aws

User Guide

Incident Manager

Incident Manager: User Guide

Table of Contents

Was ist AWS Systems Manager Incident Manager?

Incident Manager, eine Funktion vonAWS Systems Manager, soll Ihnen helfen, Vorfälle, die Ihre Anwendungen betreffen, auf AWS denen gehostet wird, zu minimieren und diese zu beheben.

Im Zusammenhang mit ist ein Vorfall jede ungeplante Unterbrechung oder Verringerung der Servicequalität, die erhebliche Auswirkungen auf den Geschäftsbetrieb haben kann. AWS Daher ist es für Unternehmen von entscheidender Bedeutung, eine Reaktionsstrategie zu entwickeln, um Vorfälle effizient zu mindern und zu beheben, und Maßnahmen zur Verhinderung future Vorfälle zu ergreifen.

Incident Manager trägt dazu bei, die Zeit für die Behebung von Vorfällen zu verkürzen, und zwar durch:

- Bereitstellung automatisierter Pläne zur effizienten Einbindung der Personen, die für die Reaktion auf die Vorfälle verantwortlich sind.
- Bereitstellung relevanter Daten zur Fehlerbehebung.
- Aktivierung automatisierter Antwortaktionen mithilfe vordefinierter Automatisierungs-Runbooks.
- Bereitstellung von Methoden für die Zusammenarbeit und Kommunikation mit allen Beteiligten.

Die in Incident Manager integrierten Funktionen und Workflows basieren auf den Best Practices für die Reaktion auf Vorfälle, die Amazon fast seit seiner Gründung entwickelt hat. Incident Manager lässt sich in Amazon CloudWatch, AWS CloudTrailAWS Systems Manager, und Amazon integrieren EventBridge. AWS-Services

Hauptkomponenten und Funktionen

In diesem Abschnitt werden die Funktionen von Incident Manager beschrieben, mit denen Sie Ihre Pläne zur Reaktion auf Vorfälle einrichten.

Reaktionsplan

Ein Reaktionsplan dient als Vorlage, die definiert, was bei einem Vorfall vorhanden sein muss. Er enthält Informationen wie:

- Wer muss reagieren, wenn ein Vorfall eintritt.
- Die etablierte automatisierte Reaktion zur Minderung des Vorfalls.

- Das Kollaborationstool, das Einsatzkräfte verwenden müssen, um zu kommunizieren und automatische Benachrichtigungen über den Vorfall zu erhalten.

Erkennung von Vorfällen

Sie können CloudWatch Amazon-Alarme und EventBridge Amazon-Ereignisse so konfigurieren, dass Vorfälle ausgelöst werden, wenn Bedingungen oder Änderungen erkannt werden, die sich auf Ihre AWS Ressourcen auswirken.

Unterstützung für Runbook-Automatisierung

Sie können Automation-Runbooks von Incident Manager aus initiieren, um Ihre kritische Reaktion auf Vorfälle zu automatisieren und Ersthelfern detaillierte Schritte zur Verfügung zu stellen.

Engagement und Eskalation

Ein Einsatzplan sieht vor, dass jeder bei jedem einzelnen Vorfall benachrichtigt wird. Sie können einzelne Kontakte angeben, die Sie zu Incident Manager hinzugefügt haben, oder einen Bereitschaftsdienst angeben, den Sie in Incident Manager erstellt haben. In den Einsatzplänen ist auch ein Eskalationspfad festgelegt, um sicherzustellen, dass die Beteiligten für Transparenz sorgen und aktiv am Prozess der Reaktion auf Vorfälle teilnehmen.

Zeitpläne für Bereitschaftsdienste

Ein Bereitschaftsdienst in Incident Manager besteht aus einer oder mehreren Rotationen, die Sie für den Zeitplan erstellen. Für jede Rotation können Sie bis zu 30 Kontakte einbeziehen. Wenn der Bereitschaftsdienst zu einem Eskalations- oder Reaktionsplan hinzugefügt wird, legt er fest, wer benachrichtigt wird, wenn ein Vorfall eintritt, der das Eingreifen eines Einsatzmitarbeiters erfordert. Bereitschaftszeiten stellen sicher, dass Sie rund um die Uhr über eine vollständige, redundante Abdeckung verfügen, die für Ihre Reaktion auf Vorfälle erforderlich ist.

Aktive Zusammenarbeit

Incident Responder reagieren aktiv auf Vorfälle, indem sie eng mit dem AWS Chatbot Kunden zusammenarbeiten. AWS Chatbotunterstützt die Erstellung von Chat-Kanälen für Incident Manager SlackMicrosoft Teams, die Amazon Chime verwenden. Einsatzkräfte können direkt miteinander kommunizieren, automatische Benachrichtigungen über Vorfälle erhalten und einige Incident Microsoft Teams Manager-Befehlszeilenschnittstellen (CLI) Slack -Operationen direkt ausführen.

Diagnose von Vorfällen

Einsatzkräfte können während eines Vorfalls up-to-date Informationen in der Incident Manager-Konsole einsehen. Auf der Grundlage der Änderungen an den Informationen können die

Einsatzkräfte dann Folgeelemente erstellen und diese mithilfe von Automation-Runbooks beheben.

Erkenntnisse aus anderen Diensten

Um die Diagnose von Vorfällen durch Einsatzkräfte zu unterstützen, können Sie die Funktion „Ergebnisse“ in Incident Manager aktivieren. Bei den Ergebnissen handelt es sich um Informationen über AWS CodeDeploy Bereitstellungen und AWS CloudFormation Stack-Aktualisierungen, die ungefähr zum Zeitpunkt eines Vorfalls stattfanden und an denen eine oder mehrere Ressourcen beteiligt waren, die wahrscheinlich mit dem Vorfall zu tun hatten. Mit diesen Informationen wird der Zeitaufwand für die Bewertung potenzieller Ursachen reduziert, wodurch sich die mittlere Wiederherstellungszeit (MTTR) nach einem Vorfall verringern kann.

Analyse nach dem Vorfall

Nach der Behebung eines Vorfalls ermitteln Sie anhand einer Analyse nach dem Vorfall Verbesserungen bei der Reaktion auf den Vorfall, einschließlich der Zeit bis zur Erkennung und Behebung des Vorfalls. Eine Analyse kann Ihnen auch dabei helfen, die Ursache der Vorfälle zu verstehen. Incident Manager erstellt empfohlene Folgemaßnahmen, anhand derer Sie Ihre Reaktion auf Vorfälle verbessern können.

Vorteile der Verwendung von Incident Manager

Erfahren Sie mehr über die Vorteile des Einsatzes von Incident Manager bei der Erkennung und Reaktion auf Vorfälle.

In diesem Abschnitt werden die Vorteile beschrieben, die Ihr Unternehmen durch die Implementierung eines Incident Manager-Reaktionsplans erzielen kann.

Diagnostizieren Sie Probleme effizient und sofort

CloudWatch Amazon-Alarme und EventBridge Amazon-Ereignisse, die Sie konfigurieren, können automatisch Vorfälle auslösen, wenn es zu ungeplanten Unterbrechungen oder Qualitätseinbußen Ihrer Services kommt.

CloudWatch Alarme erkennen und melden, wenn sich der Wert der Metrik oder des Ausdrucks relativ zu einem Schwellenwert über mehrere Zeiträume ändert. EventBridge Ereignisse entstehen als Ergebnis einer Änderung in einer Umgebung, Anwendung oder einem Dienst, die Sie in einer EventBridge Regel angegeben haben. Wenn Sie einen Alarm oder ein Ereignis erstellen, können Sie eine Aktion für einen Vorfall, der in Incident Manager erstellt werden soll, und den entsprechenden Reaktionsplan angeben, um die Bearbeitung, Eskalation und Minderung des Vorfalls zu erleichtern.

Incident Manager bietet die Möglichkeit, mithilfe von Metriken automatisch die Metriken zu einem Vorfall zu sammeln und zu verfolgen. CloudWatch Zusätzlich zu den automatisierten Metriken, die für den Vorfall generiert werden, wenn er durch einen CloudWatch Alarm erstellt wird, können Sie Metriken manuell in Echtzeit hinzufügen, um den Einsatzkräften bei einem Vorfall zusätzlichen Kontext und zusätzliche Daten zur Verfügung zu stellen.

Verwenden Sie die Incident Manager-Incident-Zeitleiste, um interessante Punkte in chronologischer Reihenfolge anzuzeigen. Einsatzkräfte können die Zeitleiste auch verwenden, um benutzerdefinierte Ereignisse hinzuzufügen, um zu beschreiben, was sie getan haben oder was passiert ist. Zu den automatisierten Sonderzielen gehören:

- Ein CloudWatch Alarm oder eine EventBridge Regel verursacht einen Vorfall.
- Incident-Metriken werden an Incident Manager gemeldet.
- Die Einsatzkräfte sind engagiert.
- Die Runbook-Schritte wurden erfolgreich abgeschlossen.

Engagieren Sie sich effektiv

Incident Manager bringt Incident Responder mithilfe von Kontakten, Bereitschaftszeitplänen, Eskalationsplänen und Chat-Kanälen zusammen. Sie definieren einzelne Kontakte direkt im Incident Manager und legen Kontaktpräferenzen fest (E-Mail, SMS oder Telefonanruf). Sie fügen Kontakte zu den Rotationen auf Abruf hinzu, um zu bestimmen, wer in einem bestimmten Zeitraum mit der Bearbeitung von Vorfällen beauftragt wird. Anhand Ihrer definierten Ansprechpartner und Bereitschaftszeitpläne erstellen Sie Eskalationspläne, um die erforderlichen Einsatzkräfte zur richtigen Zeit während eines Vorfalls einzuschalten.

Arbeiten Sie in Echtzeit zusammen

Kommunikation während eines Vorfalls ist der Schlüssel zu einer schnelleren Lösung. Mithilfe eines für die Verwendung Slack von Amazon Chime eingerichteten AWS Chatbot Clients oder Amazon Chime können Sie die Einsatzkräfte in ihrem bevorzugten verbundenen Chat-Kanal zusammenbringen, wo sie direkt mit dem Vorfall und miteinander interagieren. Microsoft Teams Incident Manager zeigt auch die Aktionen der Incident-Responder in Echtzeit im Chat-Kanal an und bietet so anderen Kontext.

Automatisieren Sie die Servicewiederherstellung

Mit Incident Manager können sich Ihre Einsatzkräfte mithilfe von Automation-Runbooks auf die wichtigsten Aufgaben konzentrieren, die zur Behebung eines Vorfalls erforderlich sind. In Incident

Manager sind Runbooks eine vordefinierte Reihe von Aktionen, die zur Lösung eines Vorfalls ergriffen werden. Sie kombinieren die Leistungsfähigkeit automatisierter Aufgaben mit manuellen Schritten nach Bedarf, sodass die Einsatzkräfte besser zur Verfügung stehen, um die Auswirkungen zu analysieren und darauf zu reagieren.

future Vorfälle verhindern

Mithilfe der Incident-Manager-Analyse nach dem Vorfall kann Ihr Team robustere Reaktionspläne entwickeln und Änderungen in Ihren Anwendungen vornehmen, um future Vorfälle und Ausfallzeiten zu verhindern. Die Analyse nach einem Vorfall ermöglicht zudem iteratives Lernen und Verbessern von Runbooks, Reaktionsplänen und Kennzahlen.

Zugehörige Services

Incident Manager lässt sich in verschiedene Dienste AWS-Services und Tools von Drittanbietern integrieren, um Sie bei der Erkennung und Behebung von Vorfällen zu unterstützen, indirekt mit den API-Vorgängen zu interagieren und die Infrastruktur zu verwalten. Weitere Informationen finden Sie unter Produkt- und Serviceintegrationen mit Incident Manager.

Zugriff auf Incident Manager

Sie können auf jede der folgenden Arten auf Incident Manager zugreifen:

- Die Incident Manager-Konsole
- AWS CLI— Allgemeine Informationen finden Sie unter Erste Schritte mit dem AWS CLI im AWS Command Line InterfaceBenutzerhandbuch. Informationen zu CLI-Befehlen für Incident Manager finden Sie unter ssm-incidentsund ssm-contactsin der AWS CLIBefehlsreferenz.
- Incident Manager API — Weitere Informationen finden Sie in der AWS Systems Manager Incident ManagerAPI-Referenz.
- AWSSDKs — Weitere Informationen finden Sie unter Tools, auf AWS denen Sie aufbauen können.

Regionen und Kontingente für Incident Manager

Incident Manager wird nicht in allen von Systems Manager AWS-Regionen unterstützten Versionen unterstützt.

Informationen zu den Regionen und Kontingenten von Incident Manager finden Sie unter AWS Systems Manager Incident ManagerEndpunkte und Kontingente in der Allgemeine Amazon Web Services-Referenz.

Preise für Incident Manager

Die Nutzung von Incident Manager ist kostenpflichtig. Weitere Informationen finden Sie unter AWSSystems Manager Manager-Preise.

> **Note**
>
> Andere AWS-Services Inhalte und AWS Inhalte Dritter, die in Verbindung mit diesem Service zur Verfügung gestellt werden, können gesonderten Gebühren unterliegen und zusätzlichen Bedingungen unterliegen.

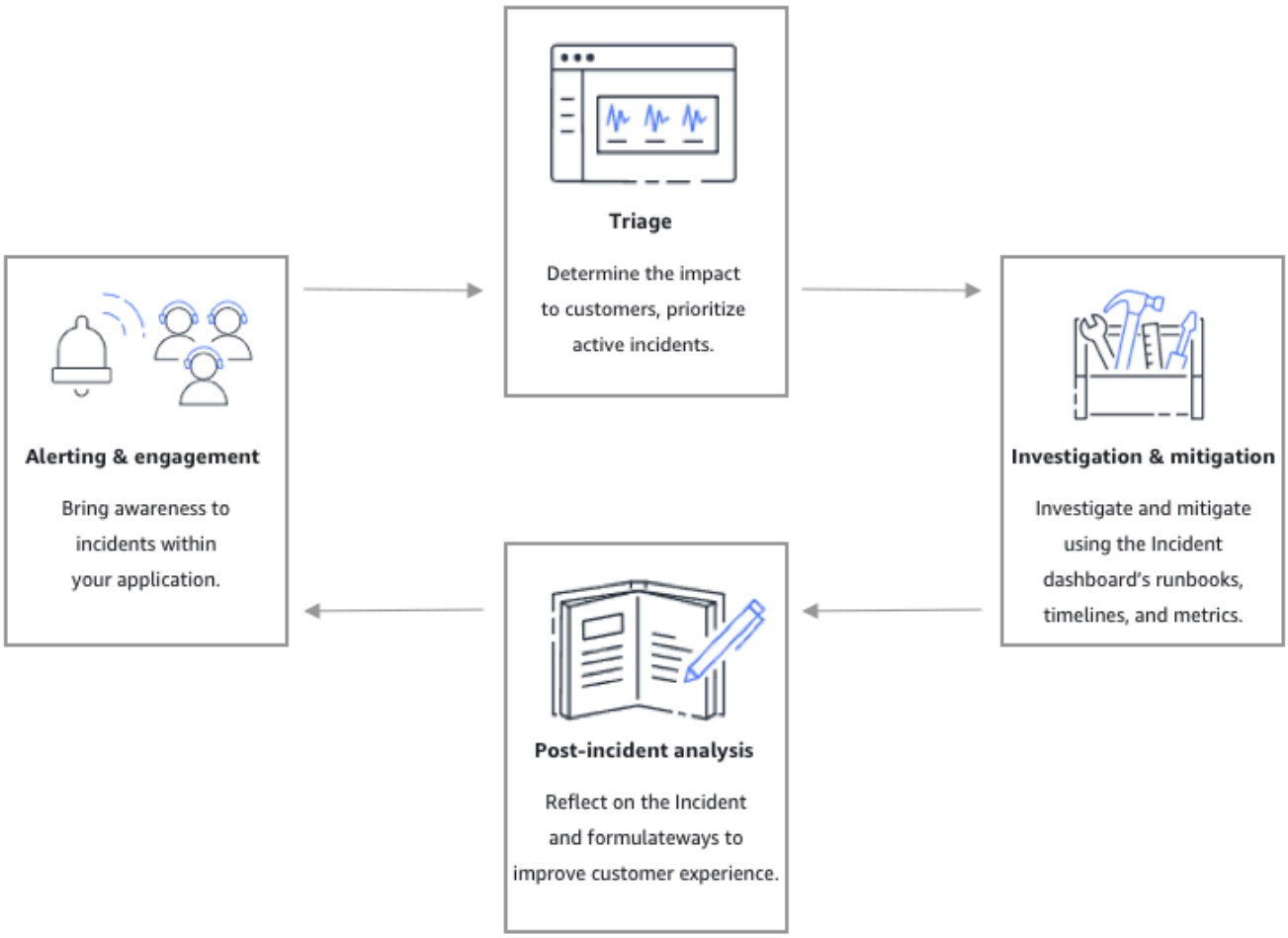
Eine Übersicht über einen ServiceTrusted Advisor, mit dem Sie die Kosten, die Sicherheit und die Leistung Ihrer AWS Umgebung optimieren können, finden Sie AWS Trusted Advisorim AWS SupportBenutzerhandbuch.

