggiornare l'incidente e interagire con esso direttamente dal Microsoft Teams canale di chat. Per informazioni, consultare Interagire tramite il canale di chat.

Per creare un canale di chat in Microsoft Teams

- Segui i passaggi del Tutorial: Inizia con Microsoft Teamsnella Guida per l'amministratore delle applicazioni Amazon Q Developer in chat e includi quanto segue nella configurazione:
  - Nel passaggio 10, per le impostazioni del ruolo, scegli il ruolo del canale.
  - Nel passaggio 10d, per i modelli di policy, seleziona Autorizzazioni di Incident Manager.
  - Nel passaggio 11, per le politiche di Channel Guardrail, per il nome della politica, scegli. `AWSIncidentManagerResolverAccess`
  - Nel passaggio 12, nella sezione Argomenti SNS, procedi come segue:
    - Per la Regione 1, selezionane Regione AWS una inclusa nel set di replica.
    - Per gli argomenti 1, seleziona l'argomento SNS che hai creato in quella regione da utilizzare per inviare notifiche di incidenti al canale di chat.
    - Per ogni regione aggiuntiva del set di replica, scegli Aggiungi un'altra regione e aggiungi gli argomenti aggiuntivi su Regioni e SNS.

Amazon Chime

Per creare un canale di chat in Amazon Chime

- Segui i passaggi indicati nel Tutorial: Inizia a usare Amazon Chime nella Guida per amministratori delle applicazioni Amazon Q Developer in chat e includi quanto segue nella tua configurazione:
  - Nel passaggio 11, per i modelli di policy, seleziona le autorizzazioni di Incident Manager.
  - Nel passaggio 12, nella sezione Argomenti SNS, seleziona gli argomenti SNS che invieranno notifiche al webhook Amazon Chime:
    - Per la regione 1, seleziona un elemento incluso nel Regione AWS set di replica.
    - Per gli argomenti 1, seleziona l'argomento SNS che hai creato in quella regione da utilizzare per inviare notifiche di incidenti al canale di chat.
    - Per ogni regione aggiuntiva del set di replica, scegli Aggiungi un'altra regione e aggiungi gli argomenti aggiuntivi su Regioni e SNS.

> **Note**
>
> Comandi di chat, utilizzabili dai soccorritori Slack e Microsoft Teams i canali di chat non sono supportati in Amazon Chime.

Attività 3: aggiungi il canale di chat a un piano di risposta in Incident Manager

Quando crei o aggiorni un piano di risposta, puoi aggiungere canali di chat tramite i quali i soccorritori possono comunicare e ricevere aggiornamenti.

Quando segui i passaggi indicati nella sezione Creazione di un piano di risposta (Facoltativo) Specificare un canale di chat per la risposta agli incidenti, seleziona il canale che desideri utilizzare per gli incidenti relativi a questo piano di risposta.

Interagire tramite il canale di chat

Per i canali in Slack e Microsoft Teams, Incident Manager consente ai soccorritori di interagire con gli incidenti direttamente dal canale di chat utilizzando i seguenti comandi: `ssm-incidents`

- inizio-incidente
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record
- update-timeline-event

Per eseguire comandi nel canale di chat di un incidente attivo, utilizza il seguente formato. Sostituisci *cli-options* con qualsiasi opzione da includere in un comando.

```
@aws ssm-incidents cli-options
```

Per esempio:

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti

È possibile utilizzare i runbook di AWS Systems Manager Automation, uno strumento di AWS Systems Manager, per automatizzare le attività comuni delle applicazioni e dell'infrastruttura nel proprio ambiente. Cloud AWS

Ogni runbook definisce un workflow di runbook, composto dalle azioni eseguite da Systems Manager sui nodi gestiti o su altri tipi di AWS risorse. È possibile utilizzare i runbook per automatizzare la manutenzione, l'implementazione e la riparazione delle risorse. AWS

In Incident Manager, un runbook favorisce la risposta e la mitigazione degli incidenti e si specifica un runbook da utilizzare come parte di un piano di risposta.

Nei piani di risposta, puoi scegliere tra dozzine di runbook preconfigurati per le attività più comunemente automatizzate oppure puoi creare runbook personalizzati. Quando si specifica un runbook nella definizione di un piano di risposta, il sistema può avviare automaticamente il runbook all'inizio di un incidente.

> **Important**
>
> Gli incidenti creati da un failover interregionale non richiamano i runbook specificati nei piani di risposta.

Per ulteriori informazioni su Systems Manager Automation, i runbook e l'utilizzo dei runbook con Incident Manager, vedere i seguenti argomenti:

- Per aggiungere un runbook a un piano di risposta, vedere. Creazione e configurazione dei piani di risposta in Incident Manager
- Per ulteriori informazioni sui runbook, consulta AWS Systems Manager Automation nella AWS Systems Manager User Guide e AWS Systems Manager Automation Runbook reference.
- Per informazioni sul costo dell'utilizzo dei runbook, consulta i prezzi di Systems Manager.
- Per informazioni sull'invocazione automatica dei runbook quando un incidente viene creato da un CloudWatch allarme Amazon o da un EventBridge evento Amazon, consulta Tutorial: Using Systems Manager Automation runbook with Incident Manager.

Argomenti

Autorizzazioni IAM necessarie per avviare ed eseguire i flussi di lavoro dei runbook

Incident Manager richiede le autorizzazioni per eseguire i runbook come parte della risposta agli incidenti. Per fornire queste autorizzazioni, si utilizzano i ruoli AWS Identity and Access Management (IAM), il ruolo del servizio Runbook e l'automazione. *`AssumeRole`*

Il ruolo di servizio Runbook è un ruolo di servizio obbligatorio. Questo ruolo fornisce a Incident Manager le autorizzazioni necessarie per accedere e avviare il flusso di lavoro per il runbook.

L'automazione `AssumeRole` fornisce le autorizzazioni necessarie per eseguire i singoli comandi specificati nel runbook.

> **Note**
>
> Se non `AssumeRole` viene specificato no, Systems Manager Automation tenta di utilizzare il ruolo del servizio Runbook per i singoli comandi. Se non si specifica un`AssumeRole`, è necessario aggiungere le autorizzazioni necessarie al ruolo del servizio Runbook. In caso contrario, il runbook non riesce a eseguire tali comandi.
> Tuttavia, come best practice di sicurezza, consigliamo di utilizzare un file separato`AssumeRole`. Con un ruolo separato`AssumeRole`, puoi limitare le autorizzazioni necessarie da aggiungere a ciascun ruolo.

Per ulteriori informazioni sull'automazione*`AssumeRole`*, consulta «Configurazione dell'accesso ai ruoli di servizio (assumi il ruolo) per le automazioni» nella Guida per l'AWS Systems Manager utente.

Puoi creare manualmente entrambi i tipi di ruolo nella console IAM.- Puoi anche lasciare che Incident Manager ne crei uno per te quando crei o aggiorni un piano di risposta.

Autorizzazioni per i ruoli di servizio Runbook

Le autorizzazioni per i ruoli del servizio Runbook vengono fornite tramite una politica simile alla seguente.

La prima istruzione consente a Incident Manager di avviare l'`StartAutomationExecution`operazione Systems Manager. Questa operazione viene quindi eseguita su risorse rappresentate dai tre formati Amazon Resource Name (ARN).

La seconda istruzione consente al ruolo del servizio Runbook di assumere un ruolo in un altro account quando tale runbook viene eseguito nell'account interessato. Per ulteriori informazioni, consulta Esecuzione di automazioni in più account nella Regioni AWS Guida per l'utente.AWS Systems Manager