Der Incident-Lebenszyklus in Incident Manager

AWS Systems Manager Incident Managerbietet ein step-by-step Framework, das auf bewährten Verfahren basiert, um Vorfälle wie Serviceausfälle oder Sicherheitsbedrohungen zu identifizieren und darauf zu reagieren. Das Hauptaugenmerk von Incident Manager liegt darauf, die betroffenen Dienste oder Anwendungen mithilfe einer vollständigen Lösung für das Incident Lifecycle Management so schnell wie möglich wieder in den Normalzustand zu versetzen.

Incident Manager bietet Tools und bewährte Verfahren für jede Phase des Incident-Lebenszyklus:

- Alarmierung und Interaktion
- Triage
- Untersuchung und Schadensbegrenzung
- Analyse nach dem Vorfall



Alarmierung und Interaktion

In der Warn- und Interaktionsphase des Incident-Lebenszyklus liegt der Schwerpunkt darauf, das Bewusstsein für Vorfälle in Ihren Anwendungen und Diensten zu schärfen. Diese Phase beginnt, bevor ein Vorfall entdeckt wird, und erfordert ein tiefes Verständnis Ihrer Anwendungen. Sie können CloudWatchAmazon-Metriken verwenden, um Daten über die Leistung Ihrer Anwendungen zu überwachen, oder Amazon nutzen, EventBridge um Warnmeldungen aus verschiedenen Quellen, Anwendungen und Diensten zu aggregieren. Nachdem Sie die Überwachung für Ihre Anwendungen eingerichtet haben, können Sie damit beginnen, Benachrichtigungen über Kennzahlen zu senden, die von der historischen Norm abweichen. Weitere Informationen zu bewährten Methoden für die Überwachung finden Sie unter. Überwachen

Um die Diagnose von Vorfällen durch Einsatzkräfte zu unterstützen, können Sie die Funktion „Ergebnisse“ in Incident Manager aktivieren. Bei den Ergebnissen handelt es sich um Informationen

über AWS CodeDeploy Bereitstellungen und AWS CloudFormation Stack-Aktualisierungen, die ungefähr zum Zeitpunkt eines Vorfalls aufgetreten sind. Mit diesen Informationen wird der Zeitaufwand für die Bewertung potenzieller Ursachen reduziert, wodurch sich die mittlere Wiederherstellungszeit (MTTR) nach einem Vorfall verringern kann.

Nachdem Sie Ihre Anwendungen auf Vorfälle überwacht haben, können Sie einen Plan zur Reaktion auf Vorfälle definieren, der während eines Vorfalls verwendet werden soll. Weitere Informationen zum Erstellen von Reaktionsplänen finden Sie unterArbeiten mit Reaktionsplänen in Incident Manager. Amazon EventBridge Events oder CloudWatch Alarms können mithilfe von Reaktionsplänen als Vorlage automatisch einen Vorfall erstellen. Weitere Informationen zur Erstellung von Vorfällen finden Sie unterVorfälle im Incident Manager erstellen.

Reaktionspläne beinhalten entsprechende Eskalations- und Einsatzpläne, um Ersthelfer in den Vorfall einzubeziehen. Weitere Informationen zur Einrichtung von Eskalationsplänen finden Sie unter. Erstellen Sie einen Eskalationsplan AWS ChatbotInformiert die Einsatzkräfte gleichzeitig über einen Chat-Kanal und leitet sie zur Detailseite des Vorfalls weiter. Mithilfe des Chat-Kanals und der Vorfalldetails kann das Team mit einem Vorfall kommunizieren und ihn analysieren. Weitere Informationen zur Einrichtung von Chat-Kanälen in Incident Manager finden Sie unterAufgabe 2: Erstellen eines Chat-Kanals inAWS Chatbot.

Triage

Bei der Triage versuchen Ersthelfer, die Auswirkungen auf die Kunden zu ermitteln. Die Ansicht mit den Vorfalldetails in der Incident Manager-Konsole bietet den Einsatzkräften Zeitpläne und Kennzahlen, anhand derer sie den Vorfall beurteilen können. Die Bewertung der Auswirkungen eines Vorfalls bildet auch die Grundlage für die Reaktionszeit, die Lösung und die Kommunikation im Zusammenhang mit dem Vorfall. Die Einsatzkräfte priorisieren Vorfälle anhand von Folgenabstufungen von 1 (kritisch) bis 5 (keine Auswirkungen).

Ihr Unternehmen kann den genauen Umfang jeder Folgenabschätzung nach Ihren Wünschen festlegen. Die folgende Tabelle enthält Beispiele dafür, wie die einzelnen Wirkungsstufen typischerweise definiert werden können.

Auswirkungscode	Name der Auswirkung	In der Stichprobe definierter Umfang
1	`Critical`	Vollständiger Anwendung sausfall, von dem die meisten Kunden betroffen sind.
2	`High`	Vollständiger Anwendung sausfall, der sich auf eine Untergruppe von Kunden auswirkt.
3	`Medium`	Teilweiser Anwendung sausfall, der sich auf Kunden auswirkt.
4	`Low`	Zeitweise auftretende Ausfälle, die nur begrenzte Auswirkun gen auf Kunden haben.
5	`No Impact`	Kunden sind derzeit nicht betroffen, aber es sind dringende Maßnahmen erforderlich, um Auswirkungen zu vermeiden.

Untersuchung und Schadensbegrenzung

Die Ansicht mit den Vorfalldetails bietet Ihrem Team Runbooks, Zeitpläne und Kennzahlen. Informationen darüber, wie Sie mit einem Vorfall arbeiten können, finden Sie unter. Einzelheiten zum Vorfall

Runbooks bieten häufig Ermittlungsschritte und können automatisch Daten abrufen oder häufig verwendete Lösungen ausprobieren. Runbooks enthalten außerdem klare, wiederholbare Schritte, die sich für Ihr Team als nützlich erwiesen haben, um Vorfälle einzudämmen. Die Runbook-Tab konzentriert sich auf den aktuellen Runbook-Schritt und zeigt vergangene und future Schritte.

Incident Manager lässt sich in Systems Manager Automation integrieren, um Runbooks zu erstellen. Verwenden Sie Runbooks für eine der folgenden Aufgaben:

- Instanzen und AWS Ressourcen verwalten
- Automatische Ausführung von Skripten
- AWS CloudFormationRessourcen verwalten

Weitere Informationen zu den unterstützten Aktionstypen finden Sie in der Aktionsreferenz von Systems Manager Automation im AWS Systems ManagerBenutzerhandbuch.

Auf der Registerkarte „Zeitleiste“ wird angezeigt, welche Aktionen ergriffen wurden. In der Zeitleiste werden jeweils ein Zeitstempel und automatisch erstellte Details aufgezeichnet. Informationen zum Hinzufügen benutzerdefinierter Ereignisse zur Zeitleiste finden Sie im Zeitplan Abschnitt auf der Seite mit den Incident-Details in diesem Benutzerhandbuch.

Auf der Registerkarte Diagnose werden automatisch aufgefüllte Messwerte und manuell hinzugefügte Metriken angezeigt. Diese Ansicht bietet wertvolle Informationen über die Aktivitäten Ihrer Anwendung während eines Vorfalls.

Auf der Registerkarte „Engagements“ können Sie dem Vorfall weitere Kontakte hinzufügen und dem betroffenen Kontakt die Ressourcen zur Verfügung stellen, damit er sich schnell auf den neuesten Stand bringen kann, sobald er in den Vorfall involviert ist. Die Kontakte werden im Rahmen definierter Eskalationspläne oder persönlicher Engagementpläne kontaktiert.

Über einen Chat-Kanal können Sie direkt mit Ihrem Vorfall und anderen Einsatzkräften in Ihrem Team interagieren. Mithilfe von AWS Chatbot können Sie Chat-Kanäle in konfigurieren. SlackMicrosoft Teams, und Amazon Chime. In den Microsoft Teams Kanälen Slack und können Einsatzkräfte mithilfe einer Reihe von Befehlen direkt vom Chat-Kanal aus auf Vorfälle reagieren. `ssm-incidents` Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

Analyse nach dem Vorfall

Incident Manager bietet einen Rahmen, um über einen Vorfall nachzudenken und Maßnahmen zu ergreifen, die erforderlich sind, um zu verhindern, dass sich der Vorfall in future wiederholt, und um die Aktivitäten zur Reaktion auf Vorfälle insgesamt zu verbessern. Zu den Verbesserungen können gehören:

- Änderungen an den Anwendungen, die an einem Vorfall beteiligt waren. Ihr Team kann diese Zeit nutzen, um das System zu verbessern und es fehlertoleranter zu machen.
- Änderungen an einem Plan zur Reaktion auf Vorfälle. Nehmen Sie sich Zeit, um die gewonnenen Erkenntnisse einfließen zu lassen.
- Änderungen an Runbooks. Ihr Team kann sich eingehend mit den zur Problemlösung erforderlichen Schritten und den Schritten befassen, die Sie automatisieren können.
- Änderungen an den Warnmeldungen. Nach einem Vorfall sind Ihrem Team möglicherweise kritische Punkte in den Kennzahlen aufgefallen, anhand derer Sie das Team früher über einen Vorfall informieren können.

Incident Manager unterstützt diese potenziellen Verbesserungen, indem er neben dem Zeitplan des Vorfalls eine Reihe von Fragen und Aktionspunkten zur Analyse des Vorfalls verwendet. Weitere Informationen zur Verbesserung durch Analyse finden Sie unterDurchführung einer Analyse nach einem Vorfall im Incident-Manager.

AWS Systems Manager Incident Manager einrichten

Wir empfehlen, AWS Systems Manager Incident Manager in dem Konto einzurichten, das Sie für die Verwaltung Ihrer Betriebsabläufe verwenden. Bevor Sie Incident Manager zum ersten Mal verwenden, führen Sie die folgenden Aufgaben aus:

Themen

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS Management Console Die Art und Weise, wie programmatischer Zugriff gewährt wird, hängt vom Benutzertyp ab, der zugreift. AWS

Um Benutzern programmgesteuerten Zugriff zu gewähren, wählen Sie eine der folgenden Optionen.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zu AWS IAM Identity Center verwendenden im AWS

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs, Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch für AWS SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Folgen Sie den Anweisungen unter Verwenden temporärer Anmeldeinformationen mit AWS Ressourcen im IAM-Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
IAM	(Nicht empfohlen) Verwenden Sie langfristige Anmeldeinformationen, um programmatische Anfragen an die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldedaten im Benutzerhandbuch. AWS CLIAWS Command Line Interface • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch für AWS SDKs und Tools. • Informationen zu AWS APIs finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Erforderliche Rolle für die Einrichtung von Incident Manager

Bevor Sie beginnen, muss Ihr Konto über die IAM-Berechtigung `iam:CreateServiceLinkedRole` verfügen. Incident Manager verwendet diese Berechtigung, um das `AWSServiceRoleforIncidentManager` in Ihrem Konto zu erstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Incident Manager.

Erste Schritte mit Incident Manager

In diesem Abschnitt wird das Thema Get Prepared in der Incident Manager-Konsole beschrieben. Sie müssen den Vorgang Get prepared in der Konsole abschließen, bevor Sie sie für das Incident-Management verwenden können. Der Assistent führt Sie durch die Einrichtung Ihres Replikationssets, mindestens eines Kontakt- und eines Eskalationsplans sowie Ihres ersten Reaktionsplans. Die folgenden Leitfäden helfen Ihnen, Incident Manager und den Incident-Lebenszyklus besser zu verstehen:

- Was ist AWS Systems Manager Incident Manager?
- Der Incident-Lebenszyklus in Incident Manager

Voraussetzungen

Wenn Sie Incident Manager zum ersten Mal verwenden, finden Sie weitere Informationen unterAWS Systems Manager Incident Manager einrichten. Wir empfehlen, Incident Manager in dem Konto einzurichten, das Sie für die Verwaltung Ihrer Betriebsabläufe verwenden.

Wir empfehlen, dass Sie die Schnelleinrichtung von Systems Manager abschließen, bevor Sie mit dem Incident Manager-Assistenten Get Prepared beginnen. Verwenden Sie Systems Manager Quick Setup, um häufig verwendete AWS Dienste und Funktionen mit empfohlenen Best Practices zu konfigurieren. Incident Manager verwendet Systems Manager-Funktionen zur Verwaltung von Vorfällen, die mit Ihnen in Verbindung stehen, AWS-Konten und bietet Vorteile, wenn Systems Manager zuerst konfiguriert wurde.

Assistent zur Vorbereitung

Wenn Sie Incident Manager zum ersten Mal verwenden, können Sie auf der Startseite des Incident Manager-Service auf den Assistenten Get Prepared zugreifen. Um nach Abschluss der Einrichtung auf den Assistenten „Vorbereiten“ zuzugreifen, wählen Sie auf der Seite mit der Liste der Incidents die Option Prepare aus.

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie auf der Startseite des Incident Manager-Service die Option Get prepared aus.

Allgemeine Einstellungen

1. Wählen Sie unter Allgemeine Einstellungen die Option Einrichten aus.
2. Lesen Sie die Allgemeinen Geschäftsbedingungen. Wenn Sie mit den Allgemeinen Geschäftsbedingungen von Incident Manager einverstanden sind, wählen Sie Ich habe die Allgemeinen Geschäftsbedingungen von Incident Manager gelesen und stimme ihnen zu und wählen Sie dann Weiter.
3. Im Bereich Regionen wird Ihre aktuelle Region als erste Region in Ihrem Replikationssatz AWS-Region angezeigt. Um Ihrem Replikationssatz weitere Regionen hinzuzufügen, wählen Sie diese aus der Liste der Regionen aus.

   Wir empfehlen, mindestens zwei Regionen einzubeziehen. Falls eine Region vorübergehend nicht verfügbar ist, können Aktivitäten im Zusammenhang mit Vorfällen trotzdem an die andere Region weitergeleitet werden.

   > **Note**
   >
   > Durch die Erstellung des Replikationssatzes wird die `AWSServiceRoleforIncidentManager` serviceverknüpfte Rolle in Ihrem Konto erstellt. Weitere Informationen zu dieser Rolle finden Sie unterVerwenden von serviceverknüpften Rollen für Incident Manager.

4. Gehen Sie wie folgt vor, um die Verschlüsselung für Ihren Replikationssatz einzurichten:

   > **Note**
   >
   > Alle Incident Manager-Ressourcen sind verschlüsselt. Weitere Informationen darüber, wie Ihre Daten verschlüsselt werden, finden Sie unterDatenschutz im Incident Manager. Weitere Informationen zu Ihrem Incident Manager-Replikationssatz finden Sie unterVerwenden Sie den Incident Manager-Replikationssatz.

   - Um einen AWS eigenen Schlüssel zu verwenden, wählen Sie AWSEigenen Schlüssel verwenden.
   - Um Ihren eigenen AWS KMS Schlüssel zu verwenden, wählen Sie Einen vorhandenen Schlüssel auswählenAWS KMS key. Wählen Sie für jede Region, die Sie in Schritt 3

ausgewählt haben, einen AWS KMS Schlüssel oder geben Sie einen AWS KMS Amazon-Ressourcennamen (ARN) ein.

> **Tip**
>
> Wenn Sie keinen verfügbaren habenAWS KMS key, wählen Sie Create an AWS KMS key.

5. (Optional) Fügen Sie dem Replikationssatz im Bereich Tags ein oder mehrere Tags hinzu. Ein Tag enthält einen Schlüssel und optional einen Wert.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Weitere Informationen finden Sie unter Taggen von Ressourcen in Incident Manager.

6. (Optional) Um die Funktion „Ergebnisse“ zu aktivieren, aktivieren Sie im Bereich „Servicezugriff“ das Kontrollkästchen Servicerolle für Ergebnisse in diesem Konto erstellen.

   Bei einem Ergebnis handelt es sich um Informationen über eine Codebereitstellung oder eine Änderung der Infrastruktur, die ungefähr zur gleichen Zeit eingetreten sind, zu der ein Vorfall entstanden ist. Ein Befund kann als mögliche Ursache für den Vorfall untersucht werden. Informationen zu diesen möglichen Ursachen werden der Seite mit den Vorfalldetails für den Vorfall hinzugefügt. Da Informationen zu diesen Implementierungen und Änderungen sofort zur Hand sind, müssen die Einsatzkräfte nicht manuell nach diesen Informationen suchen.

   > **Tip**
   >
   > Um Informationen über die zu erstellende Rolle anzuzeigen, wählen Sie Berechtigungen anzeigen.

7. Wählen Sie Create (Erstellen) aus.

   Weitere Informationen zu Replikationssätzen und Resilienz finden Sie unterResilienz in AWS Systems Manager Incident Manager.

Kontakte (optional)

1. Wählen Sie Kontakt erstellen.

Incident Manager kontaktiert Kontakte während eines Vorfalls. Weitere Informationen zu Kontakten finden Sie unterMit Kontakten im Incident Manager arbeiten.

2. Geben Sie unter Name den Namen des Kontakts ein.
3. Geben Sie unter Eindeutiger Alias einen Alias ein, um diesen Kontakt zu identifizieren.
4. Gehen Sie im Abschnitt Kontaktkanal wie folgt vor, um zu definieren, wie der Kontakt bei Vorfällen kontaktiert wird:

   a. Wählen Sie für Typ die Option E-Mail, SMS oder Sprache aus.

   b. Geben Sie als Kanalname einen eindeutigen Namen ein, um den Kanal leichter identifizieren zu können.

   c. Geben Sie unter Detail die E-Mail-Adresse oder Telefonnummer des Kontakts ein.

      Telefonnummern müssen 9—15 Zeichen lang sein und mit beginnen, + gefolgt von der Landesvorwahl und der Abonnentennummer.

   d. Um einen weiteren Kontaktkanal zu erstellen, wählen Sie Neuen Kontaktkanal hinzufügen. Wir empfehlen, für jeden Kontakt mindestens zwei Kanäle zu definieren.

5. Gehen Sie im Bereich Engagementplan wie folgt vor, um zu definieren, über welche Kanäle der Kontakt benachrichtigt werden soll und wie lange auf eine Bestätigung über jeden Kanal gewartet werden soll. Wählen Sie die Kontaktkanäle aus, über die Sie den Kontakt bei Vorfällen kontaktieren möchten.

   > **Note**
   >
   > Wir empfehlen, im Interaktionsplan mindestens zwei Geräte zu definieren.

   a. Wählen Sie als Kontaktkanalname einen Kanal aus, den Sie im Bereich Kontaktkanal angegeben haben.

   b. Geben Sie für Interaktionszeit (min) die Anzahl der Minuten ein, die gewartet werden soll, bevor der Kontaktkanal aktiviert wird.

      Wir empfehlen, dass Sie zu Beginn eines Kontakts mindestens ein Gerät für die Interaktion auswählen und dabei eine Wartezeit von **0** (null) Minuten angeben.

   c. Um dem Interaktionsplan weitere Kontaktkanäle hinzuzufügen, wählen Sie Engagement hinzufügen.

6. (Optional) Fügen Sie dem Kontakt im Bereich „Schlagworte“ ein oder mehrere Tags hinzu. Ein Tag umfasst einen Schlüssel und optional einen Wert.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Weitere Informationen finden Sie unter Taggen von Ressourcen in Incident Manager.
7. Um den Kontaktdatensatz zu erstellen und Aktivierungscodes an die definierten Kontaktkanäle zu senden, wählen Sie Weiter.
8. (Optional) Geben Sie auf der Aktivierungsseite für den Kontaktkanal den Aktivierungscode ein, der an jeden Kanal gesendet wurde.

   Sie können später neue Aktivierungscodes generieren, wenn Sie die Codes jetzt nicht eingeben können.
9. Wiederholen Sie Schritt vier, bis Sie alle Ihre Kontakte zu Incident Manager hinzugefügt haben.
10. Nachdem alle Kontakte eingegeben wurden, wählen Sie Fertig stellen.

(Optional) Eskalationspläne

1. Wählen Sie Eskalationsplan erstellen aus.

   Ein Eskalationsplan eskaliert während eines Vorfalls über Ihre Ansprechpartner und stellt so sicher, dass der Incident Manager während eines Vorfalls die richtigen Ansprechpartner einsetzt. Weitere Informationen zu Eskalationsplänen finden Sie unter. Arbeiten mit Eskalationsplänen im Incident Manager
2. Geben Sie unter Name einen eindeutigen Namen für den Eskalationsplan ein.
3. Geben Sie für Alias einen eindeutigen Alias ein, damit Sie den Eskalationsplan leichter identifizieren können.
4. Gehen Sie im Bereich Phase 1 wie folgt vor:

   a. Wählen Sie unter Eskalationskanal die Kontaktkanäle aus, mit denen Sie Kontakt aufnehmen möchten.

   b. Wenn Sie möchten, dass ein Kontakt den Verlauf der Stufen des Eskalationsplans unterbrechen kann, wählen Sie Bestätigung stoppt den Planfortschritt aus.

   c. Um einer Phase weitere Kanäle hinzuzufügen, wählen Sie Eskalationskanal hinzufügen.

5. Um eine neue Phase im Eskalationsplan zu erstellen, wählen Sie Phase hinzufügen und fügen Sie die zugehörigen Stufendetails hinzu.
6. (Optional) Fügen Sie im Bereich „Tags“ dem Eskalationsplan ein oder mehrere Tags hinzu. Ein Tag enthält einen Schlüssel und optional einen Wert.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Weitere Informationen finden Sie unter Taggen von Ressourcen in Incident Manager.
7. Wählen Sie Eskalationsplan erstellen aus.

Response-Plan

1. Wählen Sie Reaktionsplan erstellen aus. Verwenden Sie den Reaktionsplan, um Kontakte und Eskalationspläne zusammenzustellen, die Sie erstellt haben. In diesem Assistenten für die ersten Schritte sind die folgenden Abschnitte optional, insbesondere wenn Sie zum ersten Mal einen Reaktionsplan einrichten:

   - Chat-Kanal
   - Runbooks
   - Engagements
   - Integrationen von Drittanbietern

   Informationen zum späteren Hinzufügen dieser Elemente zu Reaktionsplänen finden Sie unterVorbereitung auf Vorfälle im Incident Manager.
2. Geben Sie unter Name einen eindeutigen, identifizierbaren Namen für den Reaktionsplan ein. Der Name wird verwendet, um den Reaktionsplan-ARN oder in Reaktionsplänen ohne Anzeigenamen zu erstellen.
3. (Optional) Geben Sie unter Anzeigename einen Namen ein, damit Sie diesen Reaktionsplan bei der Erstellung von Incidents leichter identifizieren können.
4. Geben Sie unter Titel einen Titel ein, um die Art des Vorfalls zu identifizieren, der sich auf diesen Reaktionsplan bezieht. Der von Ihnen angegebene Wert ist im Titel jedes Vorfalls enthalten. Der Alarm oder das Ereignis, das den Vorfall ausgelöst hat, wird ebenfalls dem Titel hinzugefügt.
5. Wählen Sie unter Auswirkung das Ausmaß der Auswirkungen aus, das Sie für Vorfälle im Zusammenhang mit diesem Reaktionsplan erwarten, z. B. **`Critical`** oder**`Low`**.

6. (Optional) Geben Sie unter Zusammenfassung eine kurze Beschreibung ein, die einen Überblick über den Vorfall bietet. Incident Manager fügt während eines Vorfalls automatisch relevante Informationen in die Zusammenfassung ein.
7. (Optional) Geben Sie für Deduplizierungszeichenfolge eine Deduplizierungszeichenfolge ein. Incident Manager verwendet diese Zeichenfolge, um zu verhindern, dass dieselbe Grundursache mehrere Vorfälle in demselben Konto verursacht.

   Eine Deduplizierungszeichenfolge ist ein Begriff oder ein Ausdruck, den das System verwendet, um nach doppelten Vorfällen zu suchen. Wenn Sie eine Deduplizierungszeichenfolge angeben, sucht Incident Manager bei der Erstellung des Vorfalls nach offenen Vorfällen, die dieselbe Zeichenfolge in dem `dedupeString` Feld enthalten. Wenn ein Duplikat erkannt wird, dedupliziert Incident Manager den neueren Vorfall in den vorhandenen Incident.

   > **Note**
   >
   > Standardmäßig dedupliziert Incident Manager automatisch mehrere Vorfälle, die durch denselben CloudWatch Amazon-Alarm oder dasselbe Amazon-Ereignis verursacht wurden. EventBridge Sie müssen keine eigene Deduplizierungszeichenfolge eingeben, um eine Duplizierung für diese Ressourcentypen zu verhindern.

8. (Optional) Fügen Sie im Bereich „Tags“ dem Reaktionsplan ein oder mehrere Tags hinzu. Ein Tag enthält einen Schlüssel und optional einen Wert.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Weitere Informationen finden Sie unter Taggen von Ressourcen in Incident Manager.
9. Wählen Sie aus der Drop-down-Liste „Engagements“ die Kontakte und Eskalationspläne aus, die für den Vorfall gelten sollen.
10. Wählen Sie Reaktionsplan erstellen aus.

Nachdem Sie einen Reaktionsplan erstellt haben, können Sie CloudWatch Amazon-Alarme oder EventBridge Amazon-Ereignisse mit dem Reaktionsplan verknüpfen. Dadurch wird automatisch ein Vorfall erstellt, der auf einem Alarm oder Ereignis basiert. Weitere Informationen finden Sie unter Vorfälle im Incident Manager erstellen.

Regions- und kontenübergreifendes Incident-Management im Incident Manager

Sie können den Incident Manager, der über eine Funktion von verfügt, so konfigurierenAWS Systems Manager, dass er mit mehreren AWS-Regionen AND-Konten arbeitet. In diesem Abschnitt werden bewährte Methoden, Einrichtungsschritte und bekannte Einschränkungen für alle Regionen und Konten beschrieben.

Themen

Regionsübergreifendes Vorfallmanagement

Incident Manager unterstützt die automatisierte und manuelle Erstellung von Vorfällen in mehreren AWS-Regionen Fällen. Wenn Sie Incident Manager zum ersten Mal mithilfe des Assistenten Get Prepared nutzen, können Sie bis zu drei AWS-Regionen für Ihren Replikationssatz angeben. Bei Vorfällen, die automatisch durch CloudWatch Amazon-Alarme oder EventBridge Amazon-Ereignisse erstellt werden, versucht Incident Manager, einen Vorfall in derselben Weise AWS-Region wie die Ereignisregel oder der Alarm zu erstellen. Wenn Incident Manager in einer der verfügbaren RegionenAWS-Region, die in Ihrem Replikationssatz angegeben sind, nicht verfügbar ist CloudWatch oder EventBridge den Vorfall automatisch in einer der verfügbaren Regionen erstellt.

Important

Beachten Sie die folgenden wichtigen Details.

- Wir empfehlen, dass Sie mindestens zwei AWS-Regionen in Ihrem Replikationssatz angeben. Wenn Sie nicht mindestens zwei Regionen angeben, kann das System in dem Zeitraum, in dem Incident Manager nicht verfügbar ist, keine Incidents erstellen.
- Incidents, die durch ein regionsübergreifendes Failover erstellt wurden, rufen keine Runbooks auf, die in den Reaktionsplänen angegeben sind.

Weitere Informationen zur Integration mit Incident Manager und zur Angabe zusätzlicher Regionen finden Sie unter. Erste Schritte mit Incident Manager

Kontoübergreifendes Incident-Management

Incident Manager verwendet AWS Resource Access Manager (AWS RAM), um Incident Manager-Ressourcen für alle Management- und Anwendungskonten gemeinsam zu nutzen. In diesem Abschnitt werden bewährte Methoden für kontenübergreifende Anwendungen, die Einrichtung kontenübergreifender Funktionen für Incident Manager und bekannte Einschränkungen der kontenübergreifenden Funktionalität in Incident Manager beschrieben.

Ein Verwaltungskonto ist das Konto, von dem aus Sie die Betriebsverwaltung durchführen. In einer Organisation ist das Verwaltungskonto für die Reaktionspläne, Kontakte, Eskalationspläne, Runbooks und andere AWS Systems Manager Ressourcen verantwortlich.

Ein Anwendungskonto ist das Konto, dem die Ressourcen gehören, aus denen Ihre Anwendungen bestehen. Bei diesen Ressourcen kann es sich um Amazon EC2 EC2-Instances, Amazon DynamoDB-Tabellen oder andere Ressourcen handeln, die Sie zum Erstellen von Anwendungen in der verwenden. AWS Cloud Anwendungskonten besitzen auch die CloudWatch Amazon-Alarme und EventBridge Amazon-Ereignisse, die zu Vorfällen in Incident Manager führen.

AWS RAMverwendet gemeinsam genutzte Ressourcen, um Ressourcen zwischen Konten gemeinsam zu nutzen. In können Sie den Reaktionsplan und die Kontaktressourcen zwischen Konten gemeinsam nutzenAWS RAM. Durch die gemeinsame Nutzung dieser Ressourcen können Anwendungskonten und Verwaltungskonten mit Interaktionen und Vorfällen interagieren. Wenn Sie einen Reaktionsplan teilen, werden alle vergangenen und future Vorfälle geteilt, die mit diesem Reaktionsplan verursacht wurden. Wenn Sie einen Kontakt teilen, werden alle vergangenen und future Interaktionen des Kontakt- oder Antwortplans geteilt.

Bewährte Methoden

Folgen Sie diesen bewährten Methoden, wenn Sie Ihre Incident Manager-Ressourcen für mehrere Konten gemeinsam nutzen:

- Aktualisieren Sie den Resource Share regelmäßig mit Reaktionsplänen und Kontakten.
- Überprüfen Sie regelmäßig die Grundsätze für die gemeinsame Nutzung von Ressourcen.
- Richten Sie Incident Manager, Runbooks und Chat-Kanäle in Ihrem Verwaltungskonto ein.

Richten Sie das kontenübergreifende Incident-Management ein und konfigurieren Sie es

In den folgenden Schritten wird beschrieben, wie Sie Incident Manager-Ressourcen einrichten und konfigurieren und sie für kontenübergreifende Funktionen verwenden. Möglicherweise haben Sie in der Vergangenheit einige Dienste und Ressourcen für kontoübergreifende Funktionen konfiguriert. Verwenden Sie diese Schritte als Checkliste mit den Anforderungen, bevor Sie Ihren ersten Vorfall mit kontenübergreifenden Ressourcen starten.

1. (Optional) Erstellen Sie Organisationen und Organisationseinheiten mithilfe von. AWS Organizations Folgen Sie den Schritten im Tutorial: Organisation erstellen und konfigurieren im AWS OrganizationsBenutzerhandbuch.
2. (Optional) Verwenden Sie die Systems Manager Quick Setup-Funktion, um die richtigen AWS Identity and Access Management Rollen einzurichten, die Sie bei der Konfiguration Ihrer kontoübergreifenden Runbooks verwenden können. Weitere Informationen finden Sie unter Quick Setup im AWS Systems Manager-Benutzerhandbuch.
3. Folgen Sie den Schritten, die im AWS Systems ManagerBenutzerhandbuch unter Automationen in mehreren AWS-Regionen und Konten ausführen aufgeführt sind, um Runbooks in Ihren Systems Manager Manager-Automatisierungsdokumenten zu erstellen. Ein Runbook kann entweder über ein Verwaltungskonto oder über eines Ihrer Anwendungskonten ausgeführt werden. Je nach Anwendungsfall müssen Sie die entsprechende AWS CloudFormation Vorlage für die Rollen installieren, die zum Erstellen und Anzeigen von Runbooks während eines Vorfalls erforderlich sind.
    - Ein Runbook im Verwaltungskonto ausführen. Das Verwaltungskonto muss die `AWS-SystemsManager-AutomationReadOnlyRole` CloudFormation Vorlage herunterladen und installieren. Geben Sie bei der Installation `AWS-SystemsManager-AutomationReadOnlyRole` die Konto-IDs aller Anwendungskonten an. Diese Rolle ermöglicht es Ihren Anwendungskonten, den Status des Runbooks auf der Seite mit den Vorfalldetails zu lesen. Das Anwendungskonto muss die `AWS-SystemsManager-AutomationAdministrationReadOnlyRole` CloudFormation Vorlage installieren. Die Seite mit den Vorfalldetails verwendet diese Rolle, um den Automatisierungsstatus vom Verwaltungskonto abzurufen.
    - Ein Runbook in einem Anwendungskonto ausführen. Das Verwaltungskonto muss die `AWS-SystemsManager-AutomationAdministrationReadOnlyRole` CloudFormation Vorlage herunterladen und installieren. Diese Rolle ermöglicht es dem Verwaltungskonto, den Status des Runbooks im Anwendungskonto zu lesen. Das Anwendungskonto muss

die AWS-SystemsManager-AutomationReadOnlyRole CloudFormation Vorlage herunterladen und installieren. Geben Sie bei der Installation `AWS-SystemsManager-AutomationReadOnlyRole` die Konto-ID des Verwaltungskontos und anderer Anwendungskonten an. Das Verwaltungskonto und andere Anwendungskonten übernehmen diese Rolle, um den Status des Runbooks zu lesen.