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
```

```
            "Resource": [
                "arn:aws:ssm:*:111122223333:automation-definition/
{{DocumentName}}:*",
                "arn:aws:ssm:*:111122223333:document/{{DocumentName}}:*",
                "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "ssm.amazonaws.com"
                }
            }
        }
    ]
}
```

Autorizzazioni di automazione AssumeRole

Quando crei o aggiorni un piano di risposta, puoi scegliere tra diverse policy AWS gestite da allegare a AssumeRole quella creata da Incident Manager. Queste policy forniscono le autorizzazioni per eseguire una serie di operazioni comuni utilizzate negli scenari di runbook di Incident Manager. Puoi scegliere una o più di queste politiche gestite per fornire le autorizzazioni per la tua politica. `AssumeRole` La tabella seguente descrive le politiche tra cui è possibile scegliere quando si crea una `AssumeRole` dalla console Incident Manager.

Nome della policy gestita da AWS	Descrizione della politica
`AmazonSSMAutomationRole`	Concede le autorizzazioni al servizio Systems Manager Automation per eseguire le attività definite nei runbook. Assegna questa policy agli amministratori e agli utenti più affidabili.
`AWSIncidentManagerResolverAccess`	Concede agli utenti l'autorizzazione ad avviare, visualizzare e aggiornare gli incidenti . Puoi anche utilizzarli per creare eventi sulla

Nome della policy gestita da AWS	Descrizione della politica
	cronologia dei clienti e elementi correlati nella dashboard degli incidenti.

È possibile utilizzare queste politiche gestite per concedere le autorizzazioni per molti scenari comuni di risposta agli incidenti. Tuttavia, le autorizzazioni richieste per le attività specifiche necessarie possono variare. In questi casi, devi fornire autorizzazioni politiche aggiuntive per il tuo. `AssumeRole` Per informazioni, consulta il riferimento all'AWS Systems Manager Automation Runbook.

Utilizzo dei parametri del runbook

Quando si aggiunge un runbook a un piano di risposta, è possibile specificare i parametri che il runbook deve utilizzare in fase di esecuzione. I piani di risposta supportano parametri con valori statici e dinamici. Per i valori statici, inserisci il valore quando definisci il parametro nel piano di risposta. Per i valori dinamici, il sistema determina il valore corretto del parametro raccogliendo informazioni dall'incidente. Incident Manager supporta i seguenti parametri dinamici:

`Incident ARN`

Quando Incident Manager crea un incidente, il sistema acquisisce il nome della risorsa Amazon (ARN) del record dell'incidente corrispondente e lo immette per questo parametro nel runbook.

> **Note**
>
> Questo valore può essere assegnato solo a parametri di tipo `String`. Se assegnato a un parametro di qualsiasi altro tipo, il runbook non viene eseguito.

`Involved resources`

Quando Incident Manager crea un incidente, il sistema acquisisce ARNs le risorse coinvolte nell'incidente. Queste risorse ARNs vengono quindi assegnate a questo parametro nel runbook.

Informazioni sulle risorse associate

Incident Manager può compilare i valori dei parametri ARNs del runbook con le AWS risorse specificate negli CloudWatch allarmi, negli EventBridge eventi e negli incidenti creati manualmente.

Questa sezione descrive i diversi tipi di risorse che Incident Manager può acquisire ARNs durante la compilazione di questo parametro.

CloudWatch allarmi

Quando viene creato un incidente a seguito di un'azione di CloudWatch allarme, Incident Manager estrae automaticamente i seguenti tipi di risorse dalle metriche associate. Quindi popola i parametri scelti con le seguenti risorse coinvolte:

AWS servizio	Tipo di risorsa
Amazon DynamoDB	Indici secondari globali Streams Tabelle
Amazon EC2	Immagini Istanze
AWS Lambda	Alias di funzioni Versioni della funzione Funzioni
Amazon Relational Database Service (Amazon RDS)	Cluster Istanze di database
Amazon Simple Storage Service (Amazon S3)	Bucket

EventBridge regole

Quando il sistema crea un incidente da un EventBridge evento, Incident Manager popola i parametri scelti con la `Resources` proprietà dell'evento. Per ulteriori informazioni, consulta EventBridgegli eventi Amazon nella Amazon EventBridge User Guide.

Incidenti creati manualmente

Quando si crea un incidente utilizzando l'azione StartIncidentAPI, Incident Manager inserisce i parametri scelti utilizzando le informazioni contenute nella chiamata API. In particolare, popola i parametri utilizzando elementi del tipo `INVOLVED_RESOURCE` che vengono passati nel `relatedItems` parametro.

> **Note**
>
> Il `INVOLVED_RESOURCES` valore può essere assegnato solo a parametri di tipo`StringList`. Se assegnato a un parametro di qualsiasi altro tipo, il runbook non viene eseguito.

Definire un runbook

Quando si crea un runbook, è possibile seguire i passaggi indicati qui oppure seguire la guida più dettagliata fornita nella sezione Working with runbook della Systems Manager User Guide. Se stai creando un runbook con più account e più regioni, consulta Running automations in multiple Regioni AWS and accounts nella Systems Manager User Guide.

Definisci un runbook

1. Aprire la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.
3. Scegliere Create automation (Crea automazione).
4. Immettete un nome di runbook univoco e identificabile.
5. Inserisci una descrizione del runbook.
6. Fornisci un ruolo IAM per il documento di automazione da assumere. Ciò consente al runbook di eseguire i comandi automaticamente. Per ulteriori informazioni, vedere Configurazione dell'accesso ai ruoli di servizio per i flussi di lavoro di automazione.
7. (Facoltativo) Aggiungi tutti i parametri di input con cui inizia il runbook. È possibile utilizzare parametri dinamici o statici all'avvio di un runbook. I parametri dinamici utilizzano i valori dell'incidente in cui viene avviato il runbook. I parametri statici utilizzano il valore fornito dall'utente.
8. (Facoltativo) Aggiungi un tipo di destinazione.
9. (Facoltativo) Aggiungi tag.

10. Compila i passaggi che il runbook eseguirà quando verrà eseguito. Ogni passaggio richiede:
    - un nome;
    - Una descrizione dello scopo della fase.
    - L'azione da eseguire durante la fase. I runbook utilizzano il tipo di azione Pause per descrivere un passaggio manuale.
    - (Facoltativo) Proprietà dei comandi.
11. Dopo aver aggiunto tutti i passaggi richiesti del runbook, scegli Create Automation.

Per abilitare la funzionalità tra più account, condividi il runbook nel tuo account di gestione con tutti gli account delle applicazioni che lo utilizzano durante un incidente.

Condividi un runbook

1. Aprire la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.
3. Nell'elenco dei documenti, scegli il documento che desideri condividere, quindi scegli Visualizza dettagli. Nella scheda Permissions (Autorizzazioni), verificare di essere il proprietario del documento. Soltanto il proprietario di un documento può condividerlo.
4. Scegli Modifica.
5. Per condividere il comando pubblicamente, scegliere Public (Pubblico), quindi selezionare Save (Salva). Per condividere il comando in privato, scegli Privato, inserisci l' Account AWS ID, scegli Aggiungi autorizzazione, quindi scegli Salva.

Modello di runbook di Incident Manager

Incident Manager fornisce il seguente modello di runbook per aiutare il team a iniziare a creare runbook nell'automazione di Systems Manager. È possibile utilizzare questo modello così com'è o modificarlo per includere dettagli specifici dell'applicazione e delle risorse.

Trova il modello di runbook di Incident Manager

1. Aprire la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.

3. Nell'area Documenti, accedete al campo **`AWSIncidents-`** di ricerca per visualizzare tutti i runbook di Incident Manager.

> **Tip**
>
> Immettete **`AWSIncidents-`** come testo libero invece di utilizzare l'opzione di filtro del prefisso del nome del documento.

Utilizzando un modello

1. Aprire la console Systems Manager all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.
3. Scegli il modello che desideri aggiornare dall'elenco dei documenti.
4. Scegli la scheda Contenuto, quindi copia il contenuto del documento.
5. Nel riquadro di navigazione, scegli Documenti.
6. Scegliere Create automation (Crea automazione).
7. Immettete un nome univoco e identificabile.
8. Scegli la scheda Editor.
9. Scegli Modifica.
10. Incolla o inserisci i dettagli copiati nell'area dell'editor del documento.
11. Scegliere Create automation (Crea automazione).

`AWSIncidents-CriticalIncidentRunbookTemplate`

`AWSIncidents-CriticalIncidentRunbookTemplate`È un modello che fornisce il ciclo di vita degli incidenti di Incident Manager in passaggi manuali. Questi passaggi sono abbastanza generici da poter essere utilizzati nella maggior parte delle applicazioni, ma sufficientemente dettagliati da consentire ai soccorritori di iniziare a risolvere gli incidenti.

Creazione e configurazione dei piani di risposta in Incident Manager

I piani di risposta consentono di pianificare come rispondere a un incidente che ha un impatto sugli utenti. Un piano di risposta funziona come un modello che include informazioni su chi coinvolgere, sulla gravità prevista dell'evento, sui runbook automatici da avviare e sulle metriche da monitorare.

Best practice

Puoi ridurre l'impatto degli incidenti sui tuoi team pianificando gli incidenti in anticipo. I team devono prendere in considerazione le seguenti best practice quando progettano un piano di risposta.

- Interazione semplificata: identifica il team più appropriato per un incidente. Se ti rivolgi a una lista di distribuzione troppo ampia o se coinvolgi i team sbagliati, puoi creare confusione e far perdere tempo ai soccorritori durante un incidente.
- Escalation affidabile: per le vostre interazioni in un piano di risposta, vi consigliamo di selezionare un piano di coinvolgimento anziché i contatti o gli orari di chiamata. Il piano di coinvolgimento dovrebbe specificare i singoli contatti o gli orari di chiamata (che contengono più contatti a rotazione) da coinvolgere durante gli incidenti. Poiché a volte i soccorritori specificati nel piano di coinvolgimento possono essere irraggiungibili, è necessario configurare i risponditori di riserva nel piano di risposta per coprire questi scenari. Con i contatti di backup, se i contatti primari e secondari non sono disponibili o se ci sono altre lacune di copertura non pianificate, Incident Manager notifica comunque l'incidente a un contatto.
- Runbook: utilizza i runbook per fornire passaggi ripetibili e comprensibili che riducono lo stress che il soccorritore prova durante un incidente.
- Collaborazione: utilizza i canali di chat per semplificare la comunicazione durante gli incidenti. I canali di chat aiutano i soccorritori a rimanere aggiornati sulle informazioni. Possono anche condividere informazioni con altri soccorritori tramite questi canali.

Creazione di un piano di risposta

Utilizzare la procedura seguente per creare un piano di risposta e automatizzare la risposta agli incidenti.

Come creare un piano di risposta

1. Apri la console Incident Manager e, nel riquadro di navigazione, scegli Piani di risposta.

2. Scegli Crea piano di risposta.
3. Per Nome, inserisci un nome di piano di risposta univoco e identificabile da utilizzare nell'Amazon Resource Name (ARN) per il piano di risposta.
4. (Facoltativo) In Nome visualizzato, inserisci un nome più leggibile dall'uomo per aiutare a identificare il piano di risposta quando crei incidenti.
5. Continua specificando i valori predefiniti per i record degli incidenti.

Specificazione dei valori predefiniti degli incidenti

Per aiutarti a gestire gli incidenti in modo più efficace, puoi specificare valori predefiniti. Incident Manager applica questi valori a tutti gli incidenti associati a un piano di risposta.

Per specificare i valori predefiniti degli incidenti

1. In Titolo, inserisci un titolo per questo incidente per aiutarti a identificarlo nella home page di Incident Manager.
2. Per Impatto, scegli un livello di impatto per indicare la portata potenziale di un incidente creato da questo piano di risposta, ad esempio Critico o Basso. Per informazioni sulle valutazioni di impatto in Incident Manager, vedereTriage.
3. (Facoltativo) In Riepilogo, inserisci un breve riepilogo del tipo di incidenti creati da questo piano di risposta.
4. (Facoltativo) Per la stringa di deduplicazione, immettere una stringa di deduplicazione. Incident Manager utilizza questa stringa per impedire che la stessa causa principale crei più incidenti nello stesso account.

   Una stringa di deduplicazione è un termine o una frase che il sistema utilizza per verificare la presenza di incidenti duplicati. Se si specifica una stringa di deduplicazione, Incident Manager cerca gli incidenti aperti che contengono la stessa stringa nel campo al momento della creazione dell'incidente. `dedupeString` Se viene rilevato un duplicato, Incident Manager deduplica l'incidente più recente nell'incidente esistente.

   > **Note**
   >
   > Per impostazione predefinita, Incident Manager deduplica automaticamente più incidenti creati dallo stesso allarme Amazon CloudWatch o evento Amazon. EventBridge Non è

necessario inserire la propria stringa di deduplicazione per impedire la duplicazione di questi tipi di risorse.

5. (Facoltativo) In Tag degli incidenti, aggiungi le chiavi e i valori dei tag da assegnare agli incidenti creati da questo piano di risposta.

   È necessario disporre dell'`TagResource`autorizzazione della risorsa di registrazione degli incidenti per impostare i tag degli incidenti all'interno del piano di risposta.

6. Continua specificando un canale di chat opzionale per consentire ai risolutori di comunicare tra loro sugli incidenti.

(Facoltativo) Specificare un canale di chat per la risposta agli incidenti

Quando includi un canale di chat in un piano di risposta, i soccorritori ricevono aggiornamenti sugli incidenti tramite il canale. Possono interagire con l'incidente direttamente dal canale di chat utilizzando i comandi della chat.

Utilizzando Amazon Q Developer nelle applicazioni di chat, puoi creare un canale per SlackMicrosoft Teams, per o per Amazon Chime da utilizzare nei tuoi piani di risposta. Per informazioni sulla creazione di un canale di chat in Amazon Q Developer in applicazioni di chat, consulta la Amazon Q Developer in chat application Administrator Guide.

> **Important**
>
> Incident Manager deve disporre delle autorizzazioni per pubblicare sull'argomento Amazon Simple Notification Service (Amazon SNS) di un canale di chat. Senza le autorizzazioni per la pubblicazione su quell'argomento SNS, non puoi aggiungerlo al piano di risposta. Incident Manager pubblica una notifica di test sull'argomento SNS per verificare le autorizzazioni.

Per ulteriori informazioni sui canali di chat, consulta. Creazione e integrazione di canali di chat per i soccorritori in Incident Manager

Per specificare un canale di chat per la risposta agli incidenti

1. Per il canale di chat, seleziona uno sviluppatore Amazon Q nel canale di chat delle applicazioni di chat in cui i soccorritori possono comunicare durante un incidente.

> **Tip**
>
> Per creare un nuovo canale di chat in Amazon Q Developer nelle applicazioni di chat, scegli Configura nuovo client Chatbot.

2. Per gli argomenti SNS del canale di chat, scegli altri argomenti SNS su cui pubblicare durante l'incidente. L'aggiunta di più argomenti SNS Regioni AWS aumenta la ridondanza nel caso in cui una regione non fosse disponibile al momento dell'incidente.
3. Continua selezionando i contatti, gli orari delle chiamate e i piani di escalation da coinvolgere durante un incidente.

(Facoltativo) Seleziona le risorse per intervenire nella risposta agli incidenti

È importante identificare i soccorritori più appropriati quando si verifica un incidente. Come best practice, ti consigliamo di fare quanto segue:

1. Aggiungi i contatti e gli orari delle chiamate come canali di escalation in un piano di escalation.

> **Note**
>
> Attualmente, la possibilità di aggiungere un contatto condiviso da un altro account a un piano di risposta non è supportata.

2. Scegli un piano di escalation come coinvolgimento in un piano di risposta.

Per ulteriori informazioni sui contatti e sui piani di escalation, consulta e. Creazione e configurazione dei contatti in Incident Manager Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager

Per selezionare le risorse da impiegare nella risposta agli incidenti

1. Per quanto riguarda gli interventi, scegli un numero qualsiasi di piani di intensificazione, orari di chiamata e contatti individuali.
2. Continua specificando facoltativamente un runbook da eseguire come parte della mitigazione degli incidenti.

(Facoltativo) Specificare un runbook per la mitigazione degli incidenti

È possibile utilizzare i runbook di AWS Systems Manager Automation, uno strumento di AWS Systems Manager, per automatizzare le attività comuni delle applicazioni e dell'infrastruttura nel proprio ambiente. Cloud AWS

Ogni runbook definisce un flusso di lavoro di runbook. Un workflow di runbook include le azioni che Systems Manager esegue sui nodi gestiti o su altri tipi di AWS risorse. In Incident Manager, un runbook favorisce la risposta e la mitigazione degli incidenti.

Per ulteriori informazioni sull'utilizzo dei runbook nei piani di risposta,. Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti

Per specificare un runbook per la mitigazione degli incidenti:

1. Per Runbook, effettuate una delle seguenti operazioni:

   - Scegli Clone runbook dal modello per creare una copia del runbook predefinito di Incident Manager. Per il nome del runbook, inserisci un nome descrittivo per il nuovo runbook.
   - Scegli Seleziona il runbook esistente. Seleziona il proprietario, il runbook e la versione da utilizzare.

   > **Tip**
   >
   > Per creare un runbook da zero, scegli Configura nuovo runbook.
   > Per ulteriori informazioni sulla creazione di runbook, consulta Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti.

2. Nell'area Parametri, fornisci tutti i parametri richiesti per il runbook selezionato.

   I parametri disponibili sono quelli specificati dal runbook. Un runbook potrebbe richiedere parametri diversi da un altro. Alcuni parametri potrebbero essere obbligatori e altri facoltativi.

   In molti casi, puoi scegliere di inserire manualmente un valore statico per un parametro, ad esempio un elenco di EC2 istanze Amazon IDs. Puoi anche lasciare che Incident Manager fornisca i valori dei parametri generati dinamicamente da un incidente.

3. (Facoltativo) Per AutomationAssumeRole, specifica il ruolo AWS Identity and Access Management (IAM) da utilizzare. Questo ruolo deve disporre delle autorizzazioni necessarie per eseguire i singoli comandi specificati nel runbook.

> **Note**
>
> Se non `AssumeRole` viene specificato no, Incident Manager tenta di utilizzare il ruolo del servizio Runbook per eseguire i singoli comandi specificati all'interno del runbook.

Scegli tra le seguenti opzioni:

- Inserisci il valore ARN: inserisci manualmente l'Amazon Resource Name (ARN) di un AssumeRole, nel formato. `arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`* Ad esempio, **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
- Usa il ruolo di servizio esistente: scegli un ruolo con le autorizzazioni richieste da un elenco di ruoli esistenti nel tuo account.
- Crea un nuovo ruolo di servizio: scegli tra le politiche AWS gestite da allegare al tuo AssumeRole. Dopo aver selezionato questa opzione, per le politiche AWS gestite, scegli una o più politiche dall'elenco.

  Puoi accettare il nome predefinito suggerito per il nuovo ruolo o inserire un nome a tua scelta.

  > **Note**
  >
  > Questo nuovo ruolo del servizio Runbook è associato al runbook specifico selezionato. Non può essere utilizzato con runbook diversi. Questo perché la sezione Resource della policy non supporterà altri runbook.

4. Per il ruolo del servizio Runbook, specifica il ruolo IAM da utilizzare per fornire le autorizzazioni necessarie per accedere e avviare il flusso di lavoro per il runbook stesso.

   Come minimo, il ruolo deve consentire l'`ssm:StartAutomationExecution`azione per il runbook specifico. Affinché il runbook funzioni su più account, il ruolo deve consentire anche l'`sts:AssumeRole`azione relativa al `AWS-SystemsManager-AutomationExecutionRole` ruolo creato durante la creazione. Gestione degli incidenti in tutte Account AWS le regioni in Incident Manager

   Scegli tra le seguenti opzioni:

- Crea un nuovo ruolo di servizio: Incident Manager crea automaticamente un ruolo del servizio Runbook che include le autorizzazioni minime richieste per avviare il flusso di lavoro del runbook.

  Per il nome del ruolo, puoi accettare il nome predefinito suggerito o inserire un nome a tua scelta. Ti consigliamo di utilizzare il nome suggerito o di mantenere il nome del runbook nel nome. Questo perché il nuovo AssumeRole è associato al runbook specifico selezionato e potrebbe non includere le autorizzazioni richieste per altri runbook.
- Usa il ruolo di servizio esistente: un ruolo IAM creato in precedenza da te o da Incident Manager concede le autorizzazioni necessarie.

  Per Nome ruolo, seleziona il nome del ruolo esistente da utilizzare.

5. Espandi Opzioni aggiuntive e scegli una delle seguenti opzioni per specificare Account AWS dove deve essere eseguito il flusso di lavoro del runbook.

   - Account del proprietario del piano di risposta: avvia il flusso di lavoro del runbook nello stesso luogo in Account AWS cui lo ha creato.
   - Account interessato: avvia il flusso di lavoro del runbook nell'account che ha avviato o segnalato l'incidente.

     Scegliete l'account Impacted quando utilizzate Incident Manager per scenari con più account e il runbook deve accedere alle risorse dell'account interessato per porvi rimedio.

6. Continua integrando facoltativamente un servizio nel piano di risposta. PagerDuty

(Facoltativo) Integrazione di un PagerDuty servizio nel piano di risposta

Integrare un PagerDuty servizio nel piano di risposta

Quando si integra Incident Manager con PagerDuty, PagerDuty crea un incidente corrispondente ogni volta che Incident Manager crea un incidente. L'incidente PagerDuty utilizza il flusso di lavoro di paging e le politiche di escalation ivi definite, oltre a quelle di Incident Manager. PagerDuty allega gli eventi della cronologia di Incident Manager come note sull'incidente.

1. Espandi le integrazioni di terze parti, quindi seleziona la casella di controllo Abilita PagerDuty integrazione.

2. Per Seleziona segreto, seleziona il segreto in Gestione dei segreti AWS cui memorizzi le credenziali per accedere al tuo PagerDuty account.

   Per informazioni sulla memorizzazione delle PagerDuty credenziali in un segreto di Secrets Manager, vedereArchiviazione delle credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS.

3. Per PagerDuty assistenza, seleziona il servizio dal tuo PagerDuty account in cui desideri creare l' PagerDuty incidente.

4. Continua aggiungendo tag opzionali e creando il piano di risposta.

Aggiungere tag e creare il piano di risposta

Per aggiungere tag e creare il piano di risposta

1. (Facoltativo) Nell'area Tag, applica una o più name/value coppie di chiavi di tag al piano di risposta.

   I tag sono metadati facoltativi assegnati a una risorsa. Con i tag, puoi classificare una risorsa in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, potresti voler etichettare un piano di risposta per identificare il tipo di incidente che intende mitigare, i tipi di canali di escalation che contiene o il piano di escalation che verrà associato ad esso. Per ulteriori informazioni sull'etichettatura delle risorse di Incident Manager, vedere. Etichettatura delle risorse in Incident Manager

2. Scegli Crea piano di risposta.

Identificazione delle potenziali cause di incidenti derivanti da altri servizi come «risultati» in Incident Manager

In Incident Manager, un risultato è costituito da informazioni su una AWS CodeDeploy distribuzione o su un aggiornamento AWS CloudFormation dello stack avvenuto nel periodo in cui si è verificato un incidente e che ha coinvolto una o più risorse probabilmente correlate all'incidente. Ogni risultato può essere esaminato come causa potenziale dell'incidente. Le informazioni su queste potenziali cause vengono aggiunte alla pagina dei dettagli dell'incidente relativa a un incidente. Con le informazioni su queste implementazioni e modifiche a portata di mano, i soccorritori non devono

cercare manualmente queste informazioni. Ciò riduce il tempo necessario per valutare le potenziali cause, il che può ridurre il tempo medio di ripristino (MTTR) da un incidente.

Attualmente, Incident Manager supporta la raccolta dei risultati da due Servizi AWS: e. AWS CodeDeployAWS CloudFormation

Findings è una funzionalità opzionale. È possibile abilitarla nella procedura guidata Get prepared, quando si effettua per la prima volta l'onboarding a Incident Manager, o successivamente nella pagina Impostazioni.

Quando abiliti la funzionalità Findings, Incident Manager crea un ruolo di servizio per te. Questo ruolo di servizio include le autorizzazioni necessarie per recuperare i risultati da CodeDeploy e. CloudFormation

Per utilizzare i risultati in uno scenario che coinvolge più account, abilita la funzionalità nell'account di gestione. Dopodiché, ogni account dell'applicazione in un'organizzazione AWS Resource Access Manager (AWS RAM) deve creare un ruolo di servizio corrispondente.

Fate riferimento ai seguenti argomenti per aiutarvi a utilizzare la funzione Findings.

Argomenti

- Abilita e crea un ruolo di servizio per i risultati
- Configura le autorizzazioni per il supporto dei risultati tra account

Abilita e crea un ruolo di servizio per i risultati

Quando abiliti la funzionalità Findings, Incident Manager crea un ruolo di servizio denominato per tuo `IncidentManagerIncidentAccessServiceRole` conto. Questo ruolo di servizio fornisce le autorizzazioni necessarie a Incident Manager per raccogliere informazioni sulle CodeDeploy distribuzioni e sugli aggiornamenti CloudFormation dello stack avvenuti nel momento in cui è stato creato un incidente.

> **Note**
>
> Se si utilizza Incident Manager con un'organizzazione, il ruolo di servizio viene creato nell'account di gestione. Per utilizzare i risultati di altri account dell'organizzazione, è necessario creare il ruolo di servizio in ogni account dell'applicazione. Per informazioni sull'utilizzo di un CloudFormation modello per creare questo ruolo negli account

dell'applicazione, consulta la fase 4 diImposta e configura la gestione degli incidenti tra account.

Questo ruolo di servizio è associato a una politica AWS gestita. Per informazioni sulle autorizzazioni contenute in questa politica, vedereAWS politica gestita: AWSIncident ManagerIncidentAccessServiceRolePolicy.

Per informazioni sull'abilitazione dei risultati durante il processo di onboarding di Incident Manager, vedere. Guida introduttiva a Incident Manager

Per informazioni sull'attivazione dei risultati dopo aver completato il processo di onboarding, consulta. Gestione della funzione Findings

Configura le autorizzazioni per il supporto dei risultati tra account

Per utilizzare la funzionalità Findings in tutti gli account con un'organizzazione configurata in AWS RAM, ogni account dell'applicazione deve configurare le autorizzazioni affinché Incident Manager assuma il ruolo di servizio dell'account di gestione per suo conto.

Queste autorizzazioni possono essere configurate in un account dell'applicazione distribuendo un CloudFormation modello fornito da AWS, che crea il ruolo. `IncidentManagerIncidentAccessServiceRole`

Per informazioni sul download e la distribuzione di questo modello in un account dell'applicazione, consulta la fase 4 di. Gestione degli incidenti in tutte Account AWS le regioni in Incident Manager

Creazione automatica o manuale di incidenti in Incident Manager

Incident Manager, uno strumento di AWS Systems Manager, ti aiuta a gestire e rispondere rapidamente agli incidenti. Puoi configurare Amazon CloudWatch e Amazon EventBridge per creare automaticamente incidenti basati su CloudWatch allarmi ed EventBridge eventi. Puoi anche creare incidenti manualmente nella pagina dell'elenco degli incidenti o utilizzando l'azione StartIncidentAPI fornita da AWS CLI o dall'SDK. AWS Incident Manager deduplica gli incidenti creati dallo stesso CloudWatch allarme o EventBridge evento nello stesso incidente.

Per gli incidenti creati automaticamente da CloudWatch allarmi o EventBridge eventi, Incident Manager tenta di creare un incidente uguale alla Regione AWS regola dell'evento o all'allarme. Nel caso in cui Incident Manager non sia disponibile in Regione AWS, CloudWatch oppure crea EventBridge automaticamente l'incidente in una delle regioni disponibili specificate nel set di repliche. Per ulteriori informazioni, consulta Gestione degli incidenti in tutte Account AWS le regioni in Incident Manager.

Quando il sistema crea un incidente, Incident Manager raccoglie automaticamente le informazioni sulle AWS risorse coinvolte nell'incidente e le aggiunge alla scheda Elementi correlati. Se avete specificato un runbook nel piano di risposta, quando il sistema crea un incidente, Incident Manager può inviare le informazioni sulle AWS risorse coinvolte nell'incidente al runbook. Il sistema può quindi indirizzare tali risorse quando avvia il runbook e tenta di risolvere il problema.

Quando il sistema crea un incidente, crea anche un elemento di lavoro operativo principale (OpsItem) in OpsCenter, un componente di Systems Manager, e lo collega all'incidente come elemento correlato. È possibile utilizzarlo OpsItem per tenere traccia del lavoro correlato e delle analisi future degli incidenti. Chiamate OpsCenter a pagamento. Per ulteriori informazioni sui OpsCenter prezzi, consulta la pagina dei prezzi di Systems Manager.

> **Important**
>
> Tieni presenti queste importanti informazioni.
>
> - Nel caso in cui Incident Manager non sia disponibile, il sistema può eseguire il failover e creare incidenti in altre aree solo Regioni AWS se sono state specificate almeno due regioni nel set di replica. Per informazioni sulla configurazione di un set di replica, vedere. Guida introduttiva a Incident Manager

- Gli incidenti creati da un failover interregionale non richiamano i runbook specificati nei piani di risposta.

Creazione automatica di incidenti con allarmi CloudWatch

CloudWatch utilizza le tue CloudWatch metriche per avvisarti dei cambiamenti nel tuo ambiente e per eseguire automaticamente l'azione di avvio dell'incidente. CloudWatch collabora con Systems Manager e Incident Manager per creare un incidente da un modello di piano di risposta quando un allarme entra in stato di allarme. Ciò richiede i seguenti prerequisiti:

- Incident Manager configurato e set di replica creato. Questo passaggio crea il ruolo collegato al servizio Incident Manager nell'account, fornendo le autorizzazioni necessarie.
- Un piano di risposta configurato di Incident Manager. Per informazioni su come configurare i piani di risposta di Incident Manager, consulta Creazione e configurazione dei piani di risposta in Incident Manager la sezione Preparazione degli incidenti di questa guida.
- CloudWatch Metriche configurate per il monitoraggio dell'applicazione. Per le best practice di monitoraggio, Monitoraggio consulta la sezione Preparazione degli incidenti di questa guida.

Per creare un allarme con un'azione Start Incident

1. Crea un allarme in CloudWatch. Per ulteriori informazioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.
2. Quando scegli l'azione da eseguire per l'allarme, seleziona Aggiungi azione Systems Manager.
3. Scegli Crea incidente e seleziona il piano di risposta per questo incidente.
4. Completa i passaggi rimanenti nella guida al tipo di allarme selezionato.

> **Tip**
>
> Puoi anche aggiungere l'azione di creazione di un incidente a qualsiasi allarme esistente.

Creazione automatica di incidenti con EventBridge eventi

EventBridge le regole controllano i modelli degli eventi. Se l'evento corrisponde al modello definito, Incident Manager crea un incidente utilizzando il piano di risposta scelto.

Creazione di incidenti utilizzando gli eventi dei partner SaaS

È possibile EventBridge configurare la ricezione di eventi da applicazioni e servizi partner SaaS (Software as a Service), consentendo l'integrazione di terze parti. Dopo aver configurato EventBridge la ricezione di eventi da partner terzi, puoi creare regole che corrispondano agli eventi dei partner per creare incidenti. Per visualizzare un elenco di integrazioni di terze parti, consulta Ricezione di eventi da un partner SaaS.

Configura EventBridge per ricevere eventi da un'integrazione SaaS.

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel riquadro di navigazione, scegliere Partner event sources (Origini eventi partner).
3. Usa la barra di ricerca per trovare il partner che desideri e scegli Configura per quel partner.
4. Scegliere Copy (Copia) per copiare l'ID account negli appunti.

> **Note**
>
> Per l'integrazione con Salesforce, utilizza i passaggi descritti nella guida per AppFlow l'utente di Amazon.

5. Andare al sito Web del partner e seguire le istruzioni per creare un'origine evento partner. Utilizzare l'ID account per questo. L'origine dell'evento che crei è disponibile solo sul tuo account.
6. Torna alla EventBridge console e scegli Partner event sources nel pannello di navigazione.
7. Selezionare il pulsante accanto all'origine eventi partner e scegliere Associate with event bus (Associa a bus di eventi).

Crea una regola che si attiva in base agli eventi di un partner SaaS

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).

4. Inserire un nome e una descrizione per la regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.

5. Per Event bus, scegli l'event bus che corrisponde a questo partner.
6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Scegli Next (Successivo).
8. Per Event source, scegli AWS eventi o eventi EventBridge partner.
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Event source, scegli EventBridgei partner
11. Per i partner, scegli il nome del partner.
12. Per Event type (Tipo di evento), scegliere All Events (Tutti gli eventi) oppure scegliere il tipo di evento da utilizzare per questa regola. Se si sceglie All Events (Tutti gli eventi), tutti gli eventi emessi da questa origine eventi partner corrisponderanno alla regola.

    Se desideri personalizzare lo schema dell'evento, scegli Modifica, apporta le modifiche e quindi scegli Salva.

13. Scegli Next (Successivo).
14. Per Seleziona un obiettivo, scegli il piano di risposta di Incident Manager, quindi scegli un piano di risposta.

    > **Note**
    >
    > Quando selezioni un piano di risposta, tutti i piani di risposta che possiedi e che sono stati condivisi con il tuo account vengono visualizzati nell'elenco a discesa dei piani di risposta.

15. EventBridge può creare il ruolo IAM necessario per l'esecuzione della regola:

    - Per creare un ruolo IAM automaticamente, seleziona Create a new role for this specific resource (Crea un nuovo ruolo per questa risorsa specifica).
    - Per utilizzare un ruolo IAM creato in precedenza, seleziona Use existing role (Utilizza un ruolo esistente).

16. Scegli Next (Successivo).

17. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridgetag Amazon nella Amazon EventBridge User Guide.
18. Scegli Next (Successivo).
19. Controlla la regola, quindi scegli Crea regola.

Creazione di incidenti utilizzando eventi AWS di servizio

EventBridge riceve anche eventi dai AWS servizi elencati in Eventi dai AWS servizi supportati. Analogamente a come configuri le regole per i partner SaaS, puoi configurarle per AWS i servizi.

Crea una regola che si attiva in base agli eventi di un servizio AWS

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).
4. Inserire un nome e una descrizione per la regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.
5. Per Event bus (Bus di eventi), scegli default.
6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Scegli Next (Successivo).
8. Per Event source, scegli AWS eventi o eventi EventBridge partner.
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per Nome del servizio, scegli il servizio che monitora un incidente.
12. Per Event type (Tipo di evento), scegliere All Events (Tutti gli eventi) oppure scegliere il tipo di evento da utilizzare per questa regola. Se si sceglie All Events (Tutti gli eventi), tutti gli eventi emessi da questa origine eventi partner corrisponderanno alla regola.

    Se desideri personalizzare lo schema dell'evento, scegli Modifica, apporta le modifiche e quindi scegli Salva.
13. Scegli Next (Successivo).

14. Per Seleziona un obiettivo, scegli il piano di risposta di Incident Manager, quindi scegli un piano di risposta.

> **Note**
>
> Quando selezioni un piano di risposta, tutti i piani di risposta che possiedi e che sono stati condivisi con il tuo account vengono visualizzati nell'elenco a discesa dei piani di risposta.

15. EventBridge può creare il ruolo IAM necessario per l'esecuzione della regola:
    - Per creare un ruolo IAM automaticamente, seleziona Create a new role for this specific resource (Crea un nuovo ruolo per questa risorsa specifica).
    - Per utilizzare un ruolo IAM creato in precedenza, seleziona Use existing role (Utilizza un ruolo esistente).
16. Scegli Next (Successivo).
17. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i EventBridgetag Amazon nella Amazon EventBridge User Guide.
18. Scegli Next (Successivo).
19. Controlla la regola, quindi scegli Crea regola.

Creazione manuale degli incidenti

I soccorritori possono tracciare manualmente un incidente utilizzando la console Incident Manager utilizzando un piano di risposta predefinito. Utilizza i seguenti passaggi per creare un incidente.

1. Apri la console Incident Manager.
2. Scegli Avvia incidente.
3. Per Piano di risposta, scegli un piano di risposta dall'elenco.
4. (Facoltativo) Per sostituire il titolo fornito dal piano di risposta definito, inserisci un titolo per l'Incidente.
5. (Facoltativo) Per ignorare l'impatto fornito dal piano di risposta definito, inserisci l'Impatto dell'incidente.

Autorizzazioni IAM richieste per l'avvio manuale degli incidenti

Per avviare manualmente gli incidenti, gli utenti necessitano delle autorizzazioni per accedere alla console Incident Manager, visualizzare i piani di risposta e avviare gli incidenti. Quando un utente avvia un incidente, Incident Manager utilizza sessioni di accesso inoltrato (FAS) per effettuare la `StartEngagement` chiamata come parte di. `StartIncident`

La seguente policy IAM fornisce le autorizzazioni necessarie per avviare manualmente gli incidenti, visualizzare i piani di risposta con cui è possibile creare gli incidenti e visualizzare e modificare gli incidenti dopo la loro creazione.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

Questa policy include le seguenti autorizzazioni:

- ssm-incidents: StartIncident - Consente agli utenti di avviare manualmente un incidente utilizzando la console o l'API. Questo crea un nuovo record di incidente da un piano di risposta.
- ssm-incidents: GetResponsePlan - Consente agli utenti di recuperare informazioni su un piano di risposta specifico.
- ssm-incidents: ListResponsePlans - Consente agli utenti di elencare tutti i piani di risposta nel proprio account.
- ssm-incidents: TagResource - Consente di aggiungere tag alle risorse di Incident Manager, inclusi incidenti e piani di risposta.
- ssm-incidents: GetIncidentRecord - Consente agli utenti di recuperare informazioni dettagliate su un incidente specifico.
- ssm-incidents: ListIncidentRecords - Consente agli utenti di elencare tutti gli incidenti nel proprio account.
- ssm-incidents: UpdateIncidentRecord - Consente agli utenti di aggiornare i dettagli di un incidente esistente.
- ssm-contacts: StartEngagement (con condizione) - Consente a Incident Manager di avviare interazioni con i contatti. La condizione garantisce che questo possa essere chiamato solo tramite Incident Manager.
- ssm: CreateOpsItem (con condizione) - Consente a Incident Manager di creare un OpsItem in OpsCenter. La condizione garantisce che questo possa essere chiamato solo tramite Incident Manager.

La chiave aws: CalledViaFirst condition garantisce che determinate autorizzazioni (come`StartEngagement`) possano essere utilizzate solo quando la richiesta arriva tramite il servizio Incident Manager. Questo approccio utilizza FAS anziché ruoli collegati ai servizi, il che impedisce potenziali chiamate tra account che potrebbero comportare rischi per la sicurezza.

Visualizzazione dei dettagli dell'incidente nella console Incident Manager

AWS Systems Manager Incident Manager tiene traccia degli incidenti dal momento in cui vengono rilevati fino alla risoluzione e all'analisi post-incidente. È possibile trovare tutti gli incidenti nella pagina dell'elenco degli incidenti nella console Incident Manager, con collegamenti diretti ai dettagli degli incidenti.

Argomenti

Visualizzazione dell'elenco degli incidenti nella console

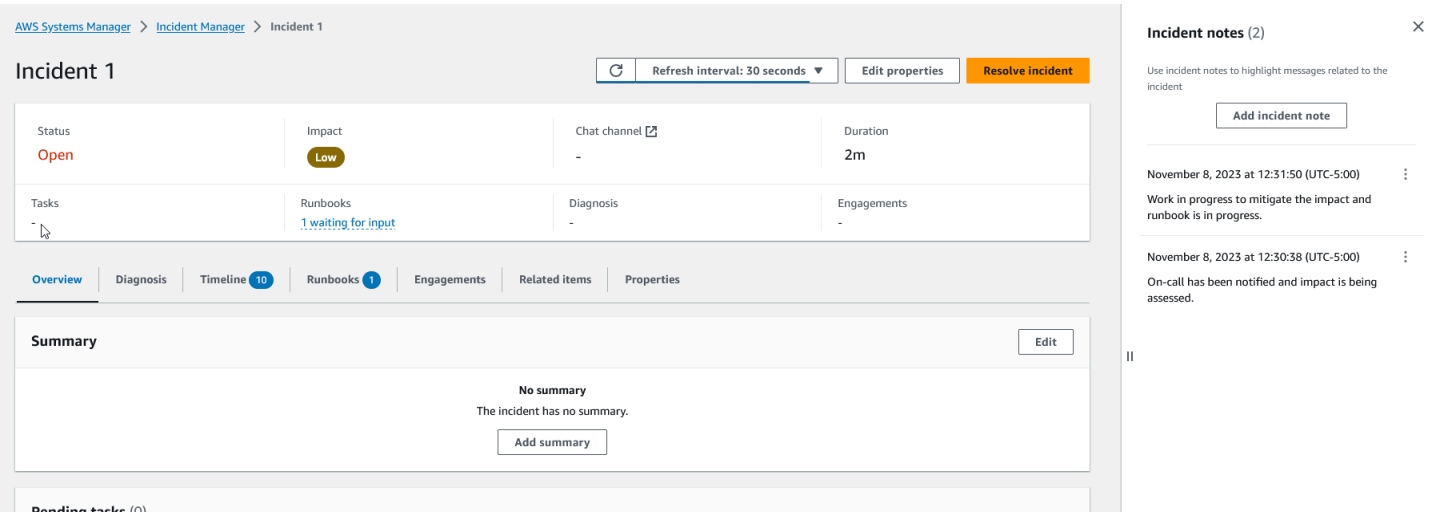
La pagina dell'elenco degli incidenti contiene tre sezioni: Incidenti aperti, Incidenti risolti e Analisi. È possibile tenere traccia manualmente dei nuovi incidenti e creare analisi da questa pagina. Per ulteriori informazioni sul monitoraggio manuale di un incidente, consulta Creazione manuale degli incidenti la sezione Creazione di un incidente di questa guida. Per ulteriori informazioni sull'analisi post-incidente, consulta la Performing a post-incident analysis in Incident Manager sezione di questa guida.

Nei dettagli dell'incidente vengono visualizzati gli incidenti aperti in riquadri con il titolo, l'impatto, la durata e il canale di chat dell'incidente. Dopo aver risolto un incidente, si passa all'elenco Incidenti risolti. Le analisi si trovano nella seconda scheda.

Visualizzazione dei dettagli degli incidenti nella console

La pagina dei dettagli dell'incidente fornisce informazioni dettagliate e strumenti che è possibile utilizzare per gestire un incidente. Da questa pagina, puoi avviare i runbook per mitigare un incidente, aggiungere note sull'incidente, coinvolgere altri risolutori e visualizzare i dettagli dell'incidente come tempistiche, metriche, proprietà e risorse correlate.

Come mostrato nell'immagine seguente, la pagina dei dettagli dell'incidente include diverse sezioni: banner principale, note sull'incidente e sette schede che contengono informazioni e risorse aggiuntive. Per impostazione predefinita, le sezioni del banner principale e delle note sull'incidente vengono visualizzate in tutte le pagine dei dettagli dell'incidente.



Questo argomento spiega gli elementi della pagina dei dettagli dell'incidente e le azioni che è possibile eseguire dalla pagina.

Banner superiore

Il banner superiore di ogni pagina dei dettagli dell'incidente include le seguenti informazioni:

- Stato: lo stato attuale di un incidente può essere Aperto o Risolto.
- Impatto: l'impatto dell'incidente sull'ambiente. Può essere alto, medio e basso. Per modificare l'impatto di un incidente, scegli Modifica proprietà.
- Canale di chat: un collegamento per accedere al canale di chat in cui è possibile visualizzare gli aggiornamenti e le notifiche degli incidenti.
- Durata: il periodo di tempo trascorso prima che un soccorritore risolva l'incidente.
- Runbook: gli stati dei runbook associati a questo incidente. Lo stato può essere in attesa di input, riuscito o non riuscito. Se lo stato di un runbook è in attesa di input, puoi selezionare il runbook per visualizzare i dettagli dell'azione. È possibile selezionare non riuscito per visualizzare i runbook scaduti, non riusciti o annullati.
- Impegni: il numero totale di impegni e lo stato di ogni impegno. Quando crei un coinvolgimento, il relativo stato è Impegnato. Una volta confermato il coinvolgimento, lo stato passa da Impegnato a Riconosciuto. Incident Manager non supporta il riconoscimento degli impegni di terze parti. Tali impegni rimangono nello stato Impegnato.

Puoi modificare il titolo, l'impatto e il canale di chat dell'incidente selezionando Modifica nell'angolo in alto a destra del banner.

Note sull'incidente

Sul lato destro dello schermo viene visualizzata la sezione Note sull'incidente. Con le note, puoi collaborare e comunicare con altri utenti che lavorano su un incidente. È possibile spiegare le mitigazioni applicate, una potenziale causa principale identificata o lo stato attuale dell'incidente. Come best practice, utilizza la sezione Note sull'incidente per pubblicare aggiornamenti sullo stato e le azioni intraprese da te o da altri in merito a un incidente. Se hai bisogno di comunicare con altri risolutori in tempo reale, utilizza il canale di chat disponibile in Incident Manager.

Per aggiungere una nota, scegli il pulsante Aggiungi nota sull'incidente, quindi inserisci la nota. Le note possono contenere aggiornamenti sullo stato dell'incidente o qualsiasi altra informazione pertinente che fornisca visibilità agli altri utenti. Se necessario, puoi anche modificare o eliminare le note sull'incidente.

> **Note**
>
> Qualsiasi utente con l'autorizzazione IAM per eseguire le `ssm-incidents:DeleteTimelineEvent` azioni `ssm-incidents:UpdateTimelineEvent` and può modificare ed eliminare le note. Tuttavia, quando condividi un incidente con un altro account, la politica delle risorse non include l'`ssm-incidents:DeleteTimelineEvent`azione. Ciò impedisce all'utente con cui condividi l'incidente di eliminare la nota. È possibile visualizzare l'audit trail di una nota degli eventi di Incident Manager nella AWS CloudTrail console.

Schede

La pagina dei dettagli dell'incidente ha sette schede, che consentono ai soccorritori di individuare e visualizzare più facilmente le informazioni durante un incidente. Le schede mostrano un contatore nel nome della scheda, che indica il numero di aggiornamenti alla scheda. Per ulteriori informazioni sul contenuto di ogni scheda e sulle azioni disponibili, continua a leggere.

Panoramica

La scheda Panoramica è la pagina di destinazione per i soccorritori. Contiene il riepilogo dell'incidente, un elenco degli eventi cronologici recenti e la fase corrente del runbook.

I soccorritori utilizzano il Summary per aggiornarsi sulle azioni intraprese, sui risultati di eventuali modifiche, sui possibili passaggi successivi e sulle informazioni sull'impatto dell'incidente. Per aggiornare il riepilogo, scegli Modifica nell'angolo in alto a destra della sezione Riepilogo.

> **Important**
>
> Se più risponditori modificano contemporaneamente il campo di riepilogo, il risponditore che invia le modifiche per ultima sovrascrive tutti gli altri input.

La sezione Eventi cronologici recenti contiene una sequenza temporale popolata da Incident Manager con i cinque eventi più recenti. Utilizza questa sezione per comprendere lo stato dell'incidente e cosa è successo di recente. Per visualizzare una cronologia completa, vai alla scheda Cronologia.

La pagina di panoramica mostra anche la fase corrente del runbook. Questo passaggio potrebbe essere un passaggio automatico eseguito nell' AWS ambiente in uso oppure una serie di istruzioni manuali per i risponditori. Per visualizzare il runbook completo, compresi i passaggi precedenti e futuri, scegli la scheda Runbook.

Diagnosi

La scheda Diagnosi contiene informazioni essenziali sulle applicazioni e sui sistemi AWS ospitati, incluse informazioni sulle metriche e, se abilitate, sui risultati.

Lavorare con le metriche

Incident Manager utilizza Amazon CloudWatch per compilare le metriche e i grafici degli allarmi presenti in questa scheda. Per ulteriori informazioni sulle migliori pratiche di gestione degli incidenti per la definizione di allarmi e metriche, consulta Monitoraggio la sezione Pianificazione degli incidenti di questa guida per l'utente.

Per aggiungere metriche

- Scegli Aggiungi nell'angolo in alto a destra di questa scheda.
  - Per aggiungere una metrica da una CloudWatch dashboard esistente, scegli Dalla dashboard esistente. CloudWatch
    a. Scegli una dashboard. Questo aggiunge tutte le metriche e gli allarmi che fanno parte della dashboard scelta.

b. (Facoltativo) Puoi anche selezionare le metriche dalla dashboard per visualizzare metriche specifiche.

- Aggiungi una singola metrica selezionando Da CloudWatch e incollando una fonte di metrica. Per copiare una fonte metrica:

  a. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.

  b. Nel riquadro di navigazione, seleziona Parametri.

  c. Nella scheda Tutte le metriche, inserisci un termine di ricerca nel campo di ricerca, ad esempio il nome di una metrica o il nome di una risorsa, e scegli Invio.

     Ad esempio, se cerchi la `CPUUtilization` metrica, vedrai i namespace e le dimensioni associate a questa metrica.

  d. Scegli uno dei risultati della ricerca per visualizzare le metriche.

  e. Scegli la scheda Fonte e copia la fonte.

I grafici metrici degli allarmi possono essere aggiunti ai dettagli dell'incidente solo tramite il relativo piano di risposta o selezionando Dalla CloudWatch dashboard esistente quando si aggiunge una metrica.

Per rimuovere le metriche, scegli Rimuovi, quindi scegli le metriche che desideri rimuovere dal menu a discesa Metriche fornito.

Visualizzazione dei risultati di e AWS CodeDeployCloudFormation

Dopo aver abilitato Findings e configurato tutti i permessi richiesti, tutti i risultati che potrebbero essere correlati a un incidente specifico vengono allegati all'incidente. I soccorritori possono visualizzare le informazioni su questi risultati nella pagina dei dettagli dell'incidente.

Per visualizzare i risultati di CodeDeploy e CloudFormation

1. Aprire la console Incident Manager.
2. Scegli il nome di un incidente su cui indagare.
3. Nella scheda Diagnosi, nell'area Risultati, confronta gli orari di inizio di ogni risultato segnalato con l'ora di inizio dell'incidente.
4. Per visualizzare ulteriori dettagli su un risultato, nella colonna Riferimento, scegli il link al CloudFormation risultato CodeDeploy o.

Sequenza temporale

Utilizzate la scheda Cronologia per tenere traccia degli eventi che si verificano durante un incidente. Incident Manager compila automaticamente gli eventi cronologici che identificano gli eventi significativi durante l'incidente. I soccorritori possono aggiungere eventi personalizzati in base alle occorrenze rilevate manualmente. Durante l'analisi post-incidente, la scheda Cronologia fornisce informazioni preziose su come prepararsi e rispondere meglio agli incidenti futuri. Per ulteriori informazioni sull'analisi post-incidente, vedere. Performing a post-incident analysis in Incident Manager

Per aggiungere un evento cronologico personalizzato, scegli Aggiungi. Seleziona una data utilizzando il calendario, quindi inserisci un'ora. Tutti gli orari vengono visualizzati nel fuso orario locale. Fornisci una breve descrizione dell'evento che appare nella timeline.

Per modificare un evento personalizzato esistente, seleziona l'evento nella timeline e scegli Modifica. Puoi modificare l'ora, la data e la descrizione degli eventi personalizzati. È possibile modificare solo eventi personalizzati.

Runbook

La scheda Runbook della pagina dei dettagli dell'incidente consente ai soccorritori di visualizzare le fasi del runbook e avviare nuovi runbook.

Per iniziare un nuovo runbook, scegli Start runbook nella sezione Runbook. Usa il campo di ricerca per trovare il runbook che vuoi iniziare. Fornisci tutti i parametri richiesti e la versione del runbook che desideri utilizzare all'avvio del runbook. I runbook avviati durante un incidente dalla scheda Runbooks utilizzano le autorizzazioni dell'account attualmente connesso.

Per accedere a una definizione di runbook in Systems Manager, scegli il titolo del runbook in Runbooks. Per passare all'istanza in esecuzione del runbook in Systems Manager, scegli i dettagli di esecuzione in Dettagli di esecuzione. Queste pagine visualizzano il modello utilizzato per avviare il runbook e i dettagli specifici dell'istanza attualmente in esecuzione del documento di automazione.

La sezione Runbook steps mostra l'elenco dei passaggi eseguiti automaticamente dal runbook selezionato o eseguiti manualmente dai risponditori. I passaggi si espandono man mano che diventano il passaggio corrente, visualizzando le informazioni necessarie per completare il passaggio o i dettagli sulle funzioni del passaggio. I passaggi automatici del runbook vengono risolti al termine dell'automazione. I passaggi manuali richiedono che i risponditori scelgano Passaggio successivo

nella parte inferiore di ogni passaggio. Al termine di un passaggio, l'output del passaggio viene visualizzato in un menu a discesa.

Per annullare l'esecuzione di un runbook, scegli Annulla runbook. Ciò interromperà l'esecuzione del runbook e non completerà gli ulteriori passaggi del runbook.

Impegni

La scheda Interventi dei dettagli dell'incidente favorisce il coinvolgimento dei soccorritori e dei team. Da questa scheda puoi vedere chi è stato coinvolto, chi ha risposto e quali soccorritori verranno coinvolti nell'ambito di un piano di intensificazione. I rispondenti possono coinvolgere altri contatti direttamente da questa scheda. Per ulteriori informazioni sulla creazione di contatti e piani di escalation, consulta le Creazione di un piano di intensificazione per il coinvolgimento dei soccorritori in Incident Manager sezioni Creazione e configurazione dei contatti in Incident Manager e le sezioni di questa guida.

Puoi configurare piani di risposta con contatti e piani di escalation per avviare automaticamente il coinvolgimento all'inizio di un incidente. Per ulteriori informazioni sulla configurazione dei piani di risposta, consulta la Creazione e configurazione dei piani di risposta in Incident Manager sezione di questa guida.

Puoi trovare informazioni su ogni contatto nella tabella. Questa tabella include le seguenti informazioni:

- Nome: collegamenti alla pagina dei dettagli dei contatti che mostra i metodi di contatto e il piano di coinvolgimento.
- Piano di escalation: collegamenti al piano di escalation che ha coinvolto il contatto.
- Fonte del contatto: identifica il servizio che ha contattato questo contatto, ad esempio o. AWS Systems Manager PagerDuty
- Impegnato: mostra quando il piano ha coinvolto un contatto o quando coinvolgere un contatto nell'ambito di un piano di escalation.
- Riconosciuto: indica se il contatto ha confermato il coinvolgimento.

Per confermare un coinvolgimento, il rispondente può eseguire una delle seguenti operazioni:

- Telefonata: inserisci **1** quando richiesto.
- SMS: rispondi al messaggio con il codice fornito o inserisci il codice fornito nella scheda Impegni dell'incidente.

- E-mail: inserisci il codice fornito nella scheda Impegni dell'incidente.

Voci correlate

La scheda Articoli correlati viene utilizzata per raccogliere risorse relative alla mitigazione degli incidenti. Queste risorse possono essere ARNs collegamenti a risorse esterne o file caricati su bucket Amazon S3. La tabella mostra un titolo descrittivo e un ARN, un link o i dettagli del bucket. Prima di utilizzare i bucket S3, consulta le best practice di sicurezza per Amazon S3 nella Amazon S3 User Guide.

Quando si caricano file in un bucket Amazon S3, il controllo delle versioni è abilitato o sospeso su quel bucket. Quando il controllo delle versioni è abilitato nel bucket, i file caricati con lo stesso nome di un file esistente vengono aggiunti come nuova versione del file. Se il controllo delle versioni è sospeso, i file caricati con lo stesso nome di un file esistente sovrascrivono il file esistente. Per ulteriori informazioni sul controllo delle versioni, consulta Using versioning in S3 bucket nella Amazon S3 User Guide.

Quando si rimuove un elemento relativo a un file, il file viene rimosso dall'incidente ma non dal bucket Amazon S3. Per ulteriori informazioni sulla rimozione di oggetti da un bucket Amazon S3, consulta Eliminazione di oggetti Amazon S3 nella Amazon S3 User Guide.

Proprietà

La scheda Proprietà fornisce i seguenti dettagli sull'incidente.

Nella sezione Proprietà dell'incidente, è possibile visualizzare quanto segue:

- Stato: descrive lo stato attuale dell'incidente. L'incidente può essere aperto o risolto.
- Ora di inizio: l'ora in cui l'incidente è stato creato in Incident Manager.
- Ora di risoluzione: l'ora in cui l'incidente è stato risolto in Incident Manager.
- Amazon Resource Name (ARN): l'ARN dell'incidente. Usa l'ARN quando fai riferimento all'incidente dalla chat o con i comandi AWS Command Line Interface ()AWS CLI.
- Piano di risposta: identifica il piano di risposta per l'incidente selezionato. La scelta del piano di risposta apre la pagina dei dettagli del piano di risposta.
- Genitore OpsItem: identifica il OpsItem creato come genitore dell'incidente. Un genitore OpsItem può avere più incidenti correlati e azioni successive. Selezionando il genitore OpsItem si apre la pagina dei OpsItems dettagli in. OpsCenter

- Analisi: identifica l'analisi creata da questo incidente. Crea un'analisi a partire da un incidente risolto per migliorare il processo di risposta all'incidente. Scegli l'analisi per aprire la pagina dei dettagli dell'analisi.
- Proprietario: l'account in cui è stato creato l'incidente.

Nella sezione Tag, puoi visualizzare e modificare le chiavi e i valori dei tag associati al record dell'incidente. Per ulteriori informazioni sui tag in Incident Manager, vedereEtichettatura delle risorse in Incident Manager.

Performing a post-incident analysis in Incident Manager

L'analisi post-incidente ti guida nell'identificazione dei miglioramenti nella risposta agli incidenti, compresi i tempi di rilevamento e mitigazione. Un'analisi può anche aiutarti a comprendere la causa principale degli incidenti. Incident Manager crea azioni consigliate per migliorare la risposta agli incidenti.

Vantaggi di un'analisi post-incidente

- Migliora la risposta agli incidenti
- Comprendi la causa principale del problema
- Affrontate le cause alla radice con azioni realizzabili
- Analizza l'impatto degli incidenti
- Acquisisci e condividi le conoscenze all'interno di un'organizzazione

Per cosa non usare un'analisi

Un'analisi è irreprensibile e non chiama le persone per nome.

«Indipendentemente da ciò che scopriamo, comprendiamo e crediamo fermamente che tutti abbiano fatto il miglior lavoro possibile, in base a ciò che conoscevano all'epoca, alle loro capacità e abilità, alle risorse disponibili e alla situazione in cui si trovavano». - Norm Kerth, Project Retrospectives: un manuale per la revisione in team

Dettagli dell'analisi

La pagina dei dettagli dell'analisi guida l'utente nella raccolta di informazioni, nella valutazione dei miglioramenti e nella creazione di azioni. La pagina dei dettagli dell'analisi è simile ai dettagli dell'incidente con alcune differenze chiave come metriche storiche, cronologia modificabile e domande per migliorare gli incidenti futuri.

Panoramica

La panoramica è un riepilogo dell'incidente. Questo riepilogo include il contesto, ciò che è accaduto, il motivo per cui è accaduto, come è stato mitigato, la durata e le azioni chiave per evitare che

l'incidente si ripeta. La panoramica è di alto livello. Esplorerai maggiori dettagli nella scheda Domande dell'analisi.

Metriche

Utilizza la scheda Metriche per visualizzare le metriche chiave della tua applicazione per tutta la durata dell'incidente. Qui puoi aggiungere grafici metrici con una o più metriche rappresentate nello stesso grafico. Le metriche utilizzate durante un incidente vengono inserite automaticamente in questa scheda. Ti consigliamo di aggiungere una descrizione, un titolo e delle annotazioni dei punti temporali chiave durante l'incidente.

Alcuni punti temporali chiave che puoi prendere in considerazione quando analizzi un grafico metrico:

- Modifica della distribuzione
- Modifica della configurazione
- Ora di inizio dell'incidente
- Ora della sveglia
- Momento del fidanzamento
- Ora di inizio della mitigazione
- Ora di risoluzione dell'incidente

Limitazioni

- CloudWatch gli allarmi e le espressioni metriche non vengono importati da un incidente.
- Le metriche che si trovano in una regione non supportata da Incident Manager non vengono importate dall'incidente.
- Le metriche negli account delle applicazioni richiedono la configurazione `CloudWatch-CrossAccountSharingRole` prima della creazione dell'analisi. Per ulteriori informazioni sul ruolo, consulta la CloudWatch console Cross-Account Cross-Region nella guida per l' CloudWatch utente.

Sequenza temporale

Descrivi i momenti chiave della sequenza temporale mentre approfondisci la comprensione dell'incidente. La cronologia degli incidenti viene compilata automaticamente in questa scheda. Puoi

eliminare i punti temporali che non sono pertinenti all'analisi. Puoi anche aggiungere e modificare i punti temporali per descrivere con maggiore precisione l'incidente e il suo impatto.

Utilizza la scheda Cronologia per rispondere alle domande che trovi nella scheda Domande sulla risposta all'incidente.

Questions

Utilizza le domande di Incident Manager per migliorare i tempi di risoluzione degli incidenti nell'applicazione e ridurre il verificarsi di incidenti. Man mano che rispondi alle domande, aggiorna le schede Metriche e Cronologia per verificarne la precisione. Le domande si concentrano su questi aspetti chiave della risposta agli incidenti:

- Rilevamento: potresti ridurre i tempi di rilevamento? Sono presenti aggiornamenti alle metriche e agli allarmi che permettono di rilevare l'incidente prima?
- Diagnosi: è possibile ridurre i tempi di diagnosi? Sono presenti aggiornamenti ai tuoi piani di risposta o di escalation che potrebbero coinvolgere prima i team di risposta corretti?
- Attenuazione: è possibile ridurre i tempi di mitigazione? Esistono passaggi del runbook che potresti aggiungere o migliorare?
- Prevenzione: è possibile evitare che si verifichino incidenti futuri? Per scoprire le cause principali di un incidente, Amazon utilizza l'approccio 5-Whys nell'indagine dei problemi.

Operazioni

Incident Manager crea delle azioni consigliate da esaminare man mano che rispondi alle domande. È possibile scegliere di accettare e completare queste azioni da questa scheda oppure ignorarle. È possibile esaminare le azioni ignorate selezionando Azioni ignorate. Le azioni sono un tipo di OpsItem azioni collegate all'analisi e all'incidente in. OpsCenter

Lista di controllo

Prima di chiudere un'analisi, utilizza la lista di controllo per esaminare le azioni che un risponditore deve intraprendere. Man mano che i risponditori completano le azioni nella lista di controllo, l'icona accanto all'azione cambia da ellisse a segno di spunta, a indicare che l'azione è completa. Se non hai completato gli elementi della lista di controllo, Incident Manager visualizza un messaggio per confermare che il risponditore desidera chiudere l'analisi senza completarla.

Modelli di analisi

Un modello di analisi fornisce una serie di domande che approfondiscono la causa principale degli incidenti. È possibile utilizzare le risposte a queste domande per migliorare le prestazioni delle applicazioni e la risposta agli incidenti.

AWS modello standard

Incident Manager fornisce un modello standard di domande basato sulle migliori pratiche di risposta agli AWS incidenti e analisi dei problemi, intitolato`AWSIncidents-PostIncidentAnalysisTemplate`.

Crea un modello di analisi

Ti invitiamo a utilizzare il `AWSIncidents-PostIncidentAnalysisTemplate` modello predefinito e ad aggiungere ulteriori domande o sezioni appropriate ai tuoi casi d'uso. Crea modelli di analisi basati sul modello predefinito Utilizza questo modello come punto di partenza per creare modelli di analisi nel tuo account di gestione. È quindi possibile duplicare i modelli di analisi in ciascuna regione in cui è stato abilitato Incident Manager.

Crea un modello di analisi

1. Richiama l'`GetDocument`azione e utilizza il relativo `Name` parametro per il download`AWSIncidents-PostIncidentAnalysisTemplate`. Per ulteriori informazioni sulla `GetDocument` sintassi, vedere Systems Manager API Reference.
2. Il contenuto della risposta contiene gli elementi costitutivi JSON per l'analisi. Usa gli elementi costitutivi delle domande per inserire domande aggiuntive nell'analisi. Ti consigliamo di aggiungere domande o sezioni nella `Incident questions` sezione.
3. Per creare il nuovo modello, utilizza l'`CreateDocument`operazione con il JSON aggiornato del passaggio precedente. Devi includere quanto segue, *`Analysis_Template_Name`* dov'è il nome del tuo modello,

   - `DocumentFormat: "JSON"`
   - `DocumentType: "ProblemAnalysisTemplate"`
   - `Name: "`*`Analysis_Template_Name`*`"`

Crea un'analisi

1. Per creare un'analisi, scegli Crea analisi dalla pagina dei dettagli dell'incidente di un incidente chiuso.
2. Scegli il modello di analisi da cui creare l'analisi e inserisci un nome descrittivo dell'analisi.
3. Scegli Create (Crea) .

Stampa un'analisi degli incidenti formattata

È possibile generare una copia di un'analisi completa o incompleta formattata per la stampa. È inoltre possibile salvare questa copia come PDF. È possibile stampare un'analisi alla volta. La stampa in batch di più analisi non è attualmente supportata.

Per stampare un'analisi formattata

1. Aprire la console Incident Manager.
2. Scegli la scheda Analisi.
3. Scegliete il titolo dell'analisi che desiderate stampare.
4. Nell'angolo in alto a destra della pagina dei dettagli dell'analisi, scegli Stampa.
5. Nella finestra di dialogo Print Incident Analysis, deselezionate le sezioni dell'analisi che non desiderate includere nella versione stampata. Per impostazione predefinita, sono selezionate tutte le sezioni.
6. Scegliete Stampa per aprire i controlli di stampa locali del dispositivo.
7. Scegli la destinazione o il formato di stampa. È possibile scegliere una stampante locale o di rete oppure salvare l'analisi in un PDF. Apportate eventuali modifiche, se desiderate, alle opzioni di stampa rimanenti, quindi scegliete Stampa.

> **Note**
>
> I controlli di stampa locali si riferiscono all'interfaccia utente fornita dal browser Web e dal dispositivo.
> Le destinazioni di stampa sono quelle configurate e accessibili dal dispositivo.

Tutorial di Incident Manager

Questi tutorial AWS di Systems Manager Incident Manager ti aiutano a creare un sistema di gestione degli incidenti più robusto. Questi tutorial coprono le attività più comuni che si verificano durante un incidente o supportano la risposta agli incidenti.

Argomenti

Tutorial: Utilizzo dei runbook di Systems Manager Automation con Incident Manager

Puoi utilizzare i runbook di AWS Systems Manager automazione per semplificare le attività comuni di manutenzione, distribuzione e riparazione dei servizi. AWS In questo tutorial, creerai un runbook personalizzato per automatizzare una risposta agli incidenti in Incident Manager. Lo scenario di questo tutorial prevede un CloudWatch allarme Amazon assegnato a una EC2 metrica Amazon. Quando l'istanza entra in uno stato che attiva l'allarme, Incident Manager esegue automaticamente le seguenti attività:

1. Crea un incidente in Incident Manager.
2. Avvia un runbook che tenta di risolvere il problema.
3. Pubblica i risultati del runbook nella pagina dei dettagli dell'incidente in Incident Manager.

Il processo descritto in questo tutorial può essere utilizzato anche con EventBridge eventi Amazon e altri tipi di AWS risorse. Automatizzando la risposta correttiva ad allarmi ed eventi, puoi ridurre l'impatto di un incidente sulla tua organizzazione e sulle sue risorse.

Questo tutorial descrive come modificare un CloudWatch allarme assegnato a un' EC2 istanza Amazon per un piano di risposta di Incident Manager. Se non hai configurato un allarme, un'istanza o un piano di risposta, ti consigliamo di configurare tali risorse prima di iniziare. Per ulteriori informazioni, consulta i seguenti argomenti:

- Utilizzo degli CloudWatch allarmi Amazon nella Guida per l' CloudWatch utente di Amazon
- EC2 Istanze Amazon nella Amazon EC2 User Guide

- EC2Istanze Amazon nella Amazon EC2 User Guide
- Creazione e configurazione dei piani di risposta in Incident Manager

> **Important**
>
> Creando AWS risorse e utilizzando le fasi di automazione del runbook, dovrai sostenere dei costi. Per ulteriori informazioni, consultare Prezzi di AWS.

Argomenti

Attività 1: creazione del runbook

Utilizzare la procedura seguente per creare un runbook nella console Systems Manager. Quando viene richiamato da un incidente di Incident Manager, il runbook riavvia un' EC2 istanza Amazon e aggiorna l'incidente con informazioni sull'esecuzione del runbook. Prima di iniziare, verifica di disporre dell'autorizzazione per creare un runbook. Per ulteriori informazioni, consulta Setting up Automation nella Guida per l'utente di AWS Systems Manager .

> **Important**
>
> Esamina i seguenti dettagli importanti sulla creazione del runbook di questo tutorial:
>
> - Il runbook è destinato a un incidente creato da una fonte di CloudWatch allarme. Se si utilizza questo runbook per altri tipi di incidenti, ad esempio incidenti creati manualmente, l'evento della sequenza temporale nel primo passaggio del runbook non verrà trovato e il sistema restituirà un errore.
> - Il runbook richiede che l'allarme includa una dimensione chiamata CloudWatch . `InstanceId` Gli allarmi per le metriche delle EC2 istanze Amazon hanno questa dimensione. Se utilizzi questo runbook con altre metriche (o con altre fonti di incidenti,

ad esempio EventBridge), devi modificare il `JsonDecode2` passaggio in modo che corrisponda ai dati acquisiti nel tuo scenario.

- Il runbook tenta di risolvere il problema che ha attivato l'allarme riavviando l'istanza Amazon. EC2 In caso di incidente reale, potresti non voler riavviare l'istanza. Aggiorna il runbook con le azioni correttive specifiche che desideri che il sistema intraprenda.

Per ulteriori informazioni sulla creazione di runbook, consulta Working with runbook nella Guida per l'utente.AWS Systems Manager

Per creare un runbook

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, scegli Documenti.
3. Scegli Automazione.
4. Per Nome, inserisci un nome descrittivo per il runbook, ad esempio. **`IncidentResponseRunbook`**
5. Scegliere la scheda Editor, quindi Edit (Modifica).
6. Incolla il contenuto seguente nell'editor:

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
```

```
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
```

```
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. Scegliere Create automation (Crea automazione).

Attività 2: creazione di un ruolo IAM

Usa il seguente tutorial per creare un ruolo AWS Identity and Access Management (IAM) che dia a Incident Manager il permesso di avviare un runbook specificato in un piano di risposta. Il runbook di questo tutorial riavvia un'istanza Amazon EC2 . Specificherai questo ruolo IAM nella prossima attività quando collegherai il runbook al tuo piano di risposta.

Crea un ruolo IAM che avvii un runbook da un piano di risposta

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. In Tipo di entità affidabile, verifica che il AWS servizio sia selezionato.
4. In Caso d'uso, nel campo Casi d'uso per altri AWS servizi, immettere**`Incident Manager`**.
5. Scegli Incident Manager, quindi scegli Avanti.
6. Nella pagina Aggiungi autorizzazioni, scegli Crea politica. L'editor delle autorizzazioni si aprirà in una nuova finestra o scheda del browser.

7. Nell'editor, scegli la scheda JSON.
8. Copia e incolla la seguente politica di autorizzazione nell'editor JSON. Sostituisci *account_ID* con l'ID dell' Account AWS .

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:111122223333:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-
RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
```

```
            ]
        }
    ]
}
```