4. (Optional) Laden Sie die AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation Vorlage für jedes Anwendungskonto in der Organisation herunter und installieren Sie sie. Geben Sie bei der Installation `AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole` die Konto-ID des Verwaltungskontos an. Diese Rolle bietet die Berechtigungen, die Incident Manager für den Zugriff auf Informationen über AWS CodeDeploy Bereitstellungen und AWS CloudFormation Stack-Updates benötigt. Diese Informationen werden als Ergebnisse für einen Vorfall gemeldet, wenn die Funktion „Ergebnisse“ aktiviert ist. Weitere Informationen finden Sie unter Arbeiten mit Ergebnissen in Incident Manager.
5. Gehen Sie wie unter beschrieben vor, um Kontakte, Eskalationspläne, Chat-Kanäle und Reaktionspläne einzurichten und zu erstellen. Vorbereitung auf Vorfälle im Incident Manager
6. Fügen Sie Ihre Kontakte und Ressourcen für den Reaktionsplan entweder zu Ihrer vorhandenen oder zu einer neuen Ressourcenfreigabe in AWS RAM hinzu. Weitere Informationen finden Sie unter Erste Schritte in AWS RAM im AWS RAM-Benutzerhandbuch. Durch das Hinzufügen von Reaktionsplänen AWS RAM können Anwendungskonten auf Vorfälle und Vorfall-Dashboards zugreifen, die mithilfe der Reaktionspläne erstellt wurden. Anwendungskonten bieten außerdem die Möglichkeit, CloudWatch Alarme und EventBridge Ereignisse einem Reaktionsplan zuzuordnen. Durch das Hinzufügen von Kontakten und Eskalationsplänen AWS RAM können Anwendungskonten über das Incident-Dashboard Interaktionen einsehen und Kontakte kontaktieren.
7. Fügen Sie Ihrer Konsole kontoübergreifende, regionsübergreifende Funktionen hinzu. CloudWatch Schritte und Informationen finden Sie unter Kontoübergreifende regionsübergreifende CloudWatch Konsole im CloudWatch Amazon-Benutzerhandbuch. Durch das Hinzufügen dieser Funktion wird sichergestellt, dass die von Ihnen erstellten Anwendungskonten und das Verwaltungskonto Metriken in den Incident- und Analyse-Dashboards anzeigen und bearbeiten können.
8. Erstellen Sie einen kontenübergreifenden EventBridge Amazon-Eventbus. Schritte und Informationen finden Sie unter EventBridge Amazon-Ereignisse zwischen AWS Konten senden und empfangen. Anschließend können Sie diesen Event-Bus verwenden, um Ereignisregeln

zu erstellen, die Vorfälle in Anwendungskonten erkennen und Vorfälle im Verwaltungskonto erstellen.

Einschränkungen

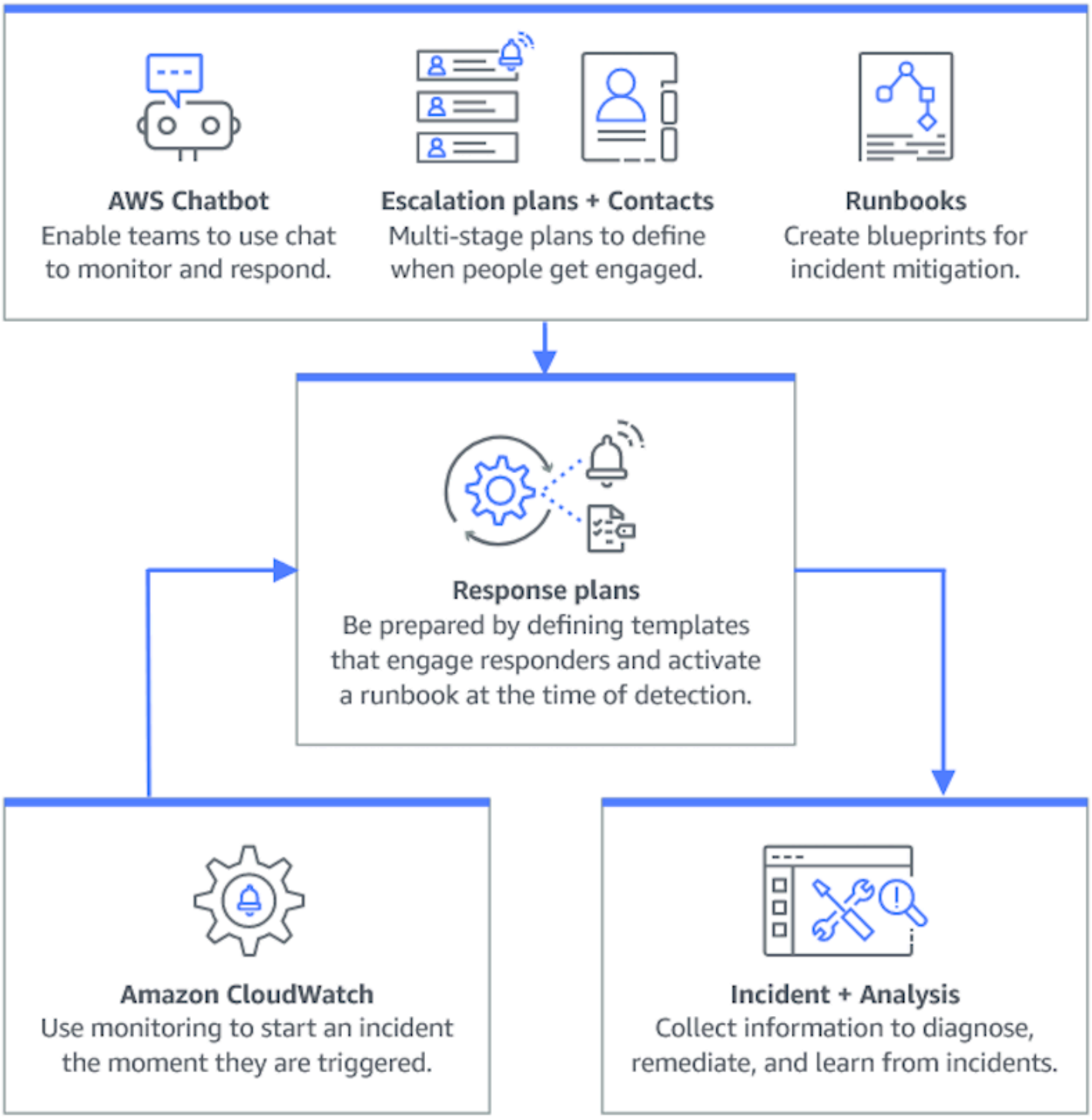
Im Folgenden sind die Einschränkungen der kontenübergreifenden Funktionalität von Incident Manager bekannt:

- Das Konto, das eine Analyse nach dem Vorfall erstellt, ist das einzige Konto, das diese einsehen und ändern kann. Wenn Sie ein Anwendungskonto verwenden, um eine Analyse nach einem Vorfall zu erstellen, können nur Mitglieder dieses Kontos diese einsehen und ändern. Das Gleiche gilt, wenn Sie ein Verwaltungskonto verwenden, um eine Analyse nach einem Vorfall zu erstellen.
- Timeline-Ereignisse werden für Automatisierungsdokumente, die in Anwendungskonten ausgeführt werden, nicht aufgefüllt. Aktualisierungen von Automatisierungsdokumenten, die in Anwendungskonten ausgeführt werden, sind auf der Registerkarte Runbook des Vorfalls sichtbar.

- Amazon Simple Notification Service-Themen können nicht kontoübergreifend verwendet werden. Amazon SNS SNS-Themen müssen in derselben Region und demselben Konto erstellt werden wie der Reaktionsplan, in dem sie verwendet werden. Wir empfehlen, das Verwaltungskonto zu verwenden, um alle SNS-Themen und Reaktionspläne zu erstellen.
- Eskalationspläne können nur mithilfe von Kontakten im selben Konto erstellt werden. Ein Kontakt, der mit Ihnen geteilt wurde, kann nicht zu einem Eskalationsplan in Ihrem Konto hinzugefügt werden.
- Schlagworte, die Reaktionsplänen, Vorfalldatensätzen und Kontakten zugewiesen wurden, können nur über das Konto des Ressourcenbesitzers eingesehen und geändert werden.

Vorbereitung auf Vorfälle im Incident Manager

Die Planung eines Vorfalls beginnt lange vor dem Incident-Lebenszyklus. Um sich auf einen Vorfall vorzubereiten, sollten Sie jedes der folgenden Themen berücksichtigen, bevor Sie Reaktionspläne erstellen. Verwenden Sie Überwachung, Kontakte, Eskalationspläne, Chat-Kanäle und Runbooks, um Reaktionspläne zu erstellen, die die Reaktion automatisieren.



Themen

- Überwachen
- Mit allgemeinen Einstellungen arbeiten
- Mit Kontakten im Incident Manager arbeiten

- Arbeiten mit Bereitschaftsplänen im Incident Manager
- Arbeiten mit Eskalationsplänen im Incident Manager
- Arbeiten mit Chat-Kanälen in Incident Manager
- Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager
- Arbeiten mit Reaktionsplänen in Incident Manager
- Arbeiten mit Ergebnissen in Incident Manager

Überwachen

Die Überwachung des Zustands Ihrer AWS gehosteten Anwendungen ist entscheidend, um die Verfügbarkeit und Leistung Ihrer Anwendungen sicherzustellen. Beachten Sie bei der Auswahl von Überwachungslösungen Folgendes:

- Kritikalität der Funktion — Wenn das System ausfallen sollte, wie gravierend wären die Auswirkungen auf nachgeschaltete Anwender?
- Gemeinsamkeit von Ausfällen — Wie häufig fällt ein System aus? Systeme, bei denen häufig eingegriffen werden muss, sollten engmaschig überwacht werden.
- Höhere Latenz — Um wie viel Zeit bis zur Erledigung einer Aufgabe benötigt wird.
- Clientseitige und serverseitige Metriken — Wenn es eine Diskrepanz zwischen verwandten Metriken auf dem Client und dem Server gibt.
- Fehler bei Abhängigkeiten — Fehler, auf die sich Ihr Team vorbereiten kann und sollte.

Nachdem Sie Reaktionspläne erstellt haben, können Sie mithilfe Ihrer Überwachungslösungen Vorfälle automatisch verfolgen, sobald sie in Ihrer Umgebung auftreten. Weitere Informationen zur Nachverfolgung und Erstellung von Vorfällen finden Sie unterNachverfolgung von Vorfällen im Incident Manager.

Weitere Informationen zur Architektur sicherer, leistungsstarker, robuster und effizienter Infrastrukturanwendungen und Workloads finden Sie im Whitepaper Well-Architected. AWS

Mit allgemeinen Einstellungen arbeiten

Nachdem Sie den Onboarding-Assistenten für Incident Manager abgeschlossen haben, können Sie bestimmte Optionen auf der Seite Einstellungen verwalten. Zu diesen Optionen gehören Ihr Replikationssatz, auf den Replikationssatz angewendete Tags und die Funktion „Ergebnisse“.

Themen

Verwenden Sie den Incident Manager-Replikationssatz

Das Incident Manager-Replikationsset repliziert Ihre Daten auf viele, AWS-Regionen um die regionsübergreifende Redundanz zu erhöhen, Incident Manager den Zugriff auf Ressourcen in verschiedenen Regionen zu ermöglichen und die Latenz für Ihre Benutzer zu reduzieren. Das Replikationsset wird auch verwendet, um Ihre Daten entweder mit einem Von AWS verwalteter Schlüssel oder Ihrem eigenen, vom Kunden verwalteten Schlüssel zu verschlüsseln. Alle Incident Manager-Ressourcen sind standardmäßig verschlüsselt. Weitere Informationen darüber, wie Ihre Ressourcen verschlüsselt sind, finden Sie unterDatenschutz im Incident Manager. Um mit Incident Manager zu beginnen, erstellen Sie zunächst Ihren Replikationssatz mithilfe des Assistenten Get prepared. Weitere Informationen zur Vorbereitung in Incident Manager finden Sie unterAssistent zur Vorbereitung.

Bearbeiten Sie Ihren Replikationssatz

Auf der Seite mit den Incident Manager-Einstellungen können Sie Ihren Replikationssatz bearbeiten. Sie können Regionen hinzufügen, Regionen löschen und den Schutz vor dem Löschen von Replikationssätzen aktivieren oder deaktivieren. Sie können den Schlüssel, mit dem Ihre Daten verschlüsselt wurden, nicht bearbeiten. Um den Schlüssel zu ändern, löschen Sie den Replikationssatz und erstellen Sie ihn neu.

Eine Region hinzufügen

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie dann im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie Region hinzufügen.
3. Wählen Sie die Region.
4. Wählen Sie Hinzufügen aus.

Eine Region löschen

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie dann im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie die Region aus, die Sie löschen möchten.
3. Wählen Sie Löschen aus.
4. Geben Sie Löschen in das Textfeld ein und wählen Sie Löschen.

Löschen Sie Ihren Replikationssatz

Wenn Sie die letzte Region in Ihrem Replikationssatz löschen, wird der gesamte Replikationssatz gelöscht. Bevor Sie die letzte Region löschen können, deaktivieren Sie den Löschschutz, indem Sie auf der Seite Einstellungen die Option Löschschutz aktivieren. Nachdem Sie Ihren Replikationssatz gelöscht haben, können Sie mithilfe des Assistenten „Vorbereiten“ einen neuen Replikationssatz erstellen.

Um eine Region aus Ihrem Replikationssatz zu löschen, warten Sie 24 Stunden, nachdem Sie sie erstellt haben. Wenn Sie versuchen, eine Region früher als 24 Stunden nach der Erstellung aus Ihrem Replikationssatz zu löschen, schlägt der Löschvorgang fehl.

Durch das Löschen Ihres Replikationssatzes werden alle Incident Manager-Daten gelöscht.

Löschen Sie den Replikationssatz

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie dann im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie die letzte Region in Ihrem Replikationssatz aus.
3. Wählen Sie Löschen aus.
4. Geben Sie Löschen in das Textfeld ein und wählen Sie Löschen aus.

Tags für einen Replikationssatz verwalten

Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Verwenden Sie Tags, um eine Ressource auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Besitzer oder Umgebung.

Um Tags für einen Replikationssatz zu verwalten

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie dann im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie im Bereich „Tags“ die Option Bearbeiten aus.
3. Führen Sie die folgenden Schritte aus, um ein Tag hinzuzufügen:
   a. Wählen Sie Neues Tag hinzufügen aus.
   b. Geben Sie einen Schlüssel und einen optionalen Wert für das Tag ein.
   c. Wählen Sie Speichern.
4. Gehen Sie wie folgt vor, um ein Tag zu löschen:
   a. Wählen Sie unter dem Tag, das Sie löschen möchten, die Option Entfernen aus.
   b. Wählen Sie Speichern.

Verwaltung der Funktion „Ergebnisse“

Die Funktion „Ergebnisse“ hilft den Einsatzkräften in Ihrem Unternehmen, mögliche Ursachen für Vorfälle kurz nach Beginn der Vorfälle zu identifizieren. Derzeit stellt Incident Manager Ergebnisse für AWS CodeDeploy Bereitstellungen und AWS CloudFormation Stack-Updates bereit.

Für die kontenübergreifende Unterstützung der Ergebnisse müssen Sie nach der Aktivierung der Funktion für jedes Anwendungskonto in der Organisation einen zusätzlichen Einrichtungsschritt durchführen.

Um die Funktion nutzen zu können, lassen Sie Incident Manager eine Servicerolle erstellen, die die erforderlichen Berechtigungen für den Datenzugriff in Ihrem Namen enthält.

Um die Funktion „Ergebnisse“ zu aktivieren

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie dann im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie im Bereich Ergebnisse die Option Servicerolle erstellen aus.
3. Überprüfen Sie die Informationen über die zu erstellende Servicerolle und wählen Sie dann Erstellen aus.

Um die Findings-Funktion zu deaktivieren

Um die Findings-Funktion nicht mehr zu verwenden, löschen Sie die `IncidentManagerIncidentAccessServiceRole` Rolle aus jedem Konto, in dem sie erstellt wurde.

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Geben Sie in das Suchfeld ei **`IncidentManagerIncidentAccessServiceRole`**.
4. Wählen Sie den Namen der Rolle und anschließend Löschen aus.
5. Geben Sie den Rollennamen in das Dialogfeld ein, um zu bestätigen, dass Sie die Rolle löschen möchten, und wählen Sie dann Löschen.

Mit Kontakten im Incident Manager arbeiten

AWS Systems Manager Incident ManagerKontaktpersonen reagieren auf Vorfälle. Ein Kontakt kann über mehrere Kanäle verfügen, die der Incident Manager während eines Vorfalls nutzen kann. Sie können den Engagementplan eines Kontakts definieren, um zu beschreiben, wie und wann der Incident Manager den Kontakt einbindet.