9. Scegli Successivo: Tag.
10. (Facoltativo) Se necessario, aggiungi dei tag alla tua policy.
11. Scegli Prossimo: Rivedi.
12. Nel campo Nome, inserisci un nome che ti aiuti a identificare il ruolo utilizzato per questo tutorial.
13. (Facoltativo) Inserisci una descrizione nel campo Descrizione.
14. Scegli Crea policy.
15. Torna alla finestra o alla scheda del browser relativa al ruolo che stai creando. Viene visualizzata la pagina Aggiungi autorizzazioni.
16. Scegli il pulsante di aggiornamento (situato accanto al pulsante Crea politica), quindi inserisci il nome della politica di autorizzazione che hai creato nella casella del filtro.
17. Scegli la politica di autorizzazione che hai creato, quindi scegli Avanti.
18. Nella pagina Nome, rivedi e crea, in Nome ruolo, inserisci un nome che ti aiuti a identificare il ruolo utilizzato per questo tutorial.
19. (Facoltativo) Inserisci una descrizione nel campo Descrizione.
20. Esamina i dettagli del ruolo, aggiungi i tag se necessario e scegli Crea ruolo.

Attività 3: collegare il runbook al piano di risposta

Collegando il runbook al piano di risposta di Incident Manager, garantisci un processo di mitigazione coerente, ripetibile e tempestivo. Il runbook funge anche da punto di partenza per i resolver per determinare la loro prossima linea d'azione.

Per assegnare il runbook al piano di risposta

1. Apri la console Incident Manager.
2. Scegli i piani di risposta.
3. Per Piano di risposta, scegli un piano di risposta esistente e scegli Modifica. Se non disponi di un piano di risposta esistente, scegli Crea piano di risposta per creare un nuovo piano di risposta.

   Completare i seguenti campi:

a. Nella sezione Runbook, scegli Seleziona runbook esistente.
b. Per Owner, verifica che l'opzione Owned by me sia selezionata.
c. Per Runbook, scegli il runbook in cui hai creato. Attività 1: creazione del runbook
d. Per Versione, scegli Predefinito al momento dell'esecuzione.
e. Nella sezione Ingressi, per il IncidentRecordArnparametro, selezionate Incident ARN.
f. Nella sezione Autorizzazioni di esecuzione, scegli il ruolo IAM in cui hai creato. Attività 2: creazione di un ruolo IAM

4. Salvare le modifiche.

Attività 4: assegnazione di un CloudWatch allarme al piano di risposta

Utilizza la seguente procedura per assegnare un CloudWatch allarme per un' EC2 istanza Amazon al tuo piano di risposta.

Per assegnare un CloudWatch allarme al tuo piano di risposta

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel pannello di navigazione, in Allarmi, scegli Tutti gli allarmi.
3. Scegli un allarme per un' EC2 istanza Amazon che desideri collegare al tuo piano di risposta.
4. Seleziona Azioni, quindi scegli Modifica. Verifica che la metrica abbia una dimensione chiamata`InstanceId`.
5. Scegli Next (Successivo).
6. Per la procedura guidata di configurazione delle azioni, selezionare Aggiungi azione Systems Manager.
7. Scegli Crea incidente.
8. Scegli il piano di risposta in cui hai creatoAttività 3: collegare il runbook al piano di risposta.
9. Seleziona Update Alarm (Aggiorna allarme).

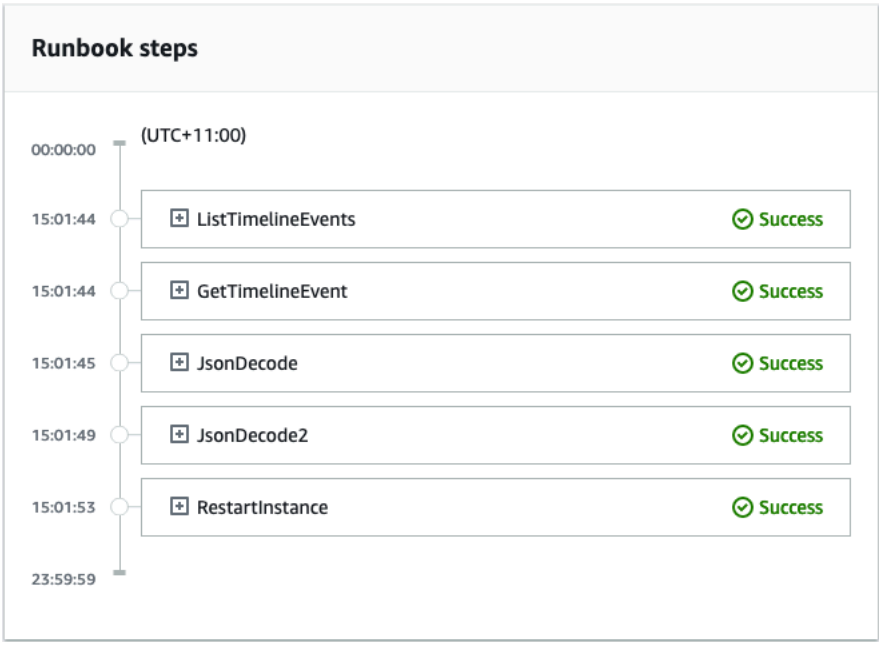
Attività 5: verifica dei risultati

Per verificare che l' CloudWatch allarme crei un incidente e quindi elabori il runbook specificato nel piano di risposta, è necessario attivare l'allarme. Dopo aver attivato l'allarme e aver terminato l'elaborazione del runbook, è possibile verificare i risultati del runbook utilizzando la procedura

seguente. Per informazioni sull'attivazione di un allarme, vedere set-alarm-statenel Command Reference.AWS CLI

1. Aprire la console Incident Manager.
2. Scegli l'incidente creato dall' CloudWatch allarme.
3. Scegli la scheda Runbooks.
4. Visualizza le azioni eseguite sulla tua EC2 istanza Amazon nella sezione relativa ai passaggi del Runbook.

   L'immagine seguente mostra come i passaggi eseguiti dal runbook creato in questo tutorial vengono riportati nella console. Ogni passaggio è elencato con un timestamp e un messaggio di stato.



   Per visualizzare tutti i dettagli dell' CloudWatch allarme, espandi il passaggio JsonDecode2, quindi espandi Output.

> **Important**
>
> È necessario eliminare tutte le modifiche alle risorse implementate durante questo tutorial che non si desidera conservare. Ciò include le modifiche alle risorse di Incident Manager, come i piani delle risorse e gli incidenti, le modifiche agli CloudWatch allarmi e il ruolo IAM che hai creato per questo tutorial.

Tutorial: Gestione degli incidenti di sicurezza in Incident Manager

Puoi utilizzare AWS Security Hub CSPM Amazon EventBridge e Incident Manager insieme per identificare e gestire gli incidenti di sicurezza nelle tue applicazioni AWS ospitate. Questo tutorial illustra la configurazione di una EventBridge regola che crea un incidente in base ai risultati inviati automaticamente da Security Hub.

> **Note**
>
> Questo tutorial utilizza EventBridge Security Hub. L'utilizzo di questi servizi potrebbe comportare dei costi.

Prerequisiti

- Configura Security Hub. Per ulteriori informazioni, consulta Configurazione AWS Security Hub CSPM.
- Crea o aggiorna i risultati in Security Hub. Per ulteriori informazioni, consulta Findings in AWS Security Hub CSPM.
- Configura un piano di risposta che Incident Manager utilizzerà come modello durante la creazione dell'incidente di sicurezza. Per ulteriori informazioni, consulta Preparazione agli incidenti in Incident Manager.

Per questo tutorial, utilizziamo uno schema predefinito per creare la EventBridge regola. Per creare la regola utilizzando un modello personalizzato, vedi Utilizzo di un modello personalizzato per creare la regola nella guida per l' AWS Security Hub CSPM utente.

Crea una EventBridge regola

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).
4. Immettere il Name (Nome) e la Description (Descrizione) della regola.

   Una regola non può avere lo stesso nome di un'altra regola nella stessa regione e sullo stesso router di eventi.
5. Per Event bus (Bus di eventi), scegli default.

6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Scegli Next (Successivo).
8. Per Event source, scegli AWS eventi o eventi EventBridge partner.
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS .
11. Per l'AWS assistenza, scegli Security Hub.
12. Per Tipo di evento, scegliete Security Hub Findings - Importato.
13. Per impostazione predefinita, EventBridge configura il modello di evento senza alcun valore di filtro. Per ogni attributo, è selezionata *`attribute name`* l'opzione Qualsiasi. Aggiorna questi filtri per creare incidenti in base ai risultati di sicurezza che hanno il maggiore impatto sull'ambiente.
14. Fare clic su Avanti.
15. Per Target types (Tipi di destinazione), scegli AWS service (Servizio).
16. Per Seleziona un obiettivo, scegli il piano di risposta di Incident Manager.
17. Per il piano di risposta, scegli un piano di risposta da utilizzare come modello per gli incidenti creati.
18. EventBridge può creare il ruolo IAM necessario per l'esecuzione della regola.
    - Per creare automaticamente un ruolo IAM, scegli Crea un nuovo ruolo per la risorsa specifica.
    - Per utilizzare un ruolo IAM già esistente nel tuo account, scegli Usa il ruolo esistente.
19. (Facoltativo) Inserire uno o più tag per la regola.
20. Scegli Next (Successivo).
21. Rivedi i dettagli della regola e scegli Create rule (Crea regola).

Ora che hai creato questa EventBridge regola, i risultati di sicurezza che corrispondono ai valori degli attributi che hai definito creeranno incidenti in Incident Manager. È possibile valutare, gestire, monitorare e creare analisi post-incidente a partire da questi incidenti.

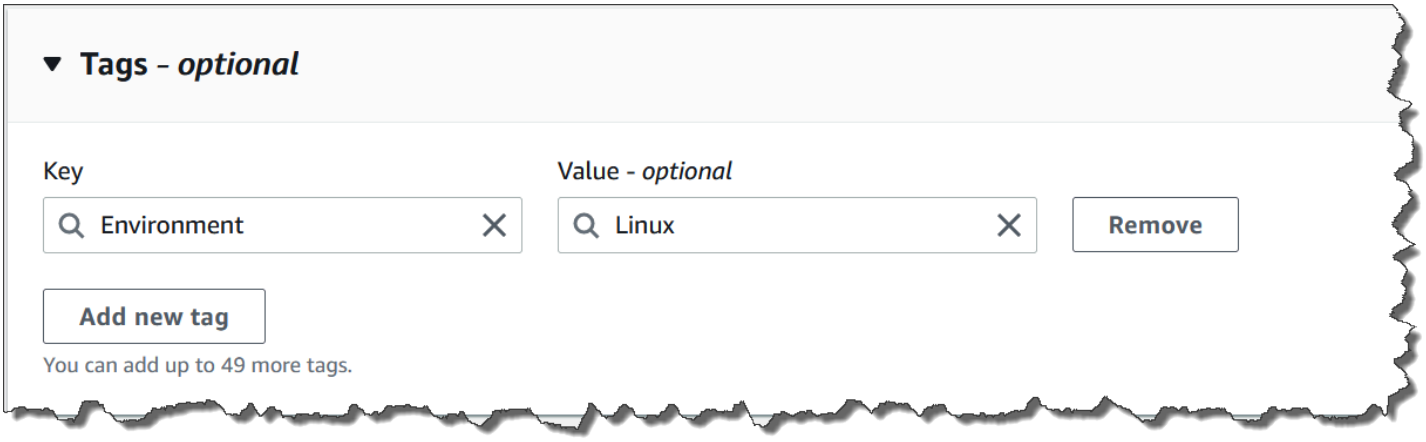
Etichettatura delle risorse in Incident Manager

I tag sono metadati opzionali che è possibile assegnare alle risorse di Incident Manager nel modo Regioni AWS specificato nel set di replica. È possibile assegnare tag ai piani di risposta, ai record degli incidenti e ai contatti. È inoltre possibile aggiungere tag agli orari e alle rotazioni delle chiamate. È inoltre possibile aggiungere tag al set di replica stesso. I tag consentono di classificare e controllare l'accesso a queste risorse in diversi modi. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili. Ti consigliamo di creare un set di chiavi di tag che soddisfi le tue esigenze per ogni tipo di risorsa Incident Manager. L'utilizzo di un set coerente di tag key semplifica la gestione di queste risorse e la gestione dell'accesso ad esse. Puoi cercare e filtrare le risorse in base ai tag. Per ulteriori informazioni sul controllo dell'accesso alle risorse tramite tag, consulta Controlling access to AWS resources using tags nella IAM User Guide.

Puoi specificare i tag nella sezione Incidente predefinito quando crei un piano di risposta. Questi tag vengono applicati al record dell'incidente quando viene creato un incidente utilizzando il piano di risposta.

> **Note**
>
> I tag non hanno alcun significato semantico. Vengono interpretati rigorosamente come una stringa di caratteri.

È possibile aggiungere o rimuovere tag utilizzando la console Incident Manager. La schermata seguente mostra l'area Tag di una pagina della console, con campi per aggiungere chiavi e valori dei tag e pulsanti per aggiungere e rimuovere tag.



Per utilizzare i tag a livello di codice, utilizzate le seguenti azioni API:

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> I tag applicati ai piani di risposta, ai record degli incidenti, ai contatti, agli orari e alle rotazioni delle chiamate e ai set di replica possono essere visualizzati e modificati solo dall'account del proprietario della risorsa.

Sicurezza in Strumento di gestione degli incidenti AWS Systems Manager

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili Strumento di gestione degli incidenti AWS Systems Manager, consulta AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Incident Manager. I seguenti argomenti mostrano come configurare Incident Manager per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere le tue risorse di Incident Manager.

Argomenti

- Analisi della configurazione e della vulnerabilità in Incident Manager
- Le migliori pratiche di sicurezza in Strumento di gestione degli incidenti AWS Systems Manager

Protezione dei dati in Incident Manager

Il modello di responsabilità AWS condivisa di si applica alla protezione dei dati in Strumento di gestione degli incidenti AWS Systems Manager. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò

include quando si lavora con Incident Manager o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Per impostazione predefinita, Incident Manager crittografa i dati in transito utilizzando SSL/TLS.

Crittografia dei dati

Incident Manager utilizza le chiavi AWS Key Management Service (AWS KMS) per crittografare le risorse di Incident Manager. Per ulteriori informazioni in merito AWS KMS, consulta la Guida per gli AWS KMS sviluppatori. AWS KMS combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Incident Manager crittografa i dati utilizzando la chiave specificata e crittografa i metadati utilizzando una chiave proprietaria. AWS Per utilizzare Incident Manager, è necessario configurare il set di replica, che include l'impostazione della crittografia. Incident Manager richiede la crittografia dei dati per l'uso.

È possibile utilizzare una chiave AWS proprietaria per crittografare il set di replica oppure è possibile utilizzare la chiave gestita dal cliente creata AWS KMS per crittografare le regioni del set di replica. Incident Manager supporta solo AWS KMS chiavi di crittografia simmetriche per crittografare i dati creati all'interno. AWS KMS Incident Manager non supporta AWS KMS chiavi con materiale chiave importato, archivi di chiavi personalizzati, codice di autenticazione dei messaggi basato su Hash (HMAC) o altri tipi di chiavi. Se si utilizzano chiavi gestite dal cliente, si utilizza la AWS KMS console o AWS KMS APIs per creare centralmente le chiavi gestite dal cliente e definire le politiche chiave che controllano il modo in cui Incident Manager può utilizzare le chiavi gestite dal cliente. Quando si utilizza una chiave gestita dal cliente per la crittografia con Incident Manager, la chiave gestita dal AWS KMS cliente deve trovarsi nella stessa regione delle risorse. Per ulteriori informazioni sulla configurazione della crittografia dei dati in Incident Manager, consultaPreparati alla procedura guidata.

Sono previsti costi aggiuntivi per l'utilizzo delle chiavi gestite dal AWS KMS cliente. Per ulteriori informazioni, consulta AWS KMS i concetti - Chiavi KMS nella Guida per gli AWS Key Management Service sviluppatori e AWS KMS i prezzi.

> **Important**
>
> Se utilizzate una AWS KMS key (chiave KMS) per crittografare il set di repliche e i dati di Incident Manager, ma in seguito decidete di eliminare il set di repliche, assicuratevi di eliminare il set di repliche prima di disabilitare o eliminare la chiave KMS.

Per consentire a Incident Manager di utilizzare la chiave gestita dal cliente per crittografare i dati, è necessario aggiungere le seguenti istruzioni sulla politica alla politica chiave della chiave gestita dal cliente. Per ulteriori informazioni sulla configurazione e la modifica della politica chiave nel tuo account, consulta Using key policy AWS KMS nella AWS Key Management Service Developer Guide. La politica fornisce le seguenti autorizzazioni:

- Consente a Incident Manager di eseguire operazioni di sola lettura per trovare Incident Manager nel tuo account. AWS KMS key
- Consente a Incident Manager di utilizzare la chiave KMS per creare sovvenzioni e descrivere la chiave, ma solo quando agisce per conto dei responsabili dell'account che dispongono del permesso di utilizzare Incident Manager. Se i responsabili specificati nell'informativa sulla politica non sono autorizzati a utilizzare le chiavi KMS e a utilizzare Incident Manager, la chiamata ha esito negativo, anche quando proviene dal servizio Incident Manager.

```
{
"Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
},
"Action": [
  "kms:CreateGrant",
  "kms:DescribeKey"
],
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:ViaService": [
      "ssm-incidents.us-east-2.amazonaws.com",
      "ssm-contacts.us-east-2.amazonaws.com"
    ]
  }
```

```
        }
      }
```

Sostituisci il `Principal` valore con il principale IAM che ha creato il set di replica.

Incident Manager utilizza un contesto di crittografia in tutte le richieste AWS KMS di operazioni crittografiche. È possibile utilizzare questo contesto di crittografia per identificare gli eventi di CloudTrail registro in cui Incident Manager utilizza le chiavi KMS. Incident Manager utilizza il seguente contesto di crittografia:

- `contactArn=`*`ARN of the contact or escalation plan`*

Identity and Access Management per Strumento di gestione degli incidenti AWS Systems Manager

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Incident Manager. IAM è un Servizio AWS software che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come Strumento di gestione degli incidenti AWS Systems Manager funziona con IAM
- Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager
- Esempi di policy basate sulle risorse per Strumento di gestione degli incidenti AWS Systems Manager
- Prevenzione intersettoriale confusa in Incident Manager
- Utilizzo di ruoli collegati ai servizi per Incident Manager
- AWS politiche gestite per Strumento di gestione degli incidenti AWS Systems Manager

- Risoluzione dei problemi di Strumento di gestione degli incidenti AWS Systems Manager identità e accesso

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (vedi Risoluzione dei problemi di Strumento di gestione degli incidenti AWS Systems Manager identità e accesso)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (vedi Come Strumento di gestione degli incidenti AWS Systems Manager funziona con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (vedi Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per maggiori informazioni sull'accesso, consultare la sezione Come accedere a Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali come utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente IAM.

I ruoli IAM sono utili per l'accesso federato degli utenti, le autorizzazioni utente IAM temporanee, l'accesso tra account, l'accesso tra servizi e le applicazioni in esecuzione su Amazon. EC2 Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e collegandole a identità o risorse. AWS Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste

politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate sull'identità possono essere policy in linea (incorporate direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consultare Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: impostano il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Le policy di sessione sono policy avanzate che si passano come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come Strumento di gestione degli incidenti AWS Systems Manager funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a Incident Manager, scopri quali funzionalità IAM sono disponibili per l'uso con Incident Manager.

Funzionalità IAM che puoi utilizzare con Strumento di gestione degli incidenti AWS Systems Manager

Funzionalità IAM	Supporto per Incident Manager
Policy basate sull'identità	Sì
Policy basate su risorse	Sì
Operazioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	Supporto per Incident Manager
Chiavi di condizione delle policy	No
ACLs	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Incident Manager e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Incident Manager non supporta politiche che negano l'accesso alle risorse condivise. AWS RAM

Politiche basate sull'identità per Incident Manager

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di policy basate sull'identità per Incident Manager

Per visualizzare esempi di politiche basate sull'identità di Incident Manager, vedere. Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager

Politiche basate sulle risorse all'interno di Incident Manager

Supporta le policy basate sulle risorse: sì

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli di IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Il servizio Incident Manager supporta solo due tipi di policy basate sulle risorse richiamate utilizzando la AWS RAM console o l' PutResourcePolicy azione, allegata a un piano di risposta o a un contatto. Questa politica definisce quali responsabili possono eseguire azioni sui piani di risposta, sui contatti, sui piani di escalation e sugli incidenti. Incident Manager utilizza politiche basate sulle risorse per condividere le risorse tra gli account.

Incident Manager non supporta politiche che negano l'accesso alle risorse condivise. AWS RAM

Per informazioni su come allegare una politica basata sulle risorse a un piano di risposta o a un contatto, consulta. Gestione degli incidenti in tutte Account AWS le regioni in Incident Manager

Esempi di policy basate sulle risorse all'interno di Incident Manager

Per visualizzare esempi di politiche basate sulle risorse di Incident Manager, vedere. Esempi di policy basate sulle risorse per Strumento di gestione degli incidenti AWS Systems Manager

Azioni politiche per Incident Manager

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Incident Manager, vedere Azioni definite da Strumento di gestione degli incidenti AWS Systems Manager nel Service Authorization Reference.

Le azioni politiche in Incident Manager utilizzano i seguenti prefissi prima dell'azione:

```
ssm-incidents
ssm-contacts
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Get`, includi la seguente azione:

```
"Action": "ssm-incidents:Get*"
```

Per visualizzare esempi di politiche basate sull'identità di Incident Manager, vedere. Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager

Incident Manager utilizza azioni in due diversi namespace, ssm-incidents e ssm-contacts. Quando crei le politiche per Incident Manager, assicurati di utilizzare lo spazio dei nomi corretto per l'azione. SSM-Incidents viene utilizzato per il piano di risposta e le azioni relative agli incidenti. SSM-Contacts viene utilizzato per azioni relative ai contatti e al coinvolgimento dei contatti. Ad esempio:

- `ssm-contacts:GetContact`
- `ssm-incidents:GetResponsePlan`

Risorse politiche per Incident Manager

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, utilizzare un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di Incident Manager e relativi ARNs, vedere Risorse definite da Strumento di gestione degli incidenti AWS Systems Manager nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da Strumento di gestione degli incidenti AWS Systems Manager.

Per visualizzare esempi di politiche basate sull'identità di Incident Manager, vedere. Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager

Le risorse di Incident Manager vengono utilizzate per creare incidenti, collaborare nei canali di chat, risolvere incidenti e coinvolgere i soccorritori. Se un utente ha accesso a un piano di risposta, ha accesso a tutti gli incidenti da esso creati. Se un utente ha accesso a un contatto o a un piano di escalation, può coinvolgere il contatto o i contatti nel piano di escalation.

Chiavi relative alle condizioni della policy per Incident Manager

Supporta le chiavi di condizione delle policy specifiche del servizio: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Accedi agli elenchi di controllo (ACLs) in Incident Manager

Supporti ACLs: No

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con Incident Manager

Supporta ABAC (tag nelle policy): No

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Incident Manager

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per Incident Manager

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso diretto (FAS) utilizzano le autorizzazioni del principale chiamante an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Incident Manager

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Incident Manager. Modifica i ruoli di servizio solo quando Incident Manager fornisce indicazioni in tal senso.

Scelta di un ruolo IAM in Incident Manager

Quando si crea una risorsa del piano di risposta in Incident Manager, è necessario scegliere un ruolo per consentire a Incident Manager di eseguire un documento di automazione di Systems Manager per conto dell'utente. Se in precedenza avete creato un ruolo di servizio o un ruolo collegato al servizio, Incident Manager fornisce un elenco di ruoli tra cui scegliere. È importante scegliere un ruolo che consenta l'accesso all'esecuzione delle istanze dei documenti di automazione. Per ulteriori informazioni, consulta Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti. Quando crei un Amazon Q Developer nel canale di chat delle applicazioni di chat da utilizzare durante un incidente, puoi selezionare un ruolo di servizio che ti consenta di utilizzare i comandi direttamente dalla chat. Per ulteriori informazioni sulla creazione di canali di chat per la collaborazione in caso di incidenti, consultaCreazione e integrazione di canali di chat per i soccorritori in Incident Manager. Per ulteriori informazioni sulle politiche IAM nelle applicazioni di chat di Amazon Q Developer, consulta Gestione delle autorizzazioni per l'esecuzione di comandi utilizzando Amazon Q Developer nelle applicazioni di chat nella guida per amministratori di Amazon Q Developer in chat application.

Ruoli collegati ai servizi per Incident Manager

Supporta i ruoli collegati ai servizi: sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni sulla creazione o la gestione dei ruoli collegati ai servizi di Incident Manager, vedere. Utilizzo di ruoli collegati ai servizi per Incident Manager

Esempi di policy basate su identità per Strumento di gestione degli incidenti AWS Systems Manager

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse di Incident Manager. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Incident Manager, incluso il formato di ARNs per ogni tipo di risorsa, vedere Azioni, risorse e chiavi di condizione Strumento di gestione degli incidenti AWS Systems Manager nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Incident Manager
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Accesso a un piano di risposta

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse di Incident Manager nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono

le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Incident Manager

Per accedere alla Strumento di gestione degli incidenti AWS Systems Manager console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse di Incident Manager presenti nel tuo. Account AWS Se si cra una

policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano risolvere gli incidenti utilizzando la console Incident Manager, collega anche la policy `IncidentManagerResolverAccess` AWS gestita di Incident Manager alle entità. Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

```
IncidentManagerResolverAccess
```

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accesso a un piano di risposta

In questo esempio, desideri concedere a un utente IAM del tuo account Amazon Web Services l'accesso a uno dei tuoi piani di risposta di Incident Manager,`exampleplan`. Desideri inoltre consentire all'utente di aggiungere, aggiornare ed eliminare il piano di risposta.

La politica concede `ssm-incidents:ListResponsePlans` le `ssm-incidents:GetResponsePlan` `ssm-incident:ListResponsePlan` autorizzazioni `ssm-incidents:UpdateResponsePlan` e all'utente.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
```

```
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan"
      },
      {
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan/*"
      }
   ]
}
```

Esempi di policy basate sulle risorse per Strumento di gestione degli incidenti AWS Systems Manager

Strumento di gestione degli incidenti AWS Systems Manager supporta politiche di autorizzazione basate sulle risorse per i piani di risposta e i contatti di Incident Manager.

Incident Manager non supporta politiche basate sulle risorse che negano l'accesso alle risorse condivise. AWS RAM

Per informazioni su come creare un piano di risposta o un contatto, consulta e. Creazione e configurazione dei piani di risposta in Incident Manager Creazione e configurazione dei contatti in Incident Manager

Limitazione dell'accesso al piano di risposta di Incident Manager per organizzazione

L'esempio seguente concede le autorizzazioni agli utenti dell'organizzazione con l'ID dell'organizzazione: `o-abc123def45` per rispondere agli incidenti creati utilizzando il piano di risposta. `myplan`