Themen

Kontaktkanäle

Kontaktkanäle sind die verschiedenen Methoden, die der Incident Manager verwendet, um einen Kontakt zu kontaktieren.

Incident Manager unterstützt die folgenden Kontaktkanäle:

- E-Mail
- Kurznachrichtendienst (SMS)

- Stimme

Aktivierung des Kontaktkanals

Um Ihre Privatsphäre und Sicherheit zu schützen, sendet Ihnen Incident Manager beim Erstellen von Kontakten einen Geräteaktivierungscode. Um Ihre Geräte während eines Vorfalls zu aktivieren, müssen Sie sie zunächst aktivieren. Geben Sie dazu den Geräteaktivierungscode auf der Seite „Kontakt erstellen“ ein.

Bestimmte Funktionen von Incident Manager beinhalten Funktionen, mit denen Benachrichtigungen an einen Kontaktkanal gesendet werden. Durch die Nutzung dieser Funktionen erklären Sie sich damit einverstanden, dass dieser Dienst Benachrichtigungen über Serviceunterbrechungen oder andere Ereignisse an die im angegebenen Workflow enthaltenen Kontaktkanäle sendet. Dazu gehören Benachrichtigungen, die im Rahmen einer Rotation des Bereitschaftsdienstes an einen Kontakt gesendet werden. Benachrichtigungen können per E-Mail, SMS-Nachricht oder Sprachanruf gesendet werden, wie in den Kontaktdetails angegeben. Durch die Verwendung dieser Funktionen bestätigen Sie, dass Sie berechtigt sind, die Kontaktkanäle, die Sie dem Incident Manager zur Verfügung stellen, hinzuzufügen.

Abmelden

Sie können diese Benachrichtigungen jederzeit stornieren, indem Sie ein Mobilgerät als Kontaktkanal entfernen. Einzelne Benachrichtigungsempfänger können Benachrichtigungen auch jederzeit stornieren, indem sie das Gerät aus ihrem Kontakt entfernen.

Um einen Kontaktkanal von einem Kontakt zu entfernen

1. Navigieren Sie zur Incident Manager-Konsole und wählen Sie im linken Navigationsbereich Kontakte aus.
2. Wählen Sie den Kontakt mit dem Kontaktkanal aus, den Sie entfernen möchten, und wählen Sie Bearbeiten.
3. Wählen Sie neben dem Kontaktkanal, den Sie entfernen möchten, die Option Entfernen aus.
4. Wählen Sie Aktualisieren aus.

Deaktivierung des Kontaktkanals

Um ein Gerät zu deaktivieren, antworten Sie auf ABMELDEN. Wenn Sie auf ABBESTELLEN antworten, kann der Incident Manager Ihr Gerät nicht mehr aktivieren.

Reaktivierung des Kontaktkanals

1. Antworten Sie auf die Nachricht von Incident Manager mit START.
2. Navigieren Sie zur Incident Manager-Konsole und wählen Sie im linken Navigationsbereich Kontakte aus.
3. Wählen Sie den Kontakt mit dem Kontaktkanal aus, den Sie entfernen möchten, und wählen Sie Bearbeiten.
4. Wählen Sie Geräte aktivieren.
5. Geben Sie den Aktivierungscode ein, der vom Incident Manager an das Gerät gesendet wurde.
6. Wählen Sie Activate.

Engagementpläne

Engagementpläne definieren, wann der Incident Manager die Kontaktkanäle nutzt. Sie können Kontaktkanäle zu Beginn eines Engagements in verschiedenen Phasen mehrfach kontaktieren. Sie können Engagementpläne in einem Eskalations- oder Reaktionsplan verwenden. Weitere Informationen zu Eskalationsplänen finden Sie unterArbeiten mit Eskalationsplänen im Incident Manager.

So erstellen Sie einen Kontakt

Gehen Sie wie folgt vor, um einen Kontakt zu erstellen.

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie in der linken Navigationsleiste Kontakte aus.
2. Wählen Sie Kontakt erstellen.
3. Geben Sie den vollständigen Namen des Kontakts ein und geben Sie einen eindeutigen und identifizierbaren Alias an.
4. Definieren Sie einen Kontaktkanal. Wir empfehlen, zwei oder mehr verschiedene Arten von Kontaktkanälen zu haben.

    a. Wählen Sie den Typ: E-Mail, SMS oder Sprachnachricht.

    b. Geben Sie einen identifizierbaren Namen für den Kontaktkanal ein.

    c. Geben Sie die Kontaktkanaldetails an, z. B. E-Mail: arosalez@example.com
5. Um mehr als einen Kontaktkanal zu definieren, wählen Sie Kontaktkanal hinzufügen. Wiederholen Sie Schritt 4 für jeden neu hinzugefügten Kontaktkanal.

6. Definieren Sie einen Engagementplan.

   > **Important**
   >
   > Um einen Kontakt zu engagieren, müssen Sie einen Engagement-Plan definieren.

   a. Wählen Sie einen Kontaktkanalnamen.

   b. Definieren Sie, wie viele Minuten ab Beginn des Engagements gewartet werden soll, bis der Incident Manager diesen Kontaktkanal aktiviert.

   c. Um einen weiteren Kontaktkanal hinzuzufügen, wählen Sie Engagement hinzufügen.

7. Nachdem Sie Ihren Engagement-Plan definiert haben, wählen Sie Erstellen. Incident Manager sendet einen Aktivierungscode an jeden der definierten Kontaktkanäle.
8. (Optional) Um die Kontaktkanäle zu aktivieren, geben Sie den Aktivierungscode ein, den der Incident Manager an jeden definierten Kontaktkanal gesendet hat.
9. (Optional) Um einen neuen Aktivierungscode zu senden, wählen Sie Neuen Code senden.
10. Wählen Sie Finish (Abschließen).

Nachdem Sie einen Kontakt definiert und seine Kontaktkanäle aktiviert haben, können Sie Kontakte zu Eskalationsplänen hinzufügen, um eine Eskalationskette zu bilden. Weitere Informationen zu Eskalationsplänen finden Sie unterArbeiten mit Eskalationsplänen im Incident Manager. Sie können einem Reaktionsplan Kontakte hinzufügen, um eine direkte Interaktion zu ermöglichen. Weitere Informationen zum Erstellen von Reaktionsplänen finden Sie unterArbeiten mit Reaktionsplänen in Incident Manager.

Importieren Sie Kontaktdaten in Ihr Adressbuch

Wenn ein Incident erstellt wird, kann der Incident Manager die Einsatzkräfte mithilfe von Sprach- oder SMS-Benachrichtigungen benachrichtigen. Um sicherzustellen, dass die Einsatzkräfte sehen, dass der Anruf oder die SMS-Benachrichtigung vom Incident Manager stammt, empfehlen wir allen Respondern, die Datei im virtuellen Incident Manager-Kartenformat (.vcf) in das Adressbuch auf ihren Mobilgeräten herunterzuladen. Die Datei wird bei Amazon gehostet CloudFront und ist in der AWS kommerziellen Partition verfügbar.

So laden Sie die Incident Manager-.vcf-Datei herunter

1. Wählen Sie auf Ihrem Mobilgerät entweder die folgende URL aus oder geben Sie sie ein: https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .vcf.
2. Speichern oder importieren Sie die Datei in das Adressbuch auf Ihrem Mobilgerät.

Arbeiten mit Bereitschaftsplänen im Incident Manager

Ein Bereitschaftsplan im Incident Manager definiert, wer benachrichtigt wird, wenn ein Vorfall eintritt, der ein Eingreifen des Bedieners erfordert. Ein Bereitschaftsplan besteht aus einer oder mehreren Rotationen, die Sie für den Zeitplan erstellen. Jede Umdrehung kann bis zu 30 Kontakte umfassen.

Nachdem Sie einen Bereitschaftsplan erstellt haben, können Sie ihn als Eskalation in Ihren Eskalationsplan aufnehmen. Wenn ein Vorfall im Zusammenhang mit diesem Eskalationsplan eintritt, benachrichtigt der Incident Manager den Operator (oder die Operatoren), der gemäß dem Zeitplan auf Abruf ist. Dieser Kontakt kann dann das Engagement bestätigen. In Ihrem Eskalationsplan können Sie einen oder mehrere Bereitschaftspläne sowie einen oder mehrere einzelne Ansprechpartner für mehrere Eskalationsphasen festlegen. Weitere Informationen finden Sie unter Arbeiten mit Eskalationsplänen im Incident Manager.

> **Tip**
>
> Als bewährte Methode empfehlen wir, in einem Eskalationsplan Kontakte und Bereitschaftspläne als Eskalationskanäle hinzuzufügen. Sie sollten dann einen Eskalationsplan als Reaktion auf einen Reaktionsplan wählen. Dieser Ansatz bietet die umfassendste Abdeckung der Reaktion auf Vorfälle in Ihrem Unternehmen.

Jeder Bereitschaftsplan unterstützt bis zu acht Rotationen. Rotationen können sich überlappen oder gleichzeitig ablaufen. Dies erhöht die Anzahl der Betreiber, die benachrichtigt werden, um im Falle eines Vorfalls zu reagieren. Sie können auch Rotationen erstellen, die nacheinander ausgeführt werden. Dies unterstützt Szenarien wie das „Follow the Sun“ -Incident-Management, bei dem Sie Gruppen auf der ganzen Welt haben, die denselben Service unterstützen.

Verwenden Sie die Themen in diesem Abschnitt, um Ihnen bei der Erstellung und Verwaltung von Bereitschaftsplänen für Ihre Incident-Response-Operationen zu helfen.

Themen

Erstellung eines Bereitschaftsplans und einer Rotation im Incident Manager

Erstellen Sie einen Bereitschaftsplan mit einem oder mehreren Rotationen von Kontakten, um auf Vorfälle während ihrer Schicht zu reagieren.

Bevor Sie beginnen

Bevor Sie einen Bereitschaftsplan erstellen, stellen Sie sicher, dass Sie zuvor die Kontakte erstellt haben, die Sie zu den Rotationen im Zeitplan hinzufügen möchten. Weitere Informationen finden Sie unter Mit Kontakten im Incident Manager arbeiten.

Berücksichtigung von Änderungen der Sommerzeit (DST)

Wenn Sie eine Rotation erstellen, geben Sie die globale Zeitzone an, die als Grundlage für die Zeiten und Daten der Schichtabdeckung dient, die Sie für diese Rotation angeben. Sie können jede von der Internet Assigned Numbers Authority (IANA) definierte Zeitzone verwenden. Beispiel: `America/Los_Angeles`, `UTC` und `Asia/Seoul`. Sie können einem Bereitschaftsplan mehr als eine Rotation hinzufügen. Wenn sich die Einsatzkräfte für jede Rotation jedoch geografisch in verschiedenen Zeitzonen befinden, sollten Sie alle Änderungen der Sommerzeit berücksichtigen, denen jede Rotation unterliegen kann.

`Europe/Dublin`Beachten Sie zum Beispiel `America/Los_Angeles` verschiedene Sommerzeitpläne. Daher kann der Zeitunterschied zwischen den beiden Zonen je nach Jahreszeit zwischen 6 und 8 Stunden variieren. Ein follow-the-sun Bereitschaftsplan hat beispielsweise eine Rotation in der `America/Los_Angeles` Zeitzone und eine Rotation in `Europe/Dublin` der Zeitzone. In diesem Beispiel kann der Zeitplan aufgrund von Sommerzeitänderungen eine einstündige Schichtlücke oder eine einstündige Schichtüberlappung enthalten.

Um diese Situationen zu vermeiden, empfehlen wir den folgenden Ansatz:

1. Verwenden Sie eine einzige Zeitzone für alle Rotationen in einem Bereitschaftsplan.
2. Ermitteln Sie lokale Zeiten, wenn Sie Responder außerhalb dieser bestimmten Zeitzone zuweisen.

Wenn Sie sich entscheiden, jede Rotation ihrer lokalen Zeitzone zuzuweisen, überprüfen Sie den Zeitplan vor jeder Sommerzeit. Passen Sie dann die Rotationsschichtzeiten nach Bedarf

an, um sicherzustellen, dass Sie unbeabsichtigte Lücken oder Überschneidungen in Ihrem Bereitschaftsdienst vermeiden, bevor Änderungen der Sommerzeit wirksam werden.

Um einen Bereitschaftsplan zu erstellen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.
3. Wählen Sie Bereitschaftsplan erstellen aus.
4. Geben Sie unter Name des Zeitplans einen Namen ein, anhand dessen Sie den Zeitplan leichter identifizieren können, z. **`MyApp Primary On-call Schedule`** B.
5. Geben Sie für den Zeitplan-Alias einen Alias für diesen Zeitplan ein, der im aktuellen Zeitplan einzigartig istAWS-Region, z. **`my-app-primary-on-call-schedule`** B.
6. (Optional) Wenden Sie im Bereich „Tags“ einen oder mehrere Tag-Schlüsselnamen und Wertepaare auf den Bereitschaftsplan an.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können beispielsweise einen Zeitplan kennzeichnen, um den Zeitraum zu identifizieren, in dem er ausgeführt wird, welche Arten von Operatoren er enthält oder welchen Eskalationsplan er unterstützt. Weitere Informationen zum Taggen von Incident Manager-Ressourcen finden Sie unterTaggen von Ressourcen in Incident Manager.
7. Fahren Sie fort, indem Sie dem Bereitschaftsplan eine oder mehrere Rotationen hinzufügen.

Erstellen einer Rotation für einen Bereitschaftsplan im Incident Manager

Eine Rotation in einem Bereitschaftsplan gibt an, wann die Schicht in Kraft ist. Es gibt auch die Kontakte an, durch die sich die Schichten drehen. Sie können bis zu acht Rotationen in einen einzigen Bereitschaftsplan aufnehmen.

Sie können alle Personen, die Sie in Incident Manager als Kontakt erstellt haben, zu einer Rotation hinzufügen. Informationen zur Verwaltung Ihrer Kontakte finden Sie unterMit Kontakten im Incident Manager arbeiten.

Während Sie Ihre Rotation konfigurieren, können Sie in einem Vorschaukalender auf der rechten Seite sehen, wie der gesamte Zeitplan aussieht.

So erstellen Sie eine Rotation für einen Bereitschaftsplan

1. Geben Sie auf der Seite Bereitschaftsplan erstellen im Abschnitt Rotation 1 für Rotationsname einen Namen ein, der die Rotation identifiziert, z. B. **`00:00 - 7:59 Support`** oder**`Dublin Support Group`**.
2. Geben Sie als Startdatum das Datum ein, an dem diese Rotation aktiv wird, in einem `YYYY/MM/DD` Format wie`2023/07/14`.
3. Wählen Sie unter Zeitzone die globale Zeitzone aus, die als Grundlage für die Zeiten und Daten der Schichtabdeckung dient, die Sie für diese Rotation angeben.

   Sie können jede von der Internet Assigned Numbers Authority (IANA) definierte Zeitzone verwenden. Zum Beispiel: „America/Los_Angeles“, „UTC“, „Asia/Seoul“. Weitere Informationen finden Sie unter Time Zone Database auf der IANA-Website.

   > **Warning**
   >
   > Sie können jede Rotation auf ihrer eigenen Zeitzone basieren. Jede Änderung der Sommerzeit in den von Ihnen ausgewählten Zeitzonen kann sich jedoch auf Ihre geplanten Versicherungsfenster auswirken. Weitere Informationen finden Sie weiter oben in diesem Thema unter Berücksichtigung von Änderungen der Sommerzeit (DST).

4. Geben Sie für die Startzeit der Rotation die Uhrzeit ein, zu der die Schicht dieser Rotation beginnt, im `hh:mm` 24-Stunden-Format, z. `16:00` B.

   Beachten Sie die Unterschiede in der Ortszeit für Kontakte in Zeitzonen, die sich von der von Ihnen angegebenen unterscheiden. Wenn Sie beispielsweise als Zeitzone und `America/Los_Angeles` `00:00` als Startzeit der Rotation wählen, entspricht dies 08:00 Uhr in Dublin, Irland, und 13:30 Uhr in Mumbai, Indien.
5. Geben Sie für Endzeit der Rotation die Uhrzeit ein, zu der die Schicht dieser Rotation endet, im `hh:mm` 24-Stunden-Format, z. `23:59` B.

   > **Note**
   >
   > Die Zeitspanne zwischen Beginn und Ende einer Rotation muss mindestens 30 Minuten betragen.

6. (Optional) Um die Rotationslänge auf 24 Stunden festzulegen, wählen Sie 24-Stunden-Abdeckung aus und geben Sie die Startzeit für diese Rotation in das Feld Startzeit der Rotation ein. Der Wert für die Endzeit der Rotation wird automatisch aktualisiert.