Il `Condition` blocco utilizza `StringEquals` le condizioni e la chiave di `aws:PrincipalOrgID` condizione, che è una chiave di condizione AWS Organizations specifica. Per ulteriori informazioni su queste chiavi di condizione, vedere Specificazione delle condizioni in una politica.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationAccess",
            "Effect": "Allow",
            "Principal": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-abc123def45"
                }
            },
            "Action": [
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:StartIncident",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:UpdateRelatedItems",
                "ssm-incidents:ListRelatedItems"
            ],
            "Resource": [
                "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
                "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
            ]
        }
    ]
}
```

Fornire a Incident Manager l'accesso ai contatti di un responsabile

L'esempio seguente concede al responsabile con l'`arn:aws:iam::999988887777:root`ARN l'autorizzazione a creare interazioni con il contatto. `mycontact`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact",
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

Prevenzione intersettoriale confusa in Incident Manager

Il problema dell'assistente confuso è un problema di sicurezza delle informazioni che si verifica quando un'entità senza l'autorizzazione a eseguire un'azione chiama un'entità con più privilegi a eseguire l'azione. Ciò può consentire ai malintenzionati di eseguire comandi o modificare risorse che altrimenti non avrebbero l'autorizzazione a eseguire o a cui non avrebbero accesso.

In effetti AWS, l'impersonificazione tra diversi servizi può portare a uno scenario sostitutivo confuso. L'impersonificazione tra servizi si verifica quando un servizio (il servizio chiamante) chiama un altro servizio (il servizio chiamato). Un malintenzionato può utilizzare il servizio di chiamata per modificare le risorse di un altro servizio utilizzando autorizzazioni che normalmente non avrebbe.

AWS fornisce ai responsabili del servizio l'accesso gestito alle risorse del vostro account per aiutarvi a proteggere la sicurezza delle vostre risorse. Ti consigliamo di utilizzare le `aws:SourceArn`chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche relative alle risorse.

Queste chiavi limitano le autorizzazioni che Strumento di gestione degli incidenti AWS Systems Manager forniscono un altro servizio a quella risorsa. Se si utilizzano entrambe le chiavi di contesto della condizione globale, il `aws:SourceAccount` valore e l'account a cui si fa riferimento nel `aws:SourceArn` valore devono utilizzare lo stesso ID account quando vengono utilizzati nella stessa dichiarazione politica.

Il valore di `aws:SourceArn` deve essere l'ARN del record dell'incidente interessato. Se non conosci l'ARN completo della risorsa o se stai specificando più risorse, usa la chiave `aws:SourceArn` global context condition con il * jolly per le parti sconosciute dell'ARN. Ad esempio, puoi impostare su. `aws:SourceArn` `arn:aws:ssm-incidents::111122223333:*`

Nel seguente esempio di politica di fiducia, utilizziamo la chiave di `aws:SourceArn` condizione per limitare l'accesso al ruolo di servizio in base all'ARN del record dell'incidente. Solo i record degli incidenti creati dal piano `myresponseplan` di risposta possono utilizzare questo ruolo.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

Utilizzo di ruoli collegati ai servizi per Incident Manager

Strumento di gestione degli incidenti AWS Systems Manager utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Incident Manager. I ruoli collegati ai servizi sono predefiniti da Incident Manager e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di Incident Manager perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Incident Manager definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Incident Manager può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Ciò protegge le risorse di Incident Manager perché non è possibile rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate al servizio per Incident Manager

Incident Manager utilizza il ruolo collegato al servizio denominato. AWSServiceRoleforIncidentManager Questo ruolo consente a Incident Manager di gestire i record degli incidenti di Incident Manager e le risorse correlate per conto dell'utente.

Il ruolo AWSService RoleforIncidentManager collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `ssm-incidents.amazonaws.com`

La politica di autorizzazione dei ruoli `AWSIncidentManagerServiceRolePolicy`consente a Incident Manager di completare le seguenti azioni sulle risorse specificate:

- Azione: `ssm-incidents:ListIncidentRecords` su tutte le risorse relative all'azione.
- Azione: `ssm-incidents:CreateTimelineEvent` su tutte le risorse relative all'azione.
- Azione: `ssm:CreateOpsItem` su tutte le risorse relative all'azione.
- Operazione: `ssm:AssociateOpsItemRelatedItem` su `all resources related to the action.`
- Azione: `ssm-contacts:StartEngagement` su tutte le risorse relative all'azione.
- Azione: `cloudwatch:PutMetricData` sulle CloudWatch metriche all'interno dei namespace `AWS/IncidentManager` e `AWS/Usage`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato al servizio per Incident Manager

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un set di replica nell'API Console di gestione AWS, nella o nell' AWS API AWS CLI, Incident Manager crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un set di replica, Incident Manager crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Incident Manager

Incident Manager non consente di modificare il ruolo collegato al AWSService RoleforIncidentManager servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Incident Manager

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Per eliminare il ruolo collegato al servizio, è necessario prima eliminare il set di repliche. L'eliminazione del set di replica elimina tutti i dati creati e archiviati in Incident Manager, inclusi i piani di risposta, i contatti e i piani di escalation. Inoltre, perderai tutti gli incidenti creati in precedenza. Eventuali allarmi e EventBridge regole che rimandano a piani di risposta eliminati non creeranno più un incidente in caso di allarme o di corrispondenza delle regole. Per eliminare il set di replica è necessario eliminare ogni regione del set.

> **Note**
>
> Se il servizio Incident Manager utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le regioni nel set di replica utilizzato da AWSService RoleforIncidentManager

1. Apri la console Incident Manager e scegli Impostazioni dalla barra di navigazione a sinistra.
2. Seleziona una regione nel set di replica.
3. Scegli Elimina.
4. Per confermare l'eliminazione della regione, inserite il nome della regione e scegliete Elimina.
5. Ripeti questi passaggi fino a eliminare tutte le regioni dal set di replica. Quando si elimina la regione finale, la console informa l'utente che elimina il set di replica che la contiene.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al servizio. AWSService RoleforIncidentManager Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Incident Manager

Incident Manager supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint.

AWS politiche gestite per Strumento di gestione degli incidenti AWS Systems Manager

Una policy AWS gestita è una policy autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo

pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per maggiori informazioni, consulta Policy gestite da AWS nella Guida per l'utente di IAM.

AWS politica gestita: AWSIncident ManagerIncidentAccessServiceRolePolicy

È possibile collegare `AWSIncidentManagerIncidentAccessServiceRolePolicy` alle entità IAM. Incident Manager attribuisce inoltre questa politica a un ruolo di Incident Manager che consente a Incident Manager di eseguire azioni per conto dell'utente.

Questa politica concede autorizzazioni di sola lettura che consentono a Incident Manager di leggere le risorse di alcuni altri per identificare i risultati relativi Servizi AWS agli incidenti in tali servizi.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `cloudformation`— Consente ai principali di descrivere gli stack. CloudFormation Ciò è necessario affinché Incident Manager identifichi CloudFormation gli eventi e le risorse relativi a un incidente.
- `codedeploy`— Consente ai responsabili di leggere le AWS CodeDeploy distribuzioni. Ciò è necessario affinché Incident Manager identifichi le CodeDeploy implementazioni e gli obiettivi correlati a un incidente.
- `autoscaling`— Consente ai responsabili di determinare se un'istanza Amazon Elastic Compute Cloud (EC2) fa parte di un gruppo Auto Scaling. Ciò è necessario per consentire a Incident Manager di fornire risultati per EC2 le istanze che fanno parte dei gruppi di Auto Scaling.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta la AWS Managed Policy AWSIncidentManagerIncidentAccessServiceRolePolicyReference Guide.

AWS Policy gestita: **AWSIncidentManagerServiceRolePolicy**

Non è possibile collegare `AWSIncidentManagerServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a Incident Manager di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Incident Manager.

Questa politica concede a Incident Manager le autorizzazioni per elencare gli incidenti, creare eventi cronologici, creare OpsItems, associare elementi correlati OpsItems, avviare interazioni e pubblicare metriche relative a un incidente. CloudWatch

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm-incidents`— Consente ai responsabili di elencare gli incidenti e creare eventi cronologici. Ciò è necessario per consentire ai soccorritori di collaborare durante un incidente sulla dashboard degli incidenti.
- `ssm`— Consente ai responsabili di creare OpsItems e associare elementi correlati. Ciò è necessario per creare un genitore OpsItem all'inizio di un incidente.
- `ssm-contacts`— Consente ai dirigenti di avviare incarichi. Ciò è necessario affinché Incident Manager possa coinvolgere i contatti durante un incidente.
- `cloudwatch`— Consente ai responsabili di pubblicare CloudWatch metriche. Ciò è necessario affinché Incident Manager pubblichi le metriche relative a un incidente e le metriche di utilizzo.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta la AWS Managed Policy AWSIncidentManagerServiceRolePolicyReference Guide.

AWS politica gestita: **AWSIncidentManagerResolverAccess**

Puoi collegarti `AWSIncidentManagerResolverAccess` alle tue entità IAM per consentire loro di avviare, visualizzare e aggiornare gli incidenti. Ciò consente loro anche di creare gli eventi relativi alla cronologia dei clienti e gli elementi correlati nella dashboard degli incidenti. Puoi anche collegare questa policy al ruolo di servizio Amazon Q Developer nelle applicazioni di chat o direttamente al tuo ruolo gestito dai clienti associato a qualsiasi canale di chat utilizzato per la collaborazione in caso di incidenti. Per ulteriori informazioni sulle politiche IAM nelle applicazioni di chat di Amazon Q Developer, consulta Gestione delle autorizzazioni per l'esecuzione di comandi utilizzando Amazon Q Developer nelle applicazioni di chat nella Guida per l'amministratore di Amazon Q Developer in chat.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm-incidents`— Consente ai responsabili di avviare incidenti, elencare piani di risposta, elencare incidenti, aggiornare incidenti, elencare eventi cronologici, creare eventi cronologici personalizzati, aggiornare eventi cronologici personalizzati, eliminare eventi cronologici personalizzati, elencare elementi correlati, creare elementi correlati e aggiornare elementi correlati.
- `ssm-contacts`— Consente ai responsabili di avviare rapporti con i contatti durante la creazione dell'incidente.

Per visualizzare maggiori dettagli sulla policy, inclusa l'ultima versione del documento sulla policy JSON, consulta la AWS Managed Policy AWSIncidentManagerResolverAccessReference Guide.

Incident Manager: aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Incident Manager da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Incident Manager.

Modifica	Descrizione	Data
AWSIncidentManagerResolverAccess — Aggiornamento della politica	Incident Manager ha aggiunto l'autorizzazione per avviare interazioni con i contatti.	20 novembre 2025
AWSIncidentManagerServiceRolePolicy — Aggiornamento della politica	Incident Manager ha aggiunto una nuova autorizzazione che consente a Incident Manager di pubblicare metriche all'interno del AWS/Usage namespace nel tuo account.	27 gennaio 2025
AWSIncidentManagerIncidentAccessServiceRolePolicy — Aggiornamento della politica	Incident Manager ha aggiunto una nuova autorizzazione aAWSIncidentManagerIncidentAccessServiceRolePolicy , a supporto della funzione Findings, che consente di verificare se un' EC2 istanza fa parte di un gruppo Auto Scaling.	20 febbraio 2024
AWSIncidentManagerIncidentAccessServiceRolePolicy : nuova policy	Incident Manager ha aggiunto una nuova politica che concede a Incident Manager le autorizzazioni per chiamare altri utenti Servizi AWS nell'ambito della gestione di un incidente.	17 novembre 2023
AWSIncidentManagerServiceRolePolicy — Aggiornamento della politica	Incident Manager ha aggiunto una nuova autorizzazione che consente a Incident Manager di pubblicare metriche nel tuo account.	16 dicembre 2022

Modifica	Descrizione	Data
AWSIncidentManagerResolverAccess: nuova policy	Incident Manager ha aggiunto una nuova politica che consente di avviare incidenti , elencare piani di risposta, elencare incidenti, aggiornare incidenti, elencare eventi cronologici, creare eventi cronologici personalizzati, aggiornare eventi cronologici personalizzati, eliminare eventi cronologici personalizzati, elencare elementi correlati , creare elementi correlati e aggiornare elementi correlati.	26 Aprile 2021
AWSIncidentManagerServiceRolePolicy: nuova policy	Incident Manager ha aggiunto una nuova politica per concedere a Incident Manager le autorizzazioni per elencare gli incidenti OpsItems, creare eventi cronologici OpsItems, creare, associare elementi correlati e avviare interventi relativi a un incidente.	26 Aprile 2021
Incident Manager ha iniziato a tenere traccia delle modifiche	Incident Manager ha iniziato a tenere traccia delle modifiche per le politiche AWS gestite.	26 Aprile 2021

Risoluzione dei problemi di Strumento di gestione degli incidenti AWS Systems Manager identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Incident Manager e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Incident Manager

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `ssm-incidents:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `ssm-incidents:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Incident Manager.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Incident Manager. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne al mio account Amazon Web Services di accedere alle mie risorse di Incident Manager

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Incident Manager supporta queste funzionalità, consulta. Come Strumento di gestione degli incidenti AWS Systems Manager funziona con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo dei contatti condivisi e dei piani di risposta in Incident Manager

Con la condivisione dei contatti, in qualità di proprietario del contatto, puoi condividere informazioni di contatto, piani di escalation e impegni con altre persone Account AWS o all'interno di un'organizzazione. AWS

Con la condivisione del piano di risposta, in qualità di proprietario del piano di risposta, puoi condividere un piano di risposta e gli incidenti correlati con altre Account AWS persone o all'interno di un'organizzazione. AWS

Il proprietario di un contatto o di un piano di risposta può condividere contatti e piani di risposta con:

- Specifico Account AWS all'interno o all'esterno della sua organizzazione in AWS Organizations
- Un'unità organizzativa all'interno della propria organizzazione in AWS Organizations
- La sua intera organizzazione in AWS Organizations

Indice

Prerequisiti per la condivisione dei contatti e dei piani di risposta

Per condividere un contatto o un piano di risposta con l'organizzazione o l'unità organizzativa in AWS Organizations:

- Devi possedere la risorsa del tuo Account AWS. Non puoi condividere un contatto o un piano di risposta che è stato condiviso con te.

- Devi abilitare la condivisione con AWS Organizations. Per ulteriori informazioni, consulta Abilita la condivisione con AWS Organizations nella Guida per l'utente AWS RAM .

Servizi correlati

La condivisione dei contatti e dei piani di risposta si integra con AWS Resource Access Manager (AWS RAM). Con AWS RAM, puoi condividere AWS le tue risorse con chiunque Account AWS o tramite AWS Organizations. Puoi condividere le risorse di tua proprietà creando una condivisione di risorse. Una condivisione delle risorse specifica le risorse da condividere e gli utenti con cui condividerle. I consumatori possono essere singoli individui Account AWS, unità organizzative o un'intera organizzazione AWS Organizations.

Per ulteriori informazioni in merito AWS RAM, consulta la Guida AWS RAM per l'utente.

Condivisione di un contatto o di un piano di risposta

Dopo aver condiviso un piano di risposta, i consumatori hanno accesso a tutti gli incidenti passati, attuali e futuri creati utilizzando quel piano di risposta.

Dopo aver condiviso un contatto, i consumatori hanno accesso alle informazioni di contatto, al piano di coinvolgimento, ai piani di escalation e alle interazioni che si verificano durante un incidente. I consumatori possono anche attivare un piano di contatto o di intensificazione durante un incidente.

Se fai parte di un'organizzazione AWS Organizations e la condivisione all'interno dell'organizzazione è abilitata, ai consumatori dell'organizzazione viene automaticamente concesso l'accesso al contatto o al piano di risposta condiviso. In caso contrario, i consumatori ricevono un invito a partecipare alla condivisione delle risorse e ottengono l'accesso al contatto o al piano di risposta condiviso dopo aver accettato l'invito.

Puoi condividere un contatto o un piano di risposta di tua proprietà utilizzando la AWS RAM console o il AWS CLI.

> **Note**
>
> Attualmente, la possibilità di aggiungere un contatto condiviso da un altro account a un piano di risposta non è supportata.

Per condividere un contatto o un piano di risposta di tua proprietà utilizzando la AWS RAM console

Consulta Creazione di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per condividere un contatto o un piano di risposta di cui sei proprietario utilizzando il AWS CLI

Utilizza il comando create-resource-share.

Interrompere la condivisione di un contatto o di un piano di risposta condiviso

Quando il proprietario di una risorsa smette di condividere un contatto o un piano di risposta con un consumatore, i contatti, i piani di risposta, i piani di escalation, le interazioni e gli incidenti non vengono più visualizzati nella console del consumatore.

> **Note**
>
> Il consumatore continua a visualizzare i contatti, i piani di risposta, i piani di intensificazione, le interazioni o gli incidenti senza aggiornamenti, se li visualizza nella console, fino a quando non aggiorna la pagina o abbandona la pagina.

Per interrompere la condivisione di un contatto o di un piano di risposta condiviso di cui sei proprietario, devi rimuoverlo dalla condivisione delle risorse. Puoi farlo utilizzando la AWS RAM console o il AWS CLI.

Per interrompere la condivisione di un contatto condiviso o di un piano di risposta di tua proprietà utilizzando la AWS RAM console

Consulta Aggiornamento di una condivisione di risorse in Guida per l'utente di AWS RAM .

Per interrompere la condivisione di un contatto o di un piano di risposta condiviso di cui sei proprietario, utilizza il AWS CLI

Utilizza il comando disassociate-resource-share.

Identificazione di un contatto o di un piano di risposta condiviso

I proprietari e i consumatori possono identificare i contatti condivisi e i piani di risposta utilizzando la console Incident Manager e AWS CLI.

Per identificare un contatto o un piano di risposta condiviso utilizzando la console Incident Manager

> **Note**
>
> I contatti, i piani di risposta, i piani di escalation, gli impegni e gli incidenti in genere non sono identificabili come risorse condivise nella console Incident Manager. Nei luoghi in cui l'Amazon Resource Name (ARN) è visibile, l'ARN contiene l'ID dell'account del proprietario.

Per identificare un contatto o un piano di risposta condiviso utilizzando il AWS CLI

Usa i ListContactscomandi ListResponsePlanso. Il comando restituisce i contatti e i piani di risposta di cui sei proprietario e i contatti e i piani di risposta che sono condivisi con te. L'ARN mostra l' Account AWS ID del contatto o del proprietario del piano di risposta.

Autorizzazioni condivise per i contatti e i piani di risposta

Autorizzazioni per i proprietari

I proprietari possono aggiornare, visualizzare, condividere, interrompere la condivisione e utilizzare i contatti e i piani di risposta. I contatti e i piani di risposta includono gli impegni e gli incidenti correlati.

Autorizzazioni per gli utenti

I consumatori possono utilizzare e visualizzare solo i piani di risposta e i contatti. I contatti e i piani di risposta includono gli impegni e gli incidenti correlati.

Fatturazione e misurazione

La fattura della risorsa viene fatturata al proprietario della risorsa. Ai consumatori non vengono fatturate le risorse condivise con loro. Non ci sono costi aggiuntivi associati alla condivisione di una risorsa.

Limiti di istanze

La condivisione di una risorsa non influisce sui limiti della risorsa nell'account del proprietario o del consumatore. Per calcolare i limiti della risorsa viene utilizzato solo l'account del proprietario.

Convalida della conformità per Strumento di gestione degli incidenti AWS Systems Manager

I revisori esterni valutano la sicurezza e la conformità nell' Strumento di gestione degli incidenti AWS Systems Manager ambito di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta AWS la documentazione sulla sicurezza.

Resilienza in Strumento di gestione degli incidenti AWS Systems Manager

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS

Incident Manager è un servizio globale a livello regionale e attualmente non supporta le zone di disponibilità.

Oltre all'infrastruttura AWS globale, Incident Manager offre diverse funzionalità per supportare le esigenze di resilienza e backup dei dati. Durante la procedura guidata di preparazione preliminare, ti viene chiesto di configurare un set di replica. Questo set di replica regionale assicura che i dati e le

risorse siano accessibili da più regioni, rendendo più gestibile la gestione degli incidenti su una rete cloud. Questa replica garantisce inoltre che i dati siano sicuri e accessibili in caso di guasto di una delle aree geografiche.

Per ulteriori informazioni sull'utilizzo del set di replica di Incident Manager, vedere. Configurazione del set di repliche di Incident Manager

Sicurezza dell'infrastruttura in Strumento di gestione degli incidenti AWS Systems Manager

In quanto servizio gestito, Strumento di gestione degli incidenti AWS Systems Manager è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere a Incident Manager attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Utilizzo Strumento di gestione degli incidenti AWS Systems Manager e interfaccia degli endpoint VPC ()AWS PrivateLink

Puoi stabilire una connessione privata tra il tuo VPC e creare un Strumento di gestione degli incidenti AWS Systems Manager endpoint VPC di interfaccia. Endpoint di interfaccia con tecnologia AWS PrivateLink. Con AWS PrivateLink, puoi accedere in modo privato alle operazioni dell'API Incident Manager senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione.. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le operazioni dell'API Incident Manager. Il traffico tra il tuo VPC e Incident Manager rimane all'interno della rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti.

Per ulteriori informazioni, consultare Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Considerazioni sugli endpoint VPC di Incident Manager

Prima di configurare un endpoint VPC di interfaccia per Incident Manager, assicurati di esaminare le proprietà, le limitazioni e AWS PrivateLink le quote degli endpoint dell'interfaccia nella Amazon VPC User Guide.

Incident Manager supporta l'esecuzione di chiamate a tutte le sue azioni API dal tuo VPC. Per utilizzare tutto Incident Manager, devi creare due endpoint VPC: uno per `ssm-incidents` e uno per. `ssm-contacts`

Creazione di un endpoint VPC di interfaccia per Incident Manager

Puoi creare un endpoint VPC per Incident Manager utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consultare Creazione di un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per Incident Manager utilizzando i nomi di servizio supportati per Incident Manager nel tuo. Regione AWS Gli esempi seguenti mostrano i formati degli endpoint dell'interfaccia per gli endpoint dual-stack IPv4 .

IPv4 formati degli endpoint

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

formati a doppio stack (IPv4 e) per endpoint IPv6

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

Per gli elenchi degli endpoint supportati per tutte le regioni, consulta Endpoint e quote di AWS Systems Manager Incident Manager nella Guida di riferimento generale.AWS

Se si abilita il DNS privato per l'endpoint di interfaccia, è possibile effettuare richieste API a Incident Manager utilizzando i nomi DNS regionali predefiniti nel formato. Gli esempi seguenti mostrano il formato predefinito dei nomi DNS regionali.

- `ssm-incidents.region.amazonaws.com`
- `ssm-contacts.region.amazonaws.com`

Per ulteriori informazioni, consultare Accesso a un servizio tramite un endpoint di interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy sugli endpoint VPC per Incident Manager

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso a Incident Manager. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse su cui è possibile eseguire queste azioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC nella Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni di Incident Manager

Di seguito è riportato un esempio di policy sugli endpoint per Incident Manager. Se associata a un endpoint, questa policy consente l'accesso alle azioni elencate di Incident Manager a tutti i responsabili su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Analisi della configurazione e della vulnerabilità in Incident Manager

La configurazione e i controlli IT sono una responsabilità condivisa tra te AWS e te, nostro cliente. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Le migliori pratiche di sicurezza in Strumento di gestione degli incidenti AWS Systems Manager

Strumento di gestione degli incidenti AWS Systems Manager offre molte funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

Argomenti

Le migliori pratiche di sicurezza preventiva per Incident Manager

Implementazione dell'accesso con privilegi minimi

Quando concedi le autorizzazioni, sei tu a decidere chi ottiene quali autorizzazioni per quali risorse di Incident Manager. È possibile abilitare operazioni specifiche che si desidera consentire su tali risorse. Pertanto, concedi solo le autorizzazioni necessarie per eseguire un'attività. L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi di sicurezza e l'impatto risultante da errori o intenzioni dannose.

Gli strumenti seguenti sono disponibili per implementare l'accesso con privilegi minimi:

- Controllo dell'accesso alle AWS risorse tramite policy e limiti di autorizzazioni per le entità IAM
- Policy di controllo dei servizi

Creazione e gestione dei contatti

Quando si attivano i contatti, Incident Manager contatta il dispositivo per confermare l'attivazione. Assicurati che le informazioni sul dispositivo siano corrette prima di attivarlo. Ciò riduce la possibilità che Incident Manager contatti il dispositivo o la persona sbagliati durante l'attivazione.

Esamina regolarmente i tuoi contatti e i tuoi piani di escalation per assicurarti che vengano contattati solo i contatti che devono essere contattati durante un incidente. Controlla regolarmente i contatti per rimuovere informazioni obsolete o errate. Se un contatto non deve più essere informato quando si verifica un incidente, rimuovilo dai relativi piani di escalation o rimuovilo da Incident Manager.

Rendi privati i canali di chat

Puoi rendere privati i canali di chat relativi agli incidenti per implementare l'accesso con privilegi minimi. Prendi in considerazione l'utilizzo di un canale di chat diverso con un elenco di utenti ristretto per ogni modello di piano di risposta. Ciò garantisce che solo i rispondenti corretti vengano inseriti in un canale di chat che può contenere informazioni sensibili.

Slacki canali creati in Amazon Q Developer nelle applicazioni di chat ereditano le autorizzazioni del ruolo IAM utilizzato per configurare Amazon Q Developer nelle applicazioni di chat. Ciò consente ai soccorritori di un Slack canale Amazon Q Developer in chat abilitato alle applicazioni di chat di richiamare qualsiasi azione consentita, come Incident Manager APIs e il recupero dei grafici delle metriche.

AWS Mantieni gli strumenti aggiornati

AWS rilascia regolarmente versioni aggiornate di strumenti e plugin che puoi utilizzare nelle tue AWS operazioni. Mantenere aggiornate queste risorse garantisce che gli utenti e le istanze dell'account abbiano accesso alle funzionalità e alle funzionalità di sicurezza più recenti di questi strumenti.

- AWS CLI — The AWS Command Line Interface (AWS CLI) è uno strumento open source che consente di interagire con i AWS servizi utilizzando i comandi nella shell della riga di comando. Per aggiornare l' AWS CLI, si esegue lo stesso comando utilizzato per installare l' AWS CLI. Si consiglia di creare un'attività pianificata sul computer locale per eseguire il comando appropriato al sistema operativo almeno una volta ogni due settimane. Per informazioni sui comandi di installazione, vedere Installazione dell'interfaccia a riga di AWS comando nella Guida per l'utente dell'interfaccia a riga di AWS comando.
- AWS Tools for Windows PowerShell — Gli strumenti per Windows PowerShell sono un insieme di PowerShell moduli basati sulle funzionalità esposte dall' AWS SDK for .NET. Gli strumenti per Windows PowerShell consentono di eseguire operazioni di script sulle AWS risorse dalla PowerShell riga di comando. Periodicamente, man mano che PowerShell vengono rilasciate

versioni aggiornate degli Strumenti per Windows, è necessario aggiornare la versione in esecuzione localmente. Per informazioni, consulta Aggiornamento AWS Tools for Windows PowerShell su Windows o Aggiornamento AWS Tools for Windows PowerShell su Linux o macOS.

Contenuti correlati

Best practice di sicurezza per Systems Manager

Procedure ottimali per la sicurezza dei detective per Incident Manager

Identifica e controlla tutte le tue risorse di Incident Manager

L'identificazione degli asset IT è un aspetto essenziale di governance e sicurezza. Identifica le risorse dei Systems Manager per valutarne il livello di sicurezza e intervenire sulle potenziali aree di debolezza. Crea gruppi di risorse per le tue risorse di Incident Manager. Per ulteriori informazioni, consulta Che cosa sono i gruppi di risorse? nella Guida per l'utente di AWS Resource Groups .

Usa AWS CloudTrail

AWS CloudTrail fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Incident Manager. Utilizzando le informazioni raccolte da AWS CloudTrail, è possibile determinare la richiesta effettuata a Incident Manager, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi. Per ulteriori informazioni, consulta Registrazione delle chiamate Strumento di gestione degli incidenti AWS Systems Manager API utilizzando AWS CloudTrail.

Monitora gli avvisi AWS di sicurezza

Controlla regolarmente gli avvisi di sicurezza pubblicati Trusted Advisor su. Account AWS Puoi farlo a livello di codice utilizzando. describe-trusted-advisor-checks

Inoltre, monitora attivamente l'indirizzo email principale registrato su ciascuno dei tuoi. Account AWS AWS ti contatterà, utilizzando questo indirizzo email, in merito a problemi di sicurezza emergenti che potrebbero interessarti.

AWS i problemi operativi di ampio impatto sono pubblicati nel AWS Service Health Dashboard. I problemi operativi sono anche pubblicati sui singoli account tramite AWS Health Dashboard. Per ulteriori informazioni, consulta la documentazione relativa ad AWS Health.

Contenuti correlati

Amazon Web Services: panoramica dei processi di sicurezza (whitepaper)

Guida introduttiva: segui le migliori pratiche di sicurezza durante la configurazione AWS delle risorse (AWS Security Blog)

Best practice di IAM

Migliori pratiche di sicurezza in AWS CloudTrail

Monitoraggio in Incident Manager

AWS Systems Manager Incident Manager si integra con i seguenti servizi che offrono funzionalità di monitoraggio e registrazione:

CloudWatch metriche

Utilizza le CloudWatch metriche per recuperare le statistiche sui punti dati per le operazioni di AWS Systems Manager Incident Manager come set ordinato di dati di serie temporali, noti come metriche. È possibile utilizzare questi parametri per verificare che le prestazioni del sistema siano quelle previste. Per ulteriori informazioni, consulta Metriche di monitoraggio in Incident Manager con Amazon CloudWatch.

CloudTrail logs

Utilizzato AWS CloudTrail per acquisire informazioni dettagliate sulle chiamate effettuate a. AWS APIs Puoi archiviare queste chiamate come file di registro in Amazon Simple Storage Service. Puoi utilizzare questi CloudTrail registri per determinare informazioni come la chiamata effettuata, l'indirizzo IP di origine da cui proviene la chiamata, chi ha effettuato la chiamata e quando è stata effettuata la chiamata. I CloudTrail log contengono informazioni sulle chiamate alle azioni API per Incident Manager. Per ulteriori informazioni, vedere. Registrazione delle chiamate Strumento di gestione degli incidenti AWS Systems Manager API utilizzando AWS CloudTrail

Trusted Advisor

AWS Trusted Advisor può aiutarti a monitorare AWS le tue risorse per migliorare prestazioni, affidabilità, sicurezza ed economicità. Quattro Trusted Advisor controlli sono disponibili per tutti gli utenti; più di 50 controlli sono disponibili per gli utenti con un piano di supporto Business o Enterprise. Per Incident Manager, Trusted Advisor verifica che la configurazione di un set di replica ne utilizzi più di uno Regione AWS per supportare il failover e la risposta regionali. Per ulteriori informazioni, consulta AWS Trusted Advisor nella Guida per l'utente di Supporto AWS .

Metriche di monitoraggio in Incident Manager con Amazon CloudWatch

Incident Manager fornisce metriche aggregate che puoi monitorare in Amazon. CloudWatch Puoi utilizzare queste metriche per identificare le tendenze degli incidenti e dei piani di risposta.

Tali parametri includono:

- Numero di incidenti creati in un determinato periodo di tempo
- Il tempo necessario per rispondere e risolvere tali incidenti
- Numero di incidenti risolti

È possibile monitorare le metriche di Incident Manager per comprendere meglio lo stato operativo e intraprendere azioni significative per promuovere l'eccellenza operativa della risposta agli incidenti. Le metriche di Incident Manager sono disponibili in tutte le regioni di Incident Manager. Le tue metriche saranno disponibili per la visualizzazione in Amazon CloudWatch per tutte le regioni specificate nel set di repliche al momento dell'onboarding su Incident Manager. Puoi visualizzare le metriche pubblicate nella regione in cui sono state intraprese le azioni per l'incidente. Non sono previsti costi aggiuntivi per queste metriche.

Sulla CloudWatch console, puoi creare dashboard con queste metriche per:

- Misura e rivedi il carico di incidenti esistente
- Verifica se il carico dell'incidente sta aumentando, diminuendo o rimanendo invariato
- Usa Incident Manager in modo più efficace per ridurre la frequenza, la durata e l'impatto degli incidenti

Questa pagina descrive le metriche di Incident Manager disponibili sulla CloudWatch console.

> **Important**
>
> Per un evento generato dal cliente, se il valore di origine in `TriggerDetails` è denominato utilizzando caratteri non ASCII, le metriche relative all'evento non verranno riportate in Amazon CloudWatch metrics, che non supporta testo non ASCII. `source`può essere fornito solo in modo programmatico, ad esempio utilizzando un SDK o. AWS CLI

Incident Manager invia le seguenti metriche a. CloudWatch

Parametro	Descrizione
`NumberOfCreateIncidents`	Numero di incidenti creati.

Parametro	Descrizione
	Dimensioni valide: [] (dimensione vuota), [ResponsePlan], [Impact], [Source], [ResponsePlan ,Impact], [ResponseP lan ,Source] Unità: numero
NumberOfResolveIncidents	Numero di incidenti risolti. Dimensioni valide: [] (dimensione vuota), [ResponsePlan], [Impact], [Source], [ResponsePlan ,Impact], [ResponseP lan ,Source] Unità: numero
TimeToFirstAcknowledgement	Differenza di fuso orario tra l'ora di creazione dell'inci dente e l'ora in cui è stato dato il primo riconosci mento dell'incidente. Dimensioni valide: [] (dimensione vuota), [ResponsePlan], [Impact], [Source], [,Impact]ResponsePlan , [ResponsePlan ,] Source Unità: secondi
TimeToResolveIncident	Differenza di tempo tra il momento in cui l'incidente è stato creato e quello in cui è stato risolto. Dimensioni valide:] (Dimensione vuota), [ResponseP lan], [Impact], [Source], [ResponseP lan ,Impact], [ResponsePlan ,Source] Unità: secondi

Visualizzazione delle metriche di Incident Manager sulla console CloudWatch

Per visualizzare le metriche di Incident Manager nella console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi `IncidentManager`.
4. Nella scheda Metriche, scegli una dimensione, quindi scegli una metrica.

Per ulteriori informazioni sull'utilizzo CloudWatch delle metriche, consulta i seguenti argomenti nella Amazon CloudWatch User Guide:

- Metriche
- Utilizzo dei CloudWatch parametri di Amazon

Dimensioni per i parametri

I parametri di Incident Manager utilizzano lo spazio dei `IncidentManager` nomi e forniscono parametri per le seguenti dimensioni:

Dimensione	Descrizione
`By Response Plan`	Visualizza le metriche aggregate per piano di risposta.
`By Impact Level`	Visualizza le metriche aggregate in base al livello di gravità.
`By Source`	Visualizza le metriche per gli incidenti creati manualmente, per CloudWatch allarme o evento. EventBridge
`Across All Incidents`	Visualizza le metriche aggregate per tutti gli incidenti nella regione corrente. AWS

Dimensione	Descrizione
`Response Plan name and Source`	Visualizza le metriche aggregate per ogni combinazione di piano di risposta e fonte.
`Response Plan Name and Impact Level`	Visualizza le metriche aggregate per ogni combinazione di piano di risposta e livello di gravità.

Registrazione delle chiamate Strumento di gestione degli incidenti AWS Systems Manager API utilizzando AWS CloudTrail

Strumento di gestione degli incidenti AWS Systems Manager è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o un Servizio AWS. CloudTrail acquisisce tutte le chiamate API per Incident Manager come eventi. Le chiamate acquisite includono chiamate dalla console Incident Manager e chiamate in codice alle operazioni dell'API Incident Manager. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Incident Manager, l'indirizzo IP da cui è stata effettuata la richiesta, quando è stata effettuata e ulteriori dettagli.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente.
- Se la richiesta è stata effettuata per conto di un utente del Centro identità IAM.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

CloudTrail è attivo nel tuo account Account AWS quando crei l'account e hai automaticamente accesso alla cronologia degli CloudTrail eventi. La cronologia CloudTrail degli eventi fornisce un record visualizzabile, ricercabile, scaricabile e immutabile degli ultimi 90 giorni di eventi di gestione registrati in un. Regione AWSPer ulteriori informazioni, consulta Lavorare con la cronologia degli CloudTrail eventi nella Guida per l'utente.AWS CloudTrail Non sono CloudTrail previsti costi per la visualizzazione della cronologia degli eventi.

Per un registro continuo degli eventi degli Account AWS ultimi 90 giorni, crea un trail o un data store di eventi CloudTrailLake.

CloudTrail sentieri

Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Tutti i percorsi creati utilizzando il Console di gestione AWS sono multiregionali. È possibile creare un trail per una singola Regione o per più Regioni tramite AWS CLI. La creazione di un percorso multiregionale è consigliata in quanto consente di registrare l'intera attività del proprio Regioni AWS account. Se si crea un trail per una singola Regione, è possibile visualizzare solo gli eventi registrati nella Regione AWS del trail. Per ulteriori informazioni sui trail, consulta Creating a trail for your Account AWS e Creating a trail for an organization nella Guida per l'utente di AWS CloudTrail .

Puoi inviare gratuitamente una copia dei tuoi eventi di gestione in corso al tuo bucket Amazon S3 CloudTrail creando un percorso, tuttavia ci sono costi di storage di Amazon S3. Per ulteriori informazioni sui CloudTrail prezzi, consulta la pagina Prezzi.AWS CloudTrail Per informazioni sui prezzi di Amazon S3, consulta Prezzi di Amazon S3.

CloudTrail Archivi di dati sugli eventi di Lake

CloudTrail Lake ti consente di eseguire query basate su SQL sui tuoi eventi. CloudTrail Lake converte gli eventi esistenti in formato JSON basato su righe in formato Apache ORC. ORC è un formato di archiviazione a colonne ottimizzato per il recupero rapido dei dati. Gli eventi vengono aggregati in archivi di dati degli eventi, che sono raccolte di eventi immutabili basate sui criteri selezionati applicando i selettori di eventi avanzati. I selettori applicati a un archivio di dati degli eventi controllano quali eventi persistono e sono disponibili per l'esecuzione della query. Per ulteriori informazioni su CloudTrail Lake, consulta Working with AWS CloudTrail Lake nella Guida per l'utente.AWS CloudTrail

CloudTrail Gli archivi e le richieste di dati sugli eventi di Lake comportano dei costi. Quando crei un datastore di eventi, scegli l'opzione di prezzo da utilizzare per tale datastore. L'opzione di prezzo determina il costo per l'importazione e l'archiviazione degli eventi, nonché il periodo di conservazione predefinito e quello massimo per il datastore di eventi. Per ulteriori informazioni sui CloudTrail prezzi, consulta la sezione Prezzi.AWS CloudTrail

Eventi di gestione di Incident Manager in CloudTrail

Gli eventi di gestione forniscono informazioni sulle operazioni di gestione eseguite sulle risorse dell'utente Account AWS. Queste operazioni sono definite anche operazioni del piano di controllo (control-plane). Per impostazione predefinita, CloudTrail registra gli eventi di gestione.

Strumento di gestione degli incidenti AWS Systems Manager registra tutte le operazioni del piano di controllo di Incident Manager come eventi di gestione. Per un elenco delle operazioni del piano di Strumento di gestione degli incidenti AWS Systems Manager controllo a cui Incident Manager accede CloudTrail, consulta l'Strumento di gestione degli incidenti AWS Systems Manager API Reference.

Esempi di eventi di Incident Manager

Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione API richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi gli eventi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`StartIncident`azione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
```

```
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`DeleteContactChannel`azione.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
```

```
    "recipientAccountId": "12345678901234567"
}
```