   Wenn Sie beispielsweise möchten, dass Ihr Bereitschaftsdienst mit dem Schichtwechsel um 11 Uhr erreichbar ist, wählen Sie 24-Stunden-Empfang und geben Sie **`11:00`** als Startzeit ein.
7. Wählen Sie unter Aktive Tage die Wochentage aus, an denen diese Rotation aktiv ist. Wenn Ihr Bereitschaftsplan beispielsweise den Wochenendschutz ausschließt, wählen Sie alle Tage außer Sonntag und Samstag aus.
8. Fahren Sie fort, indem Sie der Rotation Kontakte hinzufügen.

Hinzufügen von Kontakten zu einer Rotation in einem Bereitschaftsplan in Incident Manager

Für jede Rotation in Ihrem Bereitschaftsplan können Sie einen oder mehrere Kontakte hinzufügen, bis zu insgesamt 30. Sie wählen aus Kontakten, die in Ihrer Incident Manager-Konfiguration eingerichtet sind.

Wenn Sie einen Kontakt zu einer Rotation hinzufügen, kann der Kontakt im Rahmen seiner Bereitschaftsdienste Benachrichtigungen erhalten. Benachrichtigungen können per E-Mail, SMS oder Sprachanruf gesendet werden, wie in den Kontaktdetails angegeben.

Informationen zur Verwaltung Ihrer Kontakte und zu den Benachrichtigungsoptionen für Kontakte finden Sie unterMit Kontakten im Incident Manager arbeiten.

So fügen Sie Kontakte zu einer Rotation in einem Bereitschaftsplan hinzu

1. Wählen Sie auf der Seite Bereitschaftsplan erstellen im Abschnitt Kontakte für die Rotation die Option Kontakte hinzufügen oder entfernen aus.
2. Wählen Sie im Dialogfeld Kontakte hinzufügen oder entfernen die Aliase der Kontakte aus, die in die Rotation aufgenommen werden sollen.

   Die Reihenfolge, in der Sie die Kontakte auswählen, ist die Reihenfolge, in der sie zuerst im Rotationsplan aufgeführt werden. Sie können die Reihenfolge ändern, nachdem Sie Kontakte hinzugefügt haben.
3. Wählen Sie Confirm (Bestätigen).
4. Um die Position eines Kontakts in der Bestellung zu ändern, wählen Sie das Optionsfeld für diesen Benutzer aus und verwenden Sie die Schaltflächen Nach oben

( ) und Nach unten ( ), um die Kontaktreihenfolge zu aktualisieren.

5. Fahren Sie fort, indem Sie die individuelle Schichtwiederholung und die Länge für die Rotation angeben.

Festlegung der Schichtwiederholung und -länge und Hinzufügen von Schlagwörtern zu einer Rotation in Incident Manager

Die Schichtwiederholung gibt an, wie oft die Kontakte in einer Rotation zu- und abwechseln, wenn sie in Bereitschaft sind. Die Wiederholungsdauer kann in einer Anzahl von Tagen, Wochen oder Monaten angegeben werden.

Um die Schichtwiederholung und -länge festzulegen und einer Rotation Beschriftungen hinzuzufügen

1. Gehen Sie auf der Seite Bereitschaftsplan erstellen im Abschnitt Wiederholungseinstellungen für die Rotation wie folgt vor:

   - Geben Sie für die Art der Schichtwiederholung an, ob jede Schicht des Bereitschaftsdienstes mehrere Tage, Wochen oder Monate dauert, indem Sie zwischen `Daily`, `Weekly`, und wählen. `Monthly`
   - Geben Sie unter Schichtdauer ein, wie viele Tage, Wochen oder Monate eine Schicht dauert.

     Wenn Sie beispielsweise auswählen `Daily` und teilnehmen**1**, dauert die Bereitschaftsschicht jedes Kontakts einen Tag. Wenn Sie sich dafür entscheiden `Weekly` und teilnehmen**3**, dauert die Bereitschaftsschicht jedes Kontakts drei Wochen.

2. (Optional) Wenden Sie im Bereich Tags ein oder mehrere Tag-Schlüsselnamen- und Wertepaare auf die Rotation an.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können beispielsweise eine Rotation taggen, um den Standort der ihr zugewiesenen Kontakte, die Art der Deckung, die sie bieten soll, oder den Eskalationsplan, den sie unterstützen wird, zu identifizieren. Weitere Informationen zum Taggen von Incident Manager-Ressourcen finden Sie unterTaggen von Ressourcen in Incident Manager.

3. (Empfohlen) Verwenden Sie die Kalendervorschau, um sicherzustellen, dass es bei Ihrem Bereitschaftsplan keine unbeabsichtigten Lücken in der Deckung gibt.
4. Wählen Sie Create (Erstellen) aus.

Sie können den Bereitschaftsplan jetzt als Eskalationskanal in einen Eskalationsplan aufnehmen. Weitere Informationen finden Sie unter Erstellen Sie einen Eskalationsplan.

Verwaltung eines bestehenden Bereitschaftsplans im Incident Manager

Verwenden Sie die Inhalte in diesem Abschnitt, um Ihnen bei der Arbeit mit Bereitschaftsplänen zu helfen, die Sie bereits erstellt haben.

Themen

- Details zum Bereitschaftsdienst anzeigen
- Einen Bereitschaftsplan bearbeiten
- Einen Bereitschaftsplan kopieren
- Eine Außerkraftsetzung für eine Rotation des Bereitschaftsdienstes erstellen
- Löschen eines Bereitschaftsplans

Details zum Bereitschaftsdienst anzeigen

Eine at-a-glance Zusammenfassung eines Bereitschaftsplans finden Sie auf der Seite Bereitschaftsplandetails anzeigen. Diese Seite enthält auch Informationen darüber, wer gerade auf Abruf ist und wer als nächstes auf Abruf ist. Die Seite enthält eine Kalenderansicht, in der angezeigt wird, welche Kontakte zu einer bestimmten Zeit auf Abruf sind.

Um die Einzelheiten des Bereitschaftsdienstes einzusehen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.
3. Führen Sie in der Zeile, in der der Bereitschaftsplan angezeigt werden soll, einen der folgenden Schritte aus:

   - Um eine Übersichtsansicht des Kalenders zu öffnen, wählen Sie den Zeitplan-Alias.

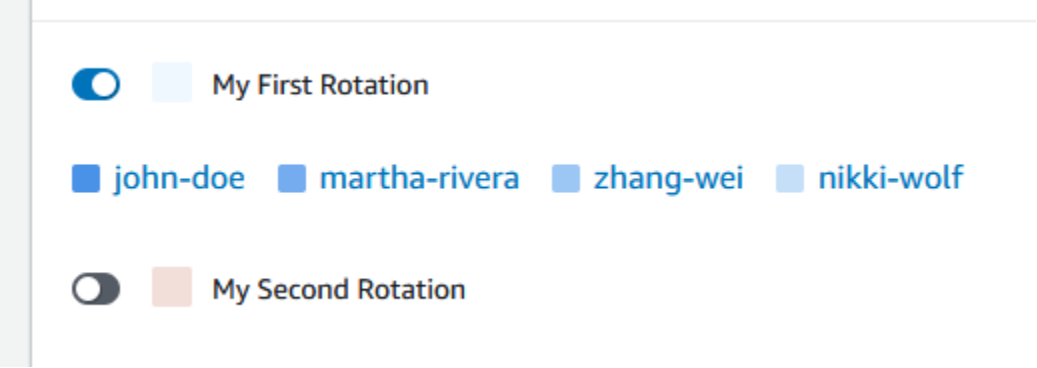
     –oder–

Wählen Sie das Optionsfeld für die Zeile aus, und wählen Sie dann Ansicht.

- Um eine Kalenderansicht des Zeitplans zu öffnen, wählen Sie Kalender anzeigen

  Wählen Sie in der Kalenderansicht den Namen eines Kontakts an einem bestimmten Datum im Zeitplan aus, um Details zur zugewiesenen Schicht zu sehen oder eine Überschreibung vorzunehmen.

- Um die Anzeige einer bestimmten Rotation im Kalender ein- oder auszuschalten, wählen Sie den Schalter neben dem Namen der Rotation.



Einen Bereitschaftsplan bearbeiten

Sie können die Konfiguration für einen Bereitschaftsplan und seine Rotationen aktualisieren, mit Ausnahme der folgenden Details:

- Der Zeitplan-Alias
- Namen der Rotation
- Startdaten der Rotation

Um einen vorhandenen Kalender als Grundlage für einen neuen Kalender mit der Möglichkeit zu verwenden, diese Werte zu ändern, können Sie stattdessen den Kalender kopieren. Weitere Informationen finden Sie unter Einen Bereitschaftsplan kopieren.

Um einen Bereitschaftsplan zu bearbeiten

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.

3. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie das Optionsfeld in der Zeile für den Bereitschaftsplan aus, den Sie bearbeiten möchten, und wählen Sie dann Bearbeiten.
   - Wählen Sie den Zeitplan-Alias für den Bereitschaftsplan, um die Seite „Bereitschaftsplandetails anzeigen“ zu öffnen, und wählen Sie dann Bearbeiten.
4. Nehmen Sie alle erforderlichen Änderungen am Bereitschaftsplan und seinen Rotationen vor. Sie können die Optionen zur Rotationskonfiguration wie Start- und Endzeiten, Kontakte und Wiederholung ändern. Sie können dem Zeitplan nach Bedarf Rotationen hinzufügen oder daraus entfernen. Die Kalendervorschau spiegelt Ihre Änderungen wider, sobald Sie sie vornehmen.

   Hinweise zum Arbeiten mit den Optionen auf der Seite finden Sie unterErstellung eines Bereitschaftsplans und einer Rotation im Incident Manager.
5. Wählen Sie Aktualisieren aus.

> **Important**
>
> Wenn Sie einen Zeitplan bearbeiten, der Überschreibungen enthält, können sich Ihre Änderungen auf die Überschreibungen auswirken. Um sicherzustellen, dass Ihre Überschreibungen wie erwartet konfiguriert bleiben, empfehlen wir, Ihre Schichtüberschreibungen genau zu überprüfen, nachdem Sie den Zeitplan aktualisiert haben.

Einen Bereitschaftsplan kopieren

Um die Konfiguration eines vorhandenen Bereitschaftsplans als Ausgangspunkt für einen neuen Zeitplan zu verwenden, können Sie eine Kopie des Kalenders erstellen und ihn nach Bedarf ändern.

Um einen Bereitschaftsplan zu kopieren

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.
3. Wählen Sie das Optionsfeld in der Zeile für den zu kopierenden Bereitschaftsplan aus.
4. Wählen Sie die Option Copy Kopieren aus.
5. Nehmen Sie alle erforderlichen Änderungen am Kalender und seinen Rotationen vor. Sie können Rotationen nach Bedarf ändern, hinzufügen oder entfernen.

> **Note**
>
> Wenn Sie einen vorhandenen Zeitplan kopieren, müssen Sie für jede Rotation neue Startdaten angeben. Kopierte Zeitpläne unterstützen keine Rotationen mit Startdaten in der Vergangenheit.

Hinweise zum Arbeiten mit den Optionen auf der Seite finden Sie unterErstellung eines Bereitschaftsplans und einer Rotation im Incident Manager.

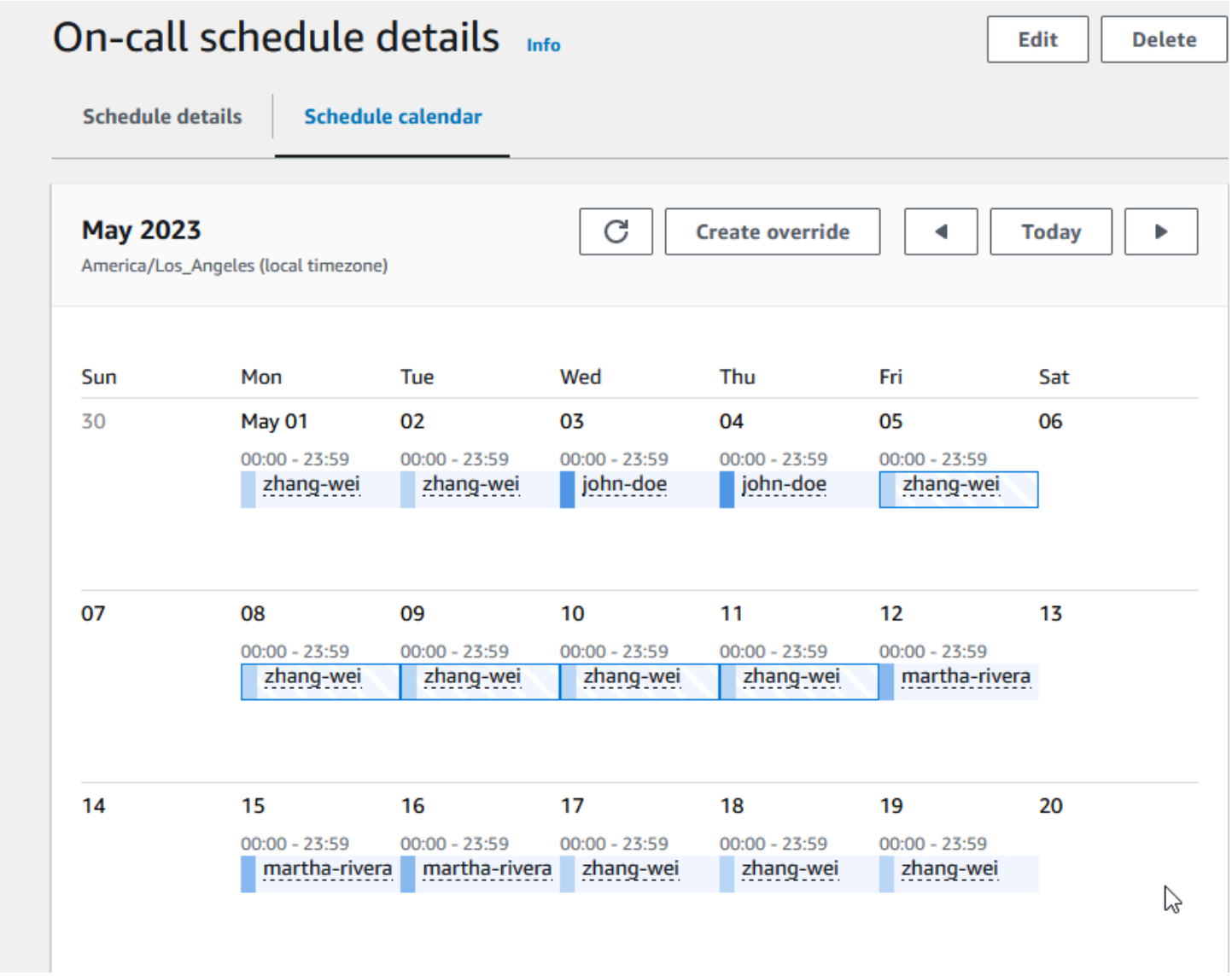
6. Wählen Sie Kopie erstellen.

Eine Außerkraftsetzung für eine Rotation des Bereitschaftsdienstes erstellen

Wenn Sie einmalige Änderungen an einem bestehenden Rotationsplan vornehmen müssen, können Sie eine Überschreibung erstellen. Mit einer Außerkraftsetzung können Sie die gesamte Schicht eines Kontakts oder einen Teil davon durch einen anderen Kontakt ersetzen. Sie können auch eine Überschreibung erstellen, die sich über mehrere Schichten erstreckt.

Sie können einem Override nur Kontakte zuweisen, die der Rotation bereits zugewiesen sind.

In der Kalendervorschau werden überschriebene Schichten mit einem gestreiften Hintergrund statt mit einem durchgehenden Hintergrund angezeigt. In der folgenden Abbildung können wir sehen, dass der Ansprechpartner Zhang Wei auf Abruf ist und Teile der Schichten für John Doe und Martha Rivera vom 5. Mai bis zum 11. Mai einschließt.



So erstellen Sie eine Außerkraftsetzung für einen Bereitschaftsplan

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.
3. Führen Sie in der Zeile, in der der Bereitschaftsplan angezeigt werden soll, einen der folgenden Schritte aus:
   - Wählen Sie den Zeitplan-Alias und dann den Tab Terminkalender aus.
   - Wählen Sie Kalender anzeigen
4. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie Create override aus.

- Wählen Sie in der Kalendervorschau den Namen eines Kontakts und wählen Sie dann Schicht überschreiben.

5. Gehen Sie im Dialogfeld „Shift-Override erstellen“ wie folgt vor:

> **Note**
>
> Ein Override muss mindestens 30 Minuten lang sein. Sie können eine Außerkraftsetzung nur für Schichten angeben, die nicht mehr als sechs Monate in der Zukunft liegen.

   a. Wählen Sie unter Drehung auswählen den Namen der Drehung aus, für die eine Überschreibung erstellt werden soll.
   b. Wählen Sie als Startdatum das Datum aus, an dem die Außerkraftsetzung beginnt, oder geben Sie es ein.
   c. Geben Sie unter Startzeit die Uhrzeit ein, zu der die Außerkraftsetzung beginnt, im `hh:mm` Format.
   d. Wählen Sie unter Enddatum das Datum aus, an dem die Außerkraftsetzung endet, oder geben Sie es ein.
   e. Geben Sie unter Endzeit die Uhrzeit ein, zu der die Außerkraftsetzung endet, im `hh:mm` Format.
   f. Wählen Sie unter „Kontakt zum Außerkraftsetzen auswählen“ den Namen des Rotationskontakts aus, der während des Außerkraftsetzungszeitraums auf Abruf ist.

6. Wählen Sie Create override aus.

Nachdem Sie eine Überschreibung erstellt haben, können Sie sie anhand des gestreiften Hintergrunds erkennen. Wenn Sie den Kontaktnamen für eine übergeordnete Schicht wählen, wird diese in einem Informationsfeld als übergeordnete Schicht gekennzeichnet. Sie können Delete override wählen, um den Vorgang zu entfernen und die ursprüngliche Bereitschaftszuweisung wiederherzustellen.

Löschen eines Bereitschaftsplans

Wenn Sie einen bestimmten Bereitschaftsplan nicht mehr benötigen, können Sie ihn aus dem Incident Manager löschen.

Wenn Eskalationspläne oder Reaktionspläne derzeit den Bereitschaftsplan als Eskalationskanal verwenden, sollten Sie ihn aus diesen Plänen entfernen, bevor Sie den Zeitplan löschen.

Um einen Bereitschaftsplan zu löschen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste Bereitschaftspläne aus.
3. Wählen Sie das Optionsfeld in der Zeile für den Bereitschaftsplan aus, den Sie löschen möchten.
4. Wählen Sie Löschen.
5. Im Bereitschaftsplan Löschen? Dialogfeld, geben Sie **`confirm`** in das Textfeld ein.
6. Wählen Sie Delete (Löschen).

Arbeiten mit Eskalationsplänen im Incident Manager

AWS Systems Manager Incident Managerbietet Eskalationswege über Ihre definierten Kontakte oder Bereitschaftspläne, die zusammen als Eskalationskanäle bezeichnet werden. Sie können mehrere Eskalationskanäle gleichzeitig in einen Incident einbeziehen. Wenn die angegebenen Kontakte im Eskalationskanal nicht antworten, eskaliert Incident Manager an die nächste Gruppe von Kontakten. Sie können auch wählen, ob ein Plan nicht mehr eskaliert, sobald ein Benutzer die Interaktion bestätigt. Sie können einem Reaktionsplan Eskalationspläne hinzufügen, sodass die Eskalation automatisch zu Beginn eines Vorfalls startet. Sie können einem aktiven Incident auch Eskalationspläne hinzufügen.

Themen

- Phasen
- Erstellen Sie einen Eskalationsplan

Phasen

Eskalationspläne verwenden Phasen, in denen jede Phase eine definierte Anzahl von Minuten dauert. Jede Phase hat die folgenden Informationen:

- Dauer — Die Zeit, die der Plan bis zum Beginn der nächsten Phase wartet. Die erste Phase des Eskalationsplans beginnt, sobald das Engagement beginnt.
- Eskalationskanal — Ein Eskalationskanal ist entweder ein einzelner Kontakt oder ein Bereitschaftsplan, der aus mehreren Kontakten besteht, die die Zuständigkeiten nach einem

definierten Zeitplan abwechseln. Der Eskalationsplan bindet jeden Kanal anhand seines definierten Engagementplans ein. Sie können jeden Eskalationskanal so einrichten, dass die Weiterentwicklung des Eskalationsplans gestoppt wird, bevor er zur nächsten Phase übergeht. Jede Phase kann mehrere Eskalationskanäle haben.

Weitere Informationen zum Festlegen einzelner Kontakte finden Sie unterMit Kontakten im Incident Manager arbeiten. Informationen zum Erstellen von Bereitschaftsplänen finden Sie unterArbeiten mit Bereitschaftsplänen im Incident Manager.

Erstellen Sie einen Eskalationsplan

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie im linken Navigationsbereich Eskalationspläne aus.
2. Wählen Sie Eskalationsplan erstellen.
3. Geben Sie unter Name einen eindeutigen Namen für den Eskalationsplan ein, z.**`My Escalation Plan`** B.
4. Geben Sie für Alias einen Alias ein, der Ihnen hilft, den Plan zu identifizieren, z.**`my-escalation-plan`** B.
5. Geben Sie unter Stagendauer die Anzahl der Minuten ein, die Incident Manager warten soll, bis zur nächsten Phase übergegangen wird.
6. Wählen Sie als Eskalationskanal einen oder mehrere Kontakte oder Bereitschaftspläne aus, um in dieser Phase Kontakt aufzunehmen.
7. (Optional) Wenn ein Kontakt den Eskalationsplan beenden soll, sobald er den Kontakt bestätigt hat, wählen Sie Bestätigung stoppt den Planfortschritt aus.
8. Um dieser Phase einen weiteren Kanal hinzuzufügen, wählen Sie Eskalationskanal hinzufügen.
9. Um dem Eskalationsplan eine weitere Stufe hinzuzufügen, wählen Sie Stufe hinzufügen.
10. Wiederholen Sie die Schritte 5 bis 9, bis Sie die gewünschten Eskalationskanäle und Stufen für diesen Eskalationsplan hinzugefügt haben.
11. (Optional) Wenden Sie im Bereich Tags ein oder mehrere Tag-Schlüssel-Name/Wert-Paare auf den Eskalationsplan an.

    Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Tags können Sie eine Ressource unterschiedlich kategorisieren, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können beispielsweise einen Eskalationsplan kennzeichnen, um die Art der Vorfälle zu identifizieren, für die er verwendet werden soll, welche Arten von Eskalationskanälen

er enthält oder welchen Eskalationsplan er unterstützt. Weitere Informationen zum Taggen von Incident Manager-Ressourcen finden Sie unterTaggen von Ressourcen in Incident Manager.

12. Wählen Sie Eskalationsplan erstellen.

Arbeiten mit Chat-Kanälen in Incident Manager

Incident Manager, eine Fähigkeit vonAWS Systems Manager, gibt Incident-Respondern die Möglichkeit, während eines Vorfalls direkt über Chat-Kanäle zu kommunizieren. Ein Chat-Kanal ist ein Chatraum, in dem Sie sich einrichten AWS Chatbot. Anschließend verbinden Sie diesen Kanal mit einem Reaktionsplan in Incident Manager.

Während eines Vorfalls nutzen die Einsatzkräfte den Chat-Kanal, um miteinander über den Vorfall zu kommunizieren. Incident Manager leitet außerdem alle Updates und Benachrichtigungen zu dem Vorfall direkt an den Chat-Kanal weiter. Diese Benachrichtigungen werden unter Verwendung eines oder mehreren Amazon Simple Notification Service (Amazon SNS) -Themen gesendet, die Sie in Ihrer Chatroom-Konfiguration angeben.

AWS Chatbotund Incident Manager unterstützen Chat-Kanäle in den folgenden Anwendungen:

- Slack
- Microsoft Teams
- Amazon Chime

Das Verfahren zum Einrichten eines Chat-Kanals für Ihre Incidents besteht aus Aufgaben in drei verschiedenen Amazon Web Services Services-Diensten.

Aufgaben

- Aufgabe 1: Amazon SNS SNS-Themen für Ihren Chat-Kanal erstellen oder aktualisieren
- Aufgabe 2: Erstellen eines Chat-Kanals inAWS Chatbot
- Aufgabe 3: Hinzufügen des Chat-Kanals zu einem Reaktionsplan in Incident Manager
- Interaktion über den Chat-Kanal

Aufgabe 1: Amazon SNS SNS-Themen für Ihren Chat-Kanal erstellen oder aktualisieren

Amazon SNS ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten (auch bekannt als Produzenten und Konsumenten) ermöglicht. Herausgeber kommunizieren asynchron mit Abonnenten, indem sie eine Nachricht erstellen und an ein Thema senden, bei dem es sich um einen logischen Zugriffspunkt und Kommunikationskanal handelt. Incident Manager verwendet ein oder mehrere Themen, die Sie einem Reaktionsplan zuordnen, um Benachrichtigungen über einen Vorfall an die Einsatzkräfte zu senden.

In einem Reaktionsplan können Sie ein oder mehrere Amazon SNS SNS-Themen zu Vorfallbenachrichtigungen hinzufügen. Als bewährte Methode sollten Sie für jedes Thema-Thema, dasAWS-Region Sie Ihrem Replikationssatz hinzugefügt haben.

> **Tip**
>
> Für einen linearen Einrichtungsablauf empfehlen wir, dass Sie Ihre Amazon SNS SNS-Themen zunächst für die Verwendung mit Incident Manager konfigurieren. Nach der Konfiguration können Sie den Chat-Kanal erstellen.

Um Amazon SNS SNS-Themen für Ihren Chat-Kanal zu erstellen oder zu aktualisieren

1. Folgen Sie den Schritten im Amazon SNS Service-Entwicklerhandbuch erstellen im Amazon Simple Notification Service-Entwicklerhandbuch.

   > **Note**
   >
   > Nachdem Sie das Thema erstellt haben, bearbeiten Sie es, um die Zugriffsrichtlinie zu aktualisieren.

2. Wählen Sie das Thema-Thema, das Sie erstellt haben, und notieren Sie den Amazon-Ressourcennamen (ARN) des Themas in einem Format wie`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
3. Wählen Sie Bearbeiten und erweitern Sie dann den Abschnitt Zugriffsrichtlinie, um zusätzliche Zugriffsberechtigungen zu konfigurieren, die über die Standardeinstellungen hinausgehen.
4. Fügen Sie dem Thema-Arma-Array der Richtlinie die folgende Anweisung hinzu:

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

Ersetzen Sie die *Platzhalterwerte* wie folgt:

- *sns-topic-arn*ist der Amazon-Ressourcenname (ARN) des Themas, das Sie für diese Region erstellt haben, im Format`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
- *Account-ID* ist die ID desAWS-Konto, in dem Sie arbeiten, z.`111122223333` B.

5. Wählen Sie Änderungen speichern.
6. Wiederholen Sie den Vorgang in jeder Region, die in Ihrem Replikationssatz enthalten ist.

Aufgabe 2: Erstellen eines Chat-Kanals inAWS Chatbot

Du kannst einen Chat-Kanal in Slack, Microsoft Teams oder Amazon Chime erstellen. Sie benötigen nur einen Chat-Kanal für jeden Antwortplan.

Für Ihre Chat-Kanäle empfehlen wir, dem Prinzip der geringsten Rechte zu folgen (Benutzern nicht mehr Berechtigungen zu gewähren, als sie für die Erledigung ihrer Aufgaben benötigen). Sie sollten auch regelmäßig die Mitgliedschaft IhrerAWS Chatbot Chat-Kanäle überprüfen. Mithilfe von Bewertungen können Sie überprüfen, ob nur die entsprechenden Responder und andere Beteiligte Zugriff auf Ihre Chat-Kanäle haben.

InAWS Chatbot aktivierten Slack-Channels und Microsoft Teams-Channels können Incident-Responder eine Reihe von Incident Manager-CLI-Befehlen direkt aus der Slack- oder Microsoft

Teams-Anwendung ausführen. Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

> **Important**
>
> Bei den Benutzern, die Sie Ihrem Chat-Kanal hinzufügen, muss es sich um dieselben Kontakte handeln, die in Ihrem Eskalations- oder Reaktionsplan aufgeführt sind. Sie können Chat-Kanälen auch weitere Benutzer hinzufügen, z. B. Beteiligte und Vorfallbeobachter.

Allgemeine InformationenAWS Chatbot dazu finden Sie unter Was istAWS Chatbot im AWS ChatbotAdministratorhandbuch.

Wähle aus den folgenden Anwendungen, um deinen Kanal zu erstellen:

Slack

Die Schritte in diesem Verfahren enthalten die empfohlenen Berechtigungseinstellungen, damit alle Kanalbenutzer Chat-Befehle mit Incident Manager verwenden können. Mithilfe unterstützter Chat-Befehle können deine Incident-Responder den Vorfall direkt über den Slack-Chat-Kanal aktualisieren und mit ihm interagieren. Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

So erstellst du einen Chat-Kanal in Slack

- Folge den Schritten unter Tutorial: Beginne mit Slack im AWS ChatbotAdministratorhandbuch und füge Folgendes in deine Konfiguration ein.
  - Wählen Sie in Schritt 10 für Rolleneinstellungen die Option Kanalrolle aus.
  - Wählen Sie in Schritt 10d für Richtlinienvorlagen die Option Incident Manager-Berechtigungen aus.
  - Wählen Sie in Schritt 11 für Channel Guardrail Policys als Richtlinienname die Option `AWSIncidentManagerResolverAccess`.
  - Gehen Sie in Schritt 12 im Abschnitt SNS-Themen wie folgt vor:
    - Wählen Sie für Region 1 eine aus,AWS-Region die in Ihrem Replikationssatz enthalten ist.
    - Wählen Sie für Themen 1 das SNS-Thema aus, das Sie in dieser Region erstellt haben, um Vorfallbenachrichtigungen an den Chat-Kanal zu senden.

- Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen und fügen Sie die zusätzlichen Regionen und SNS-Themen hinzu.

Microsoft Teams

Die Schritte in diesem Verfahren enthalten die empfohlenen Berechtigungseinstellungen, damit alle Kanalbenutzer Chat-Befehle mit Incident Manager verwenden können. Mithilfe unterstützter Chat-Befehle können Ihre Incident-Responder den Vorfall direkt über den Chat-Kanal von Microsoft Teams aktualisieren und mit ihm interagieren. Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

So erstellen Sie einen Chat-Kanal in Microsoft Teams

- Folgen Sie den Schritten unter Tutorial: Erste Schritte mit Microsoft Teams im AWS ChatbotAdministratorhandbuch und fügen Sie Folgendes in Ihre Konfiguration ein:
  - Wählen Sie in Schritt 10 für Rolleneinstellungen die Option Kanalrolle aus.
  - Wählen Sie in Schritt 10d für Richtlinienvorlagen die Option Incident Manager-Berechtigungen aus.
  - Wählen Sie in Schritt 11 für Channel Guardrail Policys als Richtlinienname die Option `AWSIncidentManagerResolverAccess`.
  - Gehen Sie in Schritt 12 im Abschnitt SNS-Themen wie folgt vor:
    - Wählen Sie für Region 1 eine aus,AWS-Region die in Ihrem Replikationssatz enthalten ist.
    - Wählen Sie für Themen 1 das SNS-Thema aus, das Sie in dieser Region erstellt haben, um Vorfallbenachrichtigungen an den Chat-Kanal zu senden.
    - Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen und fügen Sie die zusätzlichen Regionen und SNS-Themen hinzu.

Amazon Chime

So erstellen Sie einen Chat-Kanal in Amazon Chime

- Folgen Sie den Schritten unter Tutorial: Erste Schritte mit Amazon Chime im AWS ChatbotAdministratorhandbuch und fügen Sie Folgendes in Ihre Konfiguration ein:

- Wählen Sie in Schritt 11 für Richtlinienvorlagen die Option Incident Manager-Berechtigungen aus.
- Wählen Sie in Schritt 12 im Abschnitt SNS-Themen die SNS-Themen aus, die Benachrichtigungen an den Amazon Chime Chime-Webhook senden sollen:
  - Wählen Sie für Region 1 eine aus,AWS-Region die in Ihrem Replikationssatz enthalten ist.
  - Wählen Sie für Themen 1 das SNS-Thema aus, das Sie in dieser Region erstellt haben, um Vorfallbenachrichtigungen an den Chat-Kanal zu senden.
  - Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen und fügen Sie die zusätzlichen Regionen und SNS-Themen hinzu.

> **Note**
>
> Chat-Befehle, die Incident-Responder in den Chat-Kanälen von Slack und Microsoft Teams verwenden können, werden in Amazon Chime nicht unterstützt.

Aufgabe 3: Hinzufügen des Chat-Kanals zu einem Reaktionsplan in Incident Manager

Wenn Sie einen Reaktionsplan erstellen oder aktualisieren, können Sie Chat-Kanäle hinzufügen, über die die Responder kommunizieren und Updates erhalten können.

Wenn Sie den Schritten in diesem Abschnitt folgenErstellung eines Reaktionsplans, wählen Sie den Kanal aus (Optional) Angabe eines Chat-Kanals zur Reaktion auf Vorfälle, den Sie für Vorfälle im Zusammenhang mit diesem Reaktionsplan verwenden möchten.