Per informazioni sul contenuto dei CloudTrail record, consultate il contenuto dei CloudTrail record nella Guida per l'AWS CloudTrail utente.

Integrazioni di prodotti e servizi con Incident Manager

Incident Manager, uno strumento in AWS Systems Manager, si integra con i seguenti prodotti, servizi e strumenti.

Integrazione con Servizi AWS

Incident Manager si integra con gli strumenti Servizi AWS e gli strumenti descritti nella tabella seguente.

AWS CDK	AWS CDK Si tratta di un framework di sviluppo che consente di utilizzare il codice per definire l'infrastruttura cloud e utilizzarlo CloudForm ation per il provisioning. AWS CDK Supporta più linguaggi di programmazione tra cui TypeScript, JavaScript PythonJava, e C#/.Net. Per informazioni sull'utilizzo di AWS CDK con Incident Manager, consulta le seguenti sezioni nell'API Reference:AWS CDK • @aws-cdk/aws-ssmincidentsmodulo • @aws-cdk/aws-ssmcontactsmodulo
Amazon Q Developer nelle applicazioni di chat	Amazon Q Developer nelle applicazioni di chat consente ai DevOps team di sviluppo software di utilizzare le chat room dei programmi di messaggistica per monitorare e rispondere agli eventi operativi all'interno dei propri ambienti Cloud AWS. Utilizzando Amazon Q Developer nelle applicazioni di chat con Incident Manager, puoi creare canali di chat che i soccorritori possono utilizzare per monitorare e risponder e agli incidenti. Amazon Q Developer nelle applicazioni di Slack chat supporta chat room,

	Microsoft Teams canali e chat room Amazon Chime come canali di chat. Oltre alla creazione di un canale di chat, crei anche un argomento in Amazon Simple Notification Service (Amazon SNS). Amazon SNS è un servizio gestito che fornisce il recapito dei messaggi dagli editori agli abbonati. Nei piani di risposta agli incidenti, quando associ un canale di chat che hai creato al piano, scegli anche uno o più argomenti da associare al canale di chat. Questi argomenti SNS vengono utilizzati per inviare notifiche relative a un incidente ai soccorritori. Per ulteriori informazioni, consulta Creazione e integrazione di canali di chat per i soccorritori in Incident Manager.
CloudFormation	CloudFormation è un servizio che è possibile utilizzare per creare un modello con tutte le risorse necessarie per l'applicazione e quindi configurare e fornire le risorse al posto dell'uten te. Inoltre, configurerà tutte le dipendenze, in modo che possiate concentrarvi maggiormente sull'applicazione e meno sulla gestione delle risorse. Per informazioni sull'utilizzo CloudFormation con Incident Manager, vedere i seguenti argomenti nella Guida per l'AWS CloudForm ation utente: • Riferimento al tipo di risorsa Incident Manager • Contatti, tipo di risorsa, riferimento al tipo di risorsa

Amazon CloudWatch	CloudWatchmonitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi utilizzarlo CloudWatch per raccogliere e tenere traccia delle metriche, che sono variabili che puoi misurare per le tue risorse e applicazioni. È possibile configurare gli CloudWatch allarmi per creare incidenti in Incident Manager. CloudWatch collabora con Systems Manager e Incident Manager per creare un incidente da un modello di piano di risposta quando un allarme entra in stato di allarme. Per ulteriori informazioni, consulta Creazione automatica di incidenti con allarmi CloudWatch.
Amazon Chime	Amazon Chime è un ambiente di lavoro online che combina riunioni, chat e chiamate di lavoro. Puoi incontrarti, chattare ed effettuare chiamate di lavoro all'interno e all'esterno della tua organizzazione utilizzando Amazon Chime. Puoi integrare una stanza Amazon Chime nelle tue operazioni di Incident Manager creando un canale di chat per Amazon Chime in Amazon Q Developer nelle applicazioni di chat e quindi aggiungendo quel canale a un piano di risposta. Per ulteriori informazioni, consulta Creazione e integrazione di canali di chat per i soccorritori in Incident Manager.

Amazon EventBridge	EventBridgeè un servizio serverless che utilizza gli eventi per connettere i componenti dell'applicazione, semplificando la creazione di applicazioni scalabili basate sugli eventi. È possibile configurare EventBridge regole per controllare i modelli di eventi nelle AWS risorse e creare un incidente in Incident Manager quando un evento corrisponde a uno schema definito. Le tue regole possono monitorare i modelli di eventi in dozzine di applicazioni Servizi AWS e servizi di terze parti. Per ulteriori informazioni, consulta Creazione automatica di incidenti con EventBridge eventi.
Gestione dei segreti AWS	Secrets Manager consente di gestire, recuperare e ruotare le credenziali del database, le credenziali delle applicazioni, OAuth i token, le chiavi API e altri segreti durante il loro ciclo di vita. Quando integri Incident Manager con il PagerDuty servizio, crei un segreto in Secrets Manager che contiene PagerDuty le tue credenziali. Per ulteriori informazioni, consulta Archiviazione delle credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS.

AWS Systems Manager	Systems Manager è un hub operativo che puoi utilizzare per visualizzare e controllare l'infrast ruttura applicativa e una soluzione di end-to-end gestione sicura per gli ambienti cloud. I seguenti strumenti di Systems Manager si integrano direttamente con Incident Manager: • Automazione: un runbook di automazione definisce le azioni che Systems Manager esegue sulle AWS risorse. In Incident Manager, un runbook definisce una serie di passaggi automatici e manuali da utilizzare per risolvere gli incidenti. Per informazioni sulla creazione di runbook di automazione da utilizzare con Incident Manager, vedere. Integrazione dei runbook di Systems Manager Automation in Incident Manager per la correzione degli incidenti • OpsCenter— OpsCenter fornisce una posizione centrale in cui gli ingegneri operativi e i professionisti IT possono gestire gli elementi di lavoro operativi, denominat i OpsItems, correlati alle AWS risorse. È possibile creare OpsItems direttamente da un'analisi post-incidente per dare seguito al lavoro correlato. Per ulteriori informazioni, consulta Performin g a post-incident analysis in Incident Manager.

AWS Trusted Advisor	Trusted Advisorè uno strumento disponibile per AWS i clienti con un piano di supporto di base o per sviluppatori. Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibi lità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza. Per Incident Manager, Trusted Advisor verifica che la configurazione di un set di replica ne utilizzi più di uno Regione AWS per supportare il failover e la risposta regionali.

Integrazione con altri prodotti e servizi

È possibile integrare o utilizzare Incident Manager con i servizi di terze parti descritti nella tabella seguente.

Jira Cloud	Utilizzando AWS Service Management Connector, puoi integrare Incident Manager con Jira Cloud (Atlassian), una piattaforma di workflow di terze parti basata sul cloud. Dopo aver configurato l'integrazione con Jira Cloud, quando crei un nuovo incidente in Incident Manager, l'integrazione crea l'inciden te anche in Jira Cloud. Se aggiorni un incidente in Incident Manager, esegue questi aggiornam enti all'incidente corrispondente in Jira Cloud. Se risolvi un incidente in Incident Manager o Jira Cloud, l'integrazione risolve l'incidente in entrambi i servizi in base alle preferenze configurate.

	Per ulteriori informazioni, consulta Integrazione Strumento di gestione degli incidenti AWS Systems Manager (Jira Cloud) nella Guida per l'amministratore.AWS Service Management Connector
Gestione dei servizi Jira	Utilizzando AWS Service Management Connector, puoi integrare Incident Manager con Jira Service Management, una piattaforma di workflow di terze parti basata sul cloud. Dopo aver configurato l'integrazione con Jira Service Management, quando crei un nuovo incidente in Incident Manager, l'integrazione crea l'incidente anche in Jira Service Management. Se aggiorni un incidente in Incident Manager, apporta questi aggiornamenti all'incidente corrispondente in Jira Service Management. Se risolvi un incidente in Incident Manager o Jira Service Management, l'integrazione risolve l'incidente in entrambi i servizi in base alle preferenze configurate. Per ulteriori informazioni, consulta Configurazione di Jira Service Management nella Guida per l'amministratore.AWS Service Management Connector

Microsoft Teams	Microsoft Teamsfornisce strumenti collaborativi basati sul cloud per la messaggistica di gruppo, le conferenze audio e video e la condivisione di file. Puoi integrare un Microsoft Teams canale nelle tue operazioni di Incident Manager creando un canale di chat per Microsoft Team Amazon Q Developer nelle applicazioni di chat e quindi aggiungendo quel canale a un piano di risposta. Per ulteriori informazioni, consulta Creazione e integrazione di canali di chat per i soccorritori in Incident Manager.

PagerDuty	PagerDutyè uno strumento di risposta agli incidenti che supporta i flussi di lavoro di paging e le politiche di escalation. Quando integri Incident Manager con PagerDuty, puoi aggiungere un PagerDuty servizio al tuo piano di risposta. Dopodiché , viene creato un incidente corrispondente PagerDuty ogni volta che viene creato un incidente in Incident Manager. L'incidente PagerDuty utilizza il flusso di lavoro di paging e le politiche di escalation ivi definite oltre a quelle in Incident Manager. PagerDutyallega gli eventi della cronologia di Incident Manager come note sull'incidente. Per integrare Incident Manager con PagerDuty , devi prima creare un file segreto Gestione dei segreti AWS che contenga le tue PagerDuty credenziali. Per informazioni sull'aggiunta di una chiave API PagerDuty REST e altri dettagli obbligatori a un secret in Gestione dei segreti AWS, Archiviaz ione delle credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS consulta. Per informazioni sull'aggiunta di un PagerDuty servizio dal tuo PagerDuty account a un piano di risposta in Incident Manager, consulta i passaggi per l'integrazione di un PagerDuty servizio nel piano di risposta nell'argo mentoCreazione di un piano di risposta.

ServiceNow	Utilizzando AWS Service Management Connector, è possibile integrare Incident Manager con ServiceNowuna piattaforma di workflow di terze parti basata sul cloud. Dopo aver configurato l'integrazione con ServiceNow, quando si crea un nuovo incidente in Incident Manager, l'integrazione crea ServiceNow anche l'incidente in. Se si aggiorna un incidente in Incident Manager, apporta questi aggiornamenti all'incidente corrispondente in ServiceNow. Se si risolve un incidente in Incident Manager oppure ServiceNow, l'integra zione risolve l'incidente in entrambi i servizi in base alle preferenze configurate. Per ulteriori informazioni, consulta Integrati ng Strumento di gestione degli incidenti AWS Systems Manager in ServiceNow nella Administrator Guide.AWS Service Management Connector
Slack	Slackfornisce strumenti collaborativi basati sul cloud per la messaggistica di gruppo, le conferenze audio e video e la condivisione di file. Puoi integrare un Slack canale nelle tue operazioni di Incident Manager creando un canale di chat per Slack Amazon Q Developer nelle applicazioni di chat e quindi aggiungendo quel canale a un piano di risposta. Per ulteriori informazioni, consulta Creazione e integrazione di canali di chat per i soccorritori in Incident Manager.

Terraform	HashiCorp Terraform è uno strumento software open source di infrastructure as code (IaC) che fornisce un flusso di lavoro con interfaccia a riga di comando (CLI) per gestire vari servizi cloud. Per Incident Manager, puoi utilizzare Terraform per gestire o fornire quanto segue: Risorse per i contatti di SSM Incident Manager • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Fonti di dati SSM Contacts • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Risorse SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Fonti di dati SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Archiviazione delle credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS

Dopo aver attivato l'integrazione con PagerDuty for a response plan, Incident Manager funziona nei seguenti modi: PagerDuty

- Incident Manager crea un incidente corrispondente PagerDuty quando si crea un nuovo incidente in Incident Manager.
- Il flusso di lavoro di paging e le politiche di escalation create PagerDuty vengono utilizzate nell'ambiente. PagerDuty Tuttavia, Incident Manager non importa la configurazione. PagerDuty
- Incident Manager pubblica gli eventi della cronologia come note sull'incidente in PagerDuty, fino a un massimo di 2.000 note.
- È possibile scegliere di risolvere automaticamente PagerDuty gli incidenti quando si risolve l'incidente correlato in Incident Manager.

Per integrare Incident Manager con PagerDuty, devi prima creare un file segreto Gestione dei segreti AWS che contenga PagerDuty le tue credenziali. Questi consentono a Incident Manager di comunicare con il PagerDuty servizio dell'utente. È quindi possibile includere un PagerDuty servizio nei piani di risposta creati in Incident Manager.

Questo segreto creato in Secrets Manager deve contenere, nel formato JSON corretto, quanto segue:

- Una chiave API dal tuo PagerDuty account. Puoi utilizzare una chiave API REST di accesso generale o una chiave API REST con token utente.
- Un indirizzo email utente valido del tuo PagerDuty sottodominio.
- L'area PagerDuty di servizio in cui hai distribuito il sottodominio.

> **Note**
>
> Tutti i servizi in un PagerDuty sottodominio vengono distribuiti nella stessa area di servizio.

Prerequisiti

Prima di creare il segreto in Secrets Manager, assicuratevi di soddisfare i seguenti requisiti.

Chiave KMS

È necessario crittografare il segreto creato con una chiave gestita dal cliente creata in AWS Key Management Service (AWS KMS). Specificate questa chiave quando create il segreto che memorizza le vostre PagerDuty credenziali.

> **Important**
>
> Secrets Manager offre la possibilità di crittografare il segreto con una Chiave gestita da AWS, ma questa modalità di crittografia non è supportata.

La chiave gestita dal cliente deve soddisfare i seguenti requisiti:

- Tipo di chiave: scegli Symmetric.
- Utilizzo della chiave: scegli Crittografa e decrittografa.
- Regionalità: se desideri replicare il tuo piano di risposta su più livelli Regioni AWS, assicurati di selezionare la chiave multiregionale.

Policy della chiave

L'utente che sta configurando il piano di risposta deve disporre dell'autorizzazione per `kms:GenerateDataKey` e `kms:Decrypt` nella politica basata sulle risorse della chiave. Il responsabile del `ssm-incidents.amazonaws.com` servizio deve disporre dell'autorizzazione per `kms:GenerateDataKey` e `kms:Decrypt` nella politica basata sulle risorse della chiave.

La seguente politica illustra queste autorizzazioni. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Per informazioni sulla creazione di una nuova chiave gestita dal cliente, consulta Creazione di chiavi KMS con crittografia simmetrica nella Guida per gli sviluppatori.AWS Key Management Service Per ulteriori informazioni sulle AWS KMS chiavi, consulta i concetti.AWS KMS

Se una chiave gestita dal cliente esistente soddisfa tutti i requisiti precedenti, puoi modificarne la politica per aggiungere queste autorizzazioni. Per informazioni sull'aggiornamento della politica in una chiave gestita dal cliente, consulta Modifica di una politica chiave nella Guida per gli AWS Key Management Service sviluppatori.