Interaktion über den Chat-Kanal

Für Kanäle in Slack und Microsoft Teams ermöglicht Incident Manager den Respondern, mit den folgenden`ssm-incidents` Befehlen direkt vom Chat-Kanal aus mit Incidents zu interagieren:

- Zwischenfall starten
- 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

Verwenden Sie das folgende Format, um Befehle im Chat-Kanal eines aktiven Incidents auszuführen. Ersetzen Sie *cli-options* durch alle Optionen, die für einen Befehl enthalten sein sollen.

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

Beispiel:

```
@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
```

Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager

Sie können Runbooks von AWS Systems ManagerAutomation, einer Funktion von, verwendenAWS Systems Manager, um allgemeine Anwendungs- und Infrastrukturaufgaben in Ihrer AWS Cloud Umgebung zu automatisieren.

Jedes Runbook definiert einen Runbook-Workflow, der sich aus den Aktionen zusammensetzt, die Systems Manager auf Ihren verwalteten Knoten oder anderen AWS Ressourcentypen ausführt. Sie können Runbooks verwenden, um die Wartung, Bereitstellung und Problembehebung Ihrer AWS Ressourcen zu automatisieren.

In Incident Manager steuert ein Runbook die Reaktion auf Vorfälle und deren Abwehr, und Sie geben ein Runbook an, das als Teil eines Reaktionsplans verwendet werden soll.

In Ihren Reaktionsplänen können Sie aus Dutzenden von vorkonfigurierten Runbooks für häufig automatisierte Aufgaben wählen oder benutzerdefinierte Runbooks erstellen. Wenn Sie in einer Reaktionsplandefinition ein Runbook angeben, kann das System das Runbook automatisch starten, wenn ein Vorfall beginnt.

> **Important**
>
> Durch einen regionsübergreifenden Failover verursachte Vorfälle rufen keine in den Reaktionsplänen angegebenen Runbooks auf.

Weitere Informationen zu Systems Manager Automation, Runbooks und der Verwendung von Runbooks mit Incident Manager finden Sie in den folgenden Themen:

- Informationen zum Hinzufügen eines Runbooks zu einem Reaktionsplan finden Sie unterArbeiten mit Reaktionsplänen in Incident Manager.
- Weitere Informationen zu Runbooks finden Sie unter AWS Systems ManagerAutomatisierung im AWS Systems ManagerBenutzerhandbuch und in der AWS Systems ManagerAutomation-Runbook-Referenz.
- Informationen zu den Kosten für die Verwendung von Runbooks finden Sie unter Systems Manager-Preise.
- Informationen zum automatischen Aufrufen von Runbooks, wenn ein Incident durch einen CloudWatch Amazon-Alarm oder ein EventBridge Amazon-Ereignis ausgelöst wird, finden Sie unter Tutorial: Verwenden von Systems Manager Automation-Runbooks mit Incident Manager.

Themen

- Definieren Sie ein Runbook
- Incident Manager-Runbook-Vorlage

IAM-Berechtigungen sind erforderlich, um Runbook-Workflows zu starten und auszuführen

Incident Manager benötigt Berechtigungen, um Runbooks als Teil Ihrer Incident-Response ausführen zu können. Um diese Berechtigungen bereitzustellen, verwenden Sie AWS Identity and Access Management (IAM-) Rollen, die Runbook-Servicerolle und die Automatisierung. *`AssumeRole`*

Die Runbook-Servicerolle ist eine erforderliche Servicerolle. Diese Rolle gewährt dem Incident Manager die Berechtigungen, die er benötigt, um auf den Workflow für das Runbook zuzugreifen und ihn zu starten.

Die Automatisierung `AssumeRole` bietet die erforderlichen Berechtigungen, um die einzelnen Befehle auszuführen, die im Runbook angegeben sind.

> **Note**
>
> Wenn nein angegeben `AssumeRole` ist, versucht Systems Manager Automation, die Runbook-Servicerolle für einzelne Befehle zu verwenden. Wenn Sie keine angeben`AssumeRole`, müssen Sie der Runbook-Servicerolle die erforderlichen Berechtigungen hinzufügen. Wenn Sie dies nicht tun, kann das Runbook diese Befehle nicht ausführen.
> Aus Sicherheitsgründen empfehlen wir jedoch, eine separate Methode zu verwenden`AssumeRole`. Mit einer separaten `AssumeRole` Funktion können Sie die erforderlichen Berechtigungen einschränken, die Sie jeder Rolle hinzufügen müssen.

Weitere Informationen zur Automatisierung `AssumeRole` finden Sie unter „Konfiguration eines Zugriffs mit einer Servicerolle (Rolle übernehmen) für Automatisierungen“ im AWS Systems ManagerBenutzerhandbuch.

Sie können beide Rollentypen manuell selbst in der IAM-Konsole erstellen.- Sie können Incident Manager auch einen Rollentyp für Sie erstellen lassen, wenn Sie einen Reaktionsplan erstellen oder aktualisieren.

Berechtigungen für Runbook-Servicerolle

Runbook-Servicerollenberechtigungen werden über eine Richtlinie bereitgestellt, die der folgenden ähnelt.

Die erste Anweisung ermöglicht es Incident Manager, den Systems `StartAutomationExecution` Manager-Betrieb zu starten. Dieser Vorgang wird dann auf Ressourcen ausgeführt, die durch die drei Amazon Resource Name (ARN) -Formate repräsentiert werden.

Die zweite Anweisung ermöglicht es der Runbook-Servicerolle, eine Rolle in einem anderen Konto anzunehmen, wenn dieses Runbook in dem betroffenen Konto ausgeführt wird. Weitere Informationen finden Sie im Benutzerhandbuch unter Automatisierungen in mehreren AWS-Regionen Endkonten ausführen. AWS Systems Manager

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}: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"
        }
      }
    }
  ]
}
```

AssumeRole Automatisierungsberechtigungen

Wenn Sie einen Reaktionsplan erstellen oder aktualisieren, können Sie aus mehreren AWS verwalteten Richtlinien wählen, die Sie an AssumeRole die vom Incident Manager erstellten Richtlinien anhängen möchten. Diese Richtlinien gewähren Berechtigungen zur Ausführung einer

Reihe gängiger Operationen, die in Incident Manager-Runbook-Szenarien verwendet werden. Sie können eine oder mehrere dieser verwalteten Richtlinien auswählen, um Berechtigungen für Ihre `AssumeRole` Richtlinie bereitzustellen. In der folgenden Tabelle werden die Richtlinien beschrieben, aus denen Sie bei der Erstellung und in der Incident Manager-Konsole wählen können. `AssumeRole`

Name der von AWS verwalteten Richtlinie	Beschreibung der Richtlinie
`AmazonSSMAutomationRole`	Erteilt dem Systems Manager Automation-Dienst Berechtigungen zum Ausführen von Aktivitäten, die in Runbooks definiert sind. Weisen Sie diese Richtlinie Administratoren und vertrauenswürdigen Hauptbenutzern zu.
`AWSIncidentManagerResolverAccess`	Erteilt Benutzern die Berechtigung, Vorfälle zu starten, anzusehen und zu aktualisieren. Sie können sie auch verwenden, um im Incident-Dashboard Kunden-Timeline, Ereignisse und verwandte Elemente zu erstellen.

Sie können diese verwalteten Richtlinien verwenden, um Berechtigungen für viele gängige Szenarien zur Reaktion auf Vorfälle zu gewähren. Die für die spezifischen Aufgaben, die Sie benötigen, erforderlichen Berechtigungen können jedoch variieren. In diesen Fällen müssen Sie zusätzliche Richtlinienberechtigungen für Ihre bereitstellen`AssumeRole`. Informationen finden Sie in der AWS Systems ManagerAutomation-Runbook-Referenz.

Arbeiten mit Runbook-Parametern

Wenn Sie einem Antwortplan ein Runbook hinzufügen, können Sie die Parameter angeben, die das Runbook zur Laufzeit verwenden soll. Reaktionspläne unterstützen Parameter mit statischen und dynamischen Werten. Für statische Werte geben Sie den Wert ein, wenn Sie den Parameter im Reaktionsplan definieren. Für dynamische Werte ermittelt das System den richtigen Parameterwert, indem es Informationen aus dem Vorfall sammelt. Incident Manager unterstützt die folgenden dynamischen Parameter:

`Incident ARN`

Wenn Incident Manager einen Vorfall erstellt, erfasst das System den Amazon-Ressourcennamen (ARN) des entsprechenden Vorfalls-Datensatzes und trägt ihn für diesen Parameter in das Runbook ein.

> **Note**
>
> Dieser Wert kann nur Parametern des Typs `String` zugewiesen werden. Wenn er einem Parameter eines anderen Typs zugewiesen wird, kann das Runbook nicht ausgeführt werden.

`Involved resources`

Wenn Incident Manager einen Vorfall erstellt, erfasst das System die ARNs der an dem Vorfall beteiligten Ressourcen. Diese Ressourcen-ARNs werden dann diesem Parameter im Runbook zugewiesen.

Über zugehörige Ressourcen

Incident Manager kann Runbook-Parameterwerte mit den ARNs der AWS Ressourcen füllen, die in CloudWatch Alarmen, EventBridge Ereignissen und manuell erstellten Incidents angegeben sind. In diesem Abschnitt werden die verschiedenen Arten von Ressourcen beschrieben, für die Incident Manager beim Ausfüllen dieses Parameters ARNs erfassen kann.

CloudWatch-Alarme

Wenn aus einer CloudWatch Alarmaktion ein Vorfall entsteht, extrahiert Incident Manager automatisch die folgenden Arten von Ressourcen aus den zugehörigen Metriken. Anschließend werden die ausgewählten Parameter mit den folgenden beteiligten Ressourcen gefüllt:

AWS-Service	Ressourcentyp
Amazon DynamoDB	Globale sekundäre Indizes
	Streams
	Tabellen

AWS-Service	Ressourcentyp
Amazon EC2	Images Instances
AWS Lambda	Funktionsaliase Funktionsversionen Funktionen
Amazon Relational Database Service (Amazon RDS)	Cluster Datenbankinstanzen
Amazon Simple Storage Service (Amazon S3)	Buckets

EventBridge-Regeln

Wenn das System aus einem EventBridge Ereignis einen Incident erstellt, füllt der Incident Manager die ausgewählten Parameter mit der `Resources` Eigenschaft im Ereignis auf. Weitere Informationen finden Sie unter EventBridgeAmazon-Events im EventBridgeAmazon-Benutzerhandbuch.

Manuell erstellte Vorfälle

Wenn Sie mithilfe der StartIncidentAPI-Aktion einen Incident erstellen, füllt der Incident Manager die ausgewählten Parameter anhand der Informationen im API-Aufruf auf. Insbesondere füllt es Parameter auf, indem es Elemente des Typs verwendet`INVOLVED_RESOURCE`, die im `relatedItems` Parameter übergeben werden.

> **Note**
>
> Der `INVOLVED_RESOURCES` Wert kann nur Parametern vom Typ zugewiesen werden`StringList`. Wenn er einem Parameter eines anderen Typs zugewiesen wird, kann das Runbook nicht ausgeführt werden.

Definieren Sie ein Runbook

Wenn Sie ein Runbook erstellen, können Sie die hier aufgeführten Schritte befolgen oder die detailliertere Anleitung im Abschnitt Arbeiten mit Runbooks im Systems Manager-Benutzerhandbuch befolgen. Wenn Sie ein Runbook mit mehreren Konten AWS-Regionenund Regionen erstellen, finden Sie weitere Informationen unter Automatisierungen in mehreren Endkonten ausführen im Systems Manager-Benutzerhandbuch.

Definieren Sie ein Runbook

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
3. Wählen Sie Create automation (Automation erstellen).
4. Geben Sie einen eindeutigen und identifizierbaren Runbook-Namen ein.
5. Geben Sie eine Beschreibung des Runbooks ein.
6. Geben Sie eine IAM-Rolle an, die das Automatisierungsdokument übernehmen soll. Dadurch kann das Runbook Befehle automatisch ausführen. Weitere Informationen finden Sie unter Konfiguration eines Servicerollenzugriffs für Automatisierungs-Workflows.
7. (Optional) Fügen Sie alle Eingabeparameter hinzu, mit denen das Runbook beginnt. Sie können dynamische oder statische Parameter verwenden, wenn Sie ein Runbook starten. Dynamische Parameter verwenden Werte aus dem Incident, bei dem das Runbook gestartet wurde. Statische Parameter verwenden den von Ihnen angegebenen Wert.
8. (Optional) Fügen Sie einen Zieltyp hinzu.
9. (Optional) Fügen Sie Schlagworte hinzu.
10. Geben Sie die Schritte ein, die das Runbook ausführen wird, wenn es ausgeführt wird. Jeder Schritt erfordert:
    - Ein Name.
    - Eine Beschreibung des Zwecks des Schritts.
    - Die Aktion, die während des Schritts ausgeführt werden soll. Runbooks verwenden den Aktionstyp Pause, um einen manuellen Schritt zu beschreiben.
    - (Optional) Befehlseigenschaften.
11. Nachdem Sie alle erforderlichen Runbook-Schritte hinzugefügt haben, wählen Sie Create Automation aus.

Um die kontoübergreifende Funktionalität zu aktivieren, teilen Sie das Runbook in Ihrem Verwaltungskonto mit allen Anwendungskonten, die das Runbook während eines Vorfalls verwenden.

Ein Runbook teilen

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
3. Wählen Sie in der Dokumentenliste das Dokument aus, das Sie teilen möchten, und wählen Sie dann Details anzeigen. Überprüfen Sie dann auf der Registerkarte Permissions, ob Sie der Besitzer des Dokuments sind. Nur der Eigentümer eines Dokuments kann ein Dokument freigeben.
4. Wählen Sie Edit (Bearbeiten) aus.
5. Um den Befehl öffentlich freizugeben, wählen Sie Public und dann die Option Save. Wählen Sie zur privaten Freigabe des Befehls die Option Private aus, geben Sie die AWS-Konto-ID ein und wählen Sie Add permission sowie anschließend die Option Save aus.

Incident Manager-Runbook-Vorlage

Incident Manager stellt die folgende Runbook-Vorlage bereit, um Ihrem Team zu helfen, mit der Erstellung von Runbooks in Systems Manager Automation zu beginnen. Sie können diese Vorlage unverändert verwenden oder sie bearbeiten, um spezifische Informationen zu Ihrer Anwendung und Ihren Ressourcen hinzuzufügen.

Suchen Sie nach der Incident Manager-Runbook-Vorlage

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
3. Geben Sie **`AWSIncidents-`** im Bereich Dokumente das Suchfeld ein, um alle Incident Manager-Runbooks anzuzeigen.

> **Tip**
>
> Geben Sie den Text **`AWSIncidents-`** als freien Text ein, anstatt die Filteroption für das Präfix für den Dokumentennamen zu verwenden.

Verwenden einer Vorlage

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
3. Wählen Sie die Vorlage, die Sie aktualisieren möchten, aus der Dokumentenliste aus.
4. Wählen Sie die Registerkarte Inhalt und kopieren Sie dann den Inhalt des Dokuments.
5. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
6. Wählen Sie Create automation (Automation erstellen).
7. Geben Sie einen eindeutigen und identifizierbaren Namen ein.
8. Wählen Sie den Tab Editor.
9. Wählen Sie Edit (Bearbeiten) aus.
10. Fügen Sie die kopierten Details in den Bereich des Dokumenteditors ein oder geben Sie sie ein.
11. Wählen Sie Create automation (Automation erstellen).

`AWSIncidents-CriticalIncidentRunbookTemplate`

Das `AWSIncidents-CriticalIncidentRunbookTemplate` ist eine Vorlage, die den Incident Manager-Incident-Lebenszyklus in manuellen Schritten darstellt. Diese Schritte sind allgemein genug, um sie in den meisten Anwendungen zu verwenden, aber detailliert genug, damit die Einsatzkräfte mit der Problemlösung beginnen können.

Arbeiten mit Reaktionsplänen in Incident Manager

Mit Reaktionsplänen können Sie planen, wie Sie auf einen Vorfall reagieren, der sich auf Ihre Benutzer auswirkt. Ein Reaktionsplan dient als Vorlage, die Informationen darüber enthält, an wen Sie sich wenden müssen, wie schwer das Ereignis zu erwarten ist, welche automatischen Runbooks initiiert werden müssen und welche Kennzahlen überwacht werden müssen.

Bewährte Methoden

Sie können die Auswirkungen von Vorfällen auf Ihre Teams reduzieren, wenn Sie Vorfälle im Voraus planen. Teams sollten bei der Erstellung eines Reaktionsplans die folgenden bewährten Methoden berücksichtigen.

- Optimiertes Engagement — Identifizieren Sie das Team, das für einen Vorfall am besten geeignet ist. Wenn