> **Tip**
>
> È possibile specificare una chiave condizionale per limitare ulteriormente l'accesso. Ad esempio, la seguente politica consente l'accesso tramite Secrets Manager solo nella regione Stati Uniti orientali (Ohio) (us-east-2):
>
> ```
> {
>     "Sid": "Enable IM Permissions",
>     "Effect": "Allow",
>     "Principal": {
>         "Service": "ssm-incidents.amazonaws.com"
>     },
>     "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
>     "Resource": "*",
>     "Condition": {
>         "StringEquals": {
>             "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
>         }
>     }
> }
> ```

`GetSecretValue`autorizzazione

L'identità IAM (utente, ruolo o gruppo) che crea il piano di risposta deve disporre dell'autorizzazione IAM`secretsmanager:GetSecretValue`.

Per archiviare le credenziali di PagerDuty accesso in un luogo segreto Gestione dei segreti AWS

1. Segui i passaggi del Passaggio 3a in Creare un Gestione dei segreti AWS segreto nella Guida per l'Gestione dei segreti AWS utente.
2. Per il passaggio 3b, per le coppie chiave/valore, procedi come segue:
   - Scegliete la scheda Plaintext.
   - Sostituisci il contenuto predefinito della casella con la seguente struttura JSON:

     ```
     {
         "pagerDutyToken": "pagerduty-token",
         "pagerDutyServiceRegion": "pagerduty-region",
         "pagerDutyFromEmail": "pagerduty-email"
     ```

```
}
```

- Nell'esempio JSON che hai incollato, sostituisci quanto segue*placeholder values*:
  - *pagerduty-token*: Il valore di una chiave API REST di accesso generale o di una chiave API REST del token utente del tuo PagerDuty account.

    Per informazioni correlate, consulta API Access Keys nella PagerDuty Knowledge Base.
  - *pagerduty-region*: l'area di servizio del PagerDuty data center che ospita il PagerDuty sottodominio.

    Per informazioni correlate, vedere Regioni di servizio nella PagerDuty Knowledge Base.
  - *pagerduty-email*: L'indirizzo e-mail valido per un utente che appartiene al PagerDuty sottodominio.

    Per informazioni correlate, vedere Gestire gli utenti nella PagerDuty Knowledge Base.

  L'esempio seguente mostra un segreto JSON completato contenente le PagerDuty credenziali richieste:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. Nel passaggio 3c, per la chiave di crittografia, scegliete una chiave gestita dal cliente che avete creato che soddisfi i requisiti elencati nella precedente sezione Prerequisiti.
4. Nel passaggio 4c, per le autorizzazioni relative alle risorse, procedi come segue:
   - Espandi le autorizzazioni per le risorse.
   - Scegli Modifica autorizzazioni.
   - Sostituisci il contenuto predefinito della policy box con la seguente struttura JSON:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
```

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

- Scegli Save (Salva).

5. Nel passaggio 4d, per Replicate secret, procedi come segue se il piano di risposta è stato replicato su più di uno: Regione AWS
   - Espandi Replicate secret.
   - Per Regione AWS, seleziona la regione in cui hai replicato il tuo piano di risposta.
   - Per la chiave di crittografia, scegli una chiave gestita dal cliente che hai creato o replicato in questa regione che soddisfi i requisiti elencati nella sezione Prerequisiti.
   - Per ogni area aggiuntiva Regione AWS, scegli Aggiungi regione e seleziona il nome della regione e la chiave gestita dal cliente.
6. Completa i passaggi rimanenti in Creare un Gestione dei segreti AWS segreto nella Guida Gestione dei segreti AWS per l'utente.

Per informazioni su come aggiungere un PagerDuty servizio a un flusso di lavoro relativo agli incidenti di Incident Manager, vedi Integrazione di un PagerDuty servizio nel piano di risposta nell'argomentoCreazione di un piano di risposta.

Informazioni correlate

Come automatizzare la risposta agli incidenti con PagerDuty and Strumento di gestione degli incidenti AWS Systems Manager(blogCloud AWS Operations and Migrations)

Crittografia segreta Gestione dei segreti AWS nella Guida per l'utente Gestione dei segreti AWS

Risoluzione dei problemi AWS di Systems Manager Incident Manager

Se riscontri problemi durante l'utilizzo di AWS Systems Manager Incident Manager, puoi utilizzare le seguenti informazioni per risolverli secondo le nostre best practice. Se i problemi riscontrati non rientrano nell'ambito delle seguenti informazioni o se persistono dopo aver cercato di risolverli, contatta Supporto AWS.

Argomenti

Messaggio di errore: `ValidationException – We were unable to validate the Gestione dei segreti AWS secret`

Problema 1: l'identità AWS Identity and Access Management (IAM) (utente, ruolo o gruppo) che crea il piano di risposta non dispone dell'autorizzazione `secretsmanager:GetSecretValue` IAM. Le identità IAM devono disporre di questa autorizzazione per convalidare i segreti di Secrets Manager.

- Soluzione: aggiungi l'`secretsmanager:GetSecretValue`autorizzazione mancante alla policy IAM per l'identità IAM che crea il piano di risposta. Per informazioni, consulta Adding IAM identity permissions (console) o Adding IAM policies (AWS CLI) nella IAM User Guide.

Problema 2: al segreto non è associata una policy basata sulle risorse che consenta all'identità IAM di eseguire l'`GetSecretValue`azione, oppure la policy basata sulle risorse nega l'autorizzazione all'identità.

- Soluzione: crea o aggiungi una `Allow` dichiarazione alla policy basata sulle risorse del segreto che conceda l'autorizzazione all'identità IAM. `secrets:GetSecretValue` Oppure, se utilizzi un'`Deny`istruzione che include l'identità IAM, aggiorna la policy in modo che l'identità possa eseguire l'azione. Per informazioni, consulta Allegare una politica di autorizzazioni a un Gestione dei segreti AWS segreto nella Guida per l'Gestione dei segreti AWS utente.

Problema 3: a The secret non è allegata una policy basata sulle risorse che consenta l'accesso al servizio principale di Incident Manager,. `ssm-incidents.amazonaws.com`

- Soluzione: crea o aggiorna la politica basata sulle risorse per il segreto e includi la seguente autorizzazione:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Problema 4: la chiave gestita dal cliente AWS KMS key selezionata per crittografare il segreto non è una chiave gestita dal cliente, oppure la chiave gestita dal cliente selezionata non fornisce le autorizzazioni IAM `kms:Decrypt` e `kms:GenerateDataKey*` al responsabile del servizio Incident Manager. In alternativa, l'identità IAM che crea il piano di risposta potrebbe non disporre dell'autorizzazione IAM. `GetSecretValue`

- Soluzione: assicurati di soddisfare i requisiti descritti nella sezione Prerequisiti dell'argomento. Archiviazione delle credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS

Problema 5: l'ID del segreto che contiene la chiave API REST di accesso generale o la chiave API REST del token utente non è valido.

- Soluzione: assicurati di aver inserito l'ID del segreto di Secrets Manager in modo accurato, senza spazi finali. È necessario lavorare nella stessa in Regione AWS cui è memorizzato il segreto che si desidera utilizzare. Non puoi usare un segreto eliminato.

Problema 6: in rari casi, il servizio Secrets Manager potrebbe riscontrare un problema o Incident Manager potrebbe avere problemi di comunicazione con esso.

- Soluzione: attendi qualche minuto, quindi riprova. Verifica la presenza di AWS Health Dashboardeventuali problemi che potrebbero influire su entrambi i servizi.

Altre questioni relative alla risoluzione dei problemi

Se i passaggi precedenti non hanno risolto il problema, puoi trovare ulteriore assistenza nelle seguenti risorse:

- Per i problemi IAM specifici relativi a Incident Manager quando accedi alla console Incident Manager, consultaRisoluzione dei problemi di Strumento di gestione degli incidenti AWS Systems Manager identità e accesso.
- Per problemi generali di autenticazione e autorizzazione quando accedi a Console di gestione AWS, consulta Risoluzione dei problemi di IAM nella Guida per l'utente IAM

Cronologia dei documenti per Incident Manager

Modifica	Descrizione	Data
Strumento di gestione degli incidenti AWS Systems Manager documenti di migrazione pubblicati	Incident Manager ha pubblicato documenti sulla migrazione per aiutare i clienti a comprendere alcune delle opzioni disponibili per la migrazione. Strumento di gestione degli incidenti AWS Systems Manager Per ulteriori informazioni, consulta Modifica della Strumento di gestione degli incidenti AWS Systems Manager disponibilità.	21 novembre 2025
Aggiornamento della politica gestita `AWSIncidentManagerResolverAccess`	Incident Manager ha aggiornato la policy gestita `AWSIncidentManagerResolverAccess` per aggiungere ssm-contacts: StartEngagement autorizzazione per avviare interazioni con i contatti durante gli incidenti. Per ulteriori informazioni, consulta Incident Manager: aggiornamenti alle politiche gestite. AWS	20 novembre 2025
Strumento di gestione degli incidenti AWS Systems Manager non è più aperto a nuovi clienti.	Strumento di gestione degli incidenti AWS Systems Manager non è più aperto a nuovi clienti. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, vedi	7 novembre 2025

	modifica della Strumento di gestione degli incidenti AWS Systems Manager disponibilità.	
Strumento di gestione degli incidenti AWS Systems Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025.	Strumento di gestione degli incidenti AWS Systems Manager non sarà più aperto a nuovi clienti a partire dal 7 novembre 2025. Se desideri utilizzare Incident Manager, registrati prima di tale data. I clienti esistenti possono continuare a utilizzare il servizio normalmente. Per ulteriori informazioni, consulta Modifica della Strumento di gestione degli incidenti AWS Systems Manager disponibilità.	7 ottobre 2025

Modifica dei requisiti di autorizzazione per la creazione manuale degli incidenti	Le autorizzazioni IAM richieste a un utente per creare manualmente un incidente sono cambiate e non utilizzano più un ruolo collegato al servizio. Invece, Incident Manager ora utilizza le sessioni di accesso inoltrato (FAS) per le chiamate `ssm-contacts:StartEngagement` come parte di. `ssm-incidents:StartIncident` Per ulteriori informazioni, consulta Autorizzazioni IAM richieste per l'avvio manuale degli incidenti.	10 giugno 2025
Aggiornamento della politica gestita `AWSServiceRoleforIncidentManagerPolicy`	Incident Manager ha aggiunto una nuova autorizzazione `AWSServiceRoleforIncidentManagerPolicy` che consente a Incident Manager di pubblicare le metriche all'interno del `AWS/Usage` namespace nel tuo account. Per ulteriori informazioni, consulta Incident Manager: aggiornamenti alle AWS politiche gestite.	28 gennaio 2025

Aggiornamento della politica gestita `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Incident Manager ha aggiunto una nuova autorizzazione a `AWSIncidentManagerIncidentAccessServiceRolePolicy` , a supporto della funzione Findings, che consente di verificare se un' EC2 istanza fa parte di un gruppo Auto Scaling. Per ulteriori informazioni, consulta gli aggiornamenti di Incident Manager alle politiche AWS gestite.	20 febbraio 2024
Supporto HashiCorp Terraform aggiuntivo: rotazioni su chiamata	Terraform ha aggiunto il supporto per Incident Manager. Ora puoi fornire o gestire le risorse su chiamata di Incident Manager utilizzando Terraform. Per informazioni su questa e altre integrazioni di terze parti con Incident Manager, vedi Integrazione con altri prodotti e servizi.	2 febbraio 2024

Nuova funzionalità: risultati tratti da altri Servizi AWS	I risultati forniscono informazioni sulle modifiche relative agli AWS CloudFormation stack e alle AWS CodeDeploy implementazioni avvenute più o meno nello stesso periodo in cui è stato creato un incidente in Incident Manager. Nella console Incident Manager, è possibile visualizzare informazioni di riepilogo su tali modifiche e, in molti casi, accedere ai collegamenti alle CodeDeploy console CloudFormation or per informazioni complete sulla modifica. I risultati riducono il tempo necessario per valutare le potenziali cause degli incidenti. Riducono inoltre le possibilità che i soccorritori accedano all'account o alla console sbagliati per indagare sulla causa di un incidente. Questa funzionalità introduce anche una nuova politica gestita`AWSIncidentManagerIncidentAccessServiceRolePolicy` , che consente a Incident Manager di leggere le risorse di altri siti Servizi AWS per identificare i risultati relativi agli incidenti. Per ulteriori informazioni, consulta i seguenti argomenti:	15 novembre 2023

	• Lavorare con i risultati • AWS politica gestita: AWSIncidentManagerIncidentAccessServiceRolePolicy	
Elenchi aggiornati di integrazioni con Incident Manager	L'argomento Integrazioni di prodotti e servizi con Incident Manager è stato ampliato per elencare e descrivere tutti gli Servizi AWS strumenti, anche di terze parti, che è possibile integrare con Incident Manager nelle operazioni di rilevamento e risposta agli incidenti.	9 giugno 2023

Integrazione con AWS Trusted Advisor	Trusted Advisor ora verifica che la configurazione di un set di replica ne utilizzi più di uno Regione AWS per supportar e il failover e la risposta regionali. Per gli incidenti creati da CloudWatch allarmi o EventBridge eventi, Incident Manager crea un incidente uguale Regione AWS alla regola di allarme o evento. Se Incident Manager non è temporaneamente disponibi le in tale regione, il sistema tenta di creare un incidente in un'altra regione nel set di repliche. Se il set di repliche include solo una regione, qualora Incident Manager non fosse disponibile, il sistema non è in grado di creare un record di incidente. Per evitare questa situazione, Trusted Advisor segnala quando un set di replica è configurato per una sola regione. Per informazioni sull'utilizzo di Trusted Advisor, AWS Trusted Advisorconsultat e la Guida per l'Supporto AWS utente.	28 aprile 2023

Microsoft TeamsUtilizzalo come canale di chat nei piani di risposta	Grazie all'integrazione con Microsoft Teams Amazon Q Developer nelle applicazioni di chat, ora puoi utilizzare Microsoft Teams il canale di chat nei tuoi piani di risposta. Ciò si aggiunge al supporto per i canali Slack di chat di Amazon Chime. Durante un incidente, Incident Manager invia notifiche di stato direttamente a un canale di chat per tenere informati tutti i soccorritori. I soccorritori possono anche comunicare tra loro e utilizzare AWS CLI i comandi relativi agli incidenti nell'Microsoft Teamsapplicazione per aggiornare e interagire con gli incidenti. Per ulteriori informazioni, consulta Utilizzo dei canali di chat in Incident Manager.	4 aprile 2023

Nuova funzionalità: orari delle chiamate	Una pianificazione delle chiamate in Incident Manager definisce chi riceve una notifica quando si verifica un incidente che richiede l'intervento dell'operatore. Una pianificazione di chiamata consiste in una o più rotazioni create dall'utente per la pianificazione. Ogni rotazione può includere fino a 30 contatti. Dopo aver creato un programma di chiamata, puoi includerlo come intensifi cazione nel tuo piano di escalation. Quando si verifica un incidente associato a quel piano di escalation, Incident Manager avvisa l'operatore (o gli operatori) che sono in servizio in base alla pianifica zione. Per ulteriori informazi oni, vedere Utilizzo degli orari di chiamata in Incident Manager.	28 marzo 2023

Stampa un'analisi degli incidenti formattata o salvala come PDF	La pagina di analisi degli incidenti ora include un pulsante Stampa per generare una versione dell'analisi formattata per la stampa. Utilizzando le destinazioni di stampa configurate per il dispositivo, è possibile salvare l'analisi degli incidenti come PDF o inviarla a una stampante locale o di rete. Per ulteriori informazioni, consulta Stampare un'analisi formattata degli incidenti.	17 gennaio 2023
PagerDuty integrazione: Incident Manager ora copia gli eventi della cronologia degli incidenti negli incidenti PagerDuty	Quando si attiva l'integrazione con PagerDuty un piano di risposta, Incident Manager aggiunge gli eventi cronologici creati da quel piano al record dell'incidente corrispondente in. PagerDuty PagerDuty aggiunge gli eventi della sequenza temporale come note sull'incidente, fino a un massimo di 2.000 note. Per ulteriori informazioni su queste modifiche, consulta i seguenti argomenti: • Archivia le credenziali di PagerDuty accesso in un luogo segreto Gestione dei segreti AWS • Integra un PagerDuty servizio nel piano di risposta	15 dicembre 2022

Integrazione di Incident Manager con le CloudWatch metriche.	Ora puoi pubblicare le metriche relative agli incidenti in. CloudWatch Per ulteriori informazioni, consulta le metriche. CloudWatch AWSIncidentManagerServiceRolePolicy Ha incluso un'autorizzazione aggiuntiva per consentire al nostro servizio di pubblicare metriche per tuo conto.	15 dicembre 2022
Ha avviato le note sull'incidente e aggiornato la schermata dei dettagli dell'incidente	Puoi collaborare e comunicare con altri utenti che lavorano su un incidente utilizzando le note sull'incidente. Inoltre, puoi visualizzare gli stati dei runbook e degli impegni dalla schermata Dettagli dell'incidente. Per ulteriori informazioni, consulta Dettagli sull'incidente.	16 novembre 2022

Integra i piani di PagerDuty escalation e i flussi di lavoro di paging nei piani di risposta di Incident Manager	Ora puoi integrare Incident Manager PagerDuty e aggiungere un PagerDuty servizio a un piano di risposta. Dopo aver configurato l'integrazione, Incident Manager può creare un incidente corrispondente PagerDuty per ogni nuovo incidente creato in Incident Manager. PagerDuty utilizza il flusso di lavoro di paging e le politiche di escalation definite nell'ambiente. PagerDuty Per ulteriori informazioni, consulta i seguenti argomenti: • Integrazioni di prodotti e servizi con Incident Manager • Archivia le credenziali di PagerDuty accesso in modo segreto Gestione dei segreti AWS • Integra un PagerDuty servizio nel piano di risposta dell'argomento Creazione di un piano di risposta • Risoluzione dei problemi	16 novembre 2022

Ha avviato le note sull'incidente e ha aggiornato la schermata dei dettagli dell'incidente.	Puoi collaborare e comunicare con altri utenti che lavorano su un incidente utilizzando le note sull'incidente. Inoltre, puoi visualizzare gli stati dei runbook e degli impegni dalla schermata Dettagli dell'incidente. Per ulteriori informazioni, consulta Dettagli sull'incidente.	16 novembre 2022
Supporto per l'etichettatura dei set di replica	È ora possibile assegnare tag al set di replica in. Strumento di gestione degli incidenti AWS Systems Manager Ciò si aggiunge al supporto esistente per l'assegnazione di tag ai piani di risposta, ai record degli incidenti e ai contatti Regioni AWS specificati nel set di replica. Per informazioni, consultare gli argomenti seguenti: • Preparati alla procedura guidata • Etichettatura delle risorse di Incident Manager	2 novembre 2022

Integrazione di Incident Manager con Atlassian Jira Service Management	Puoi integrare Incident Manager con Jira Service Management utilizzando il Service Management Connector per Jira AWS Service Management. Dopo aver configurato l'integrazione, i nuovi incidenti creati in Incident Manager creano un incidente corrispondente in Jira. Se aggiorni un incidente in Incident Manager, gli aggiornamenti vengono aggiunti all'incidente corrispondente in Jira. Se risolvi un incidente in Incident Manager o Jira, viene risolto anche l'incidente corrispondente, in base alle preferenze configurate. Per ulteriori informazioni, consulta Configurazione di Jira Service Management nella Guida per l'amministratore di AWS Service Management Connector.	6 ottobre 2022

Supporto avanzato per l'etichettatura	Incident Manager supporta l'assegnazione di tag ai piani di risposta, ai record degli incidenti e ai contatti nel modo Regioni AWS specificato nel set di replica. Incident Manager supporta anche l'assegnazione automatica di tag agli incidenti creati dai piani di risposta. Per ulteriori informazioni, vedere Etichettatura delle risorse di Incident Manager.	28 giugno 2022

Integrazione di Incident Manager con ServiceNow	È possibile integrare Incident Manager con ServiceNow utilizzando il AWS Service Management Connector per ServiceNow. Dopo aver configurato l'integrazione, i nuovi incidenti creati in Incident Manager creano un incidente corrispondente in ServiceNow. Se si aggiorna un incidente in Incident Manager, gli aggiornamenti vengono aggiunti all'incidente corrispondente in ServiceNow. Se si risolve un incidente in Incident Manager oppure ServiceNow, viene risolto anche l'incidente corrispondente, in base alle preferenze configurate. Per ulteriori informazioni, vedere Integrazione di AWS Systems Manager Incident Manager in ServiceNow.	9 giugno 2022

Importa i dettagli di contatto	Quando viene creato un incidente, Incident Manager può avvisare i soccorritori utilizzando notifiche vocali o SMS. Per garantire che i soccorritori vedano che la chiamata o la notifica SMS proviene da Incident Manager, consigliamo a tutti i soccorritori di scaricare il file in formato scheda virtuale (.vcf) di Incident Manager nella rubrica dei propri dispositivi mobili. Per ulteriori informazi oni, consulta Importare i dati di contatto nella rubrica.	18 maggio 2022

Molteplici miglioramenti delle funzionalità per migliorare la creazione e la risoluzione degli incidenti	Incident Manager ha introdotto i seguenti miglioramenti delle funzionalità per migliorare la creazione e la risoluzione degli incidenti: • Crea automaticamente incidenti in altro Regioni AWS: nel caso in cui Incident Manager non sia disponibile in un Regione AWS momento in cui Amazon CloudWatch o Amazon EventBridge creano un incidente, questi servizi ora creano automatic amente l'incidente in una delle regioni disponibili specificate nel set di replica. Per ulteriori informazioni, consulta Gestione degli incidenti tra regioni. • Compila automaticamente i parametri del runbook con i metadati degli incidenti : ora puoi configurare Incident Manager per raccogliere informazioni sulle AWS risorse dagli incidenti. Incident Manager può quindi compilare i parametri del runbook con le informazioni raccolte. Per ulteriori informazioni, vedere Tutorial: Using Systems Manager Automation	17 maggio 2022

	runbook with Incident Manager. • Raccolta automatica di informazioni sulle AWS risorse: quando il sistema crea un incidente, Incident Manager ora raccoglie automaticamente le informazioni sulle AWS risorse coinvolte nell'incidente. Incident Manager aggiunge quindi queste informazioni alla scheda Elementi correlati.	
Supporto per più runbook	Incident Manager ora supporta l'esecuzione di più runbook durante un incidente per la pagina dei dettagli dell'incidente.	14 gennaio 2022
Incident Manager è stato lanciato nel nuovo Regioni AWS	Incident Manager è ora disponibile nelle nuove regioni: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 e eu-west-3. Per ulteriori informazioni sulle regioni e sulle Riferimenti generali di AWS quote di Incident Manager, consulta la guida di riferimento.	8 novembre 2021
Riconoscimento del coinvolgimento della console	Ora puoi confermare gli impegni direttamente dalla console Incident Manager.	5 agosto 2021

Scheda Proprietà	Incident Manager ha introdotto una scheda delle proprietà nella pagina dei dettagli dell'incidente, che fornisce ulteriori informazioni sugli incidenti, sull'elemento principale OpsItem e sulla relativa analisi post-incidente.	3 agosto 2021
Avvio di Incident Manager	Incident Manager è una console di gestione degli incidenti progettata per aiutare gli utenti a mitigare e ripristinare gli incidenti che interessano le applicazioni AWS ospitate.	10 maggio 2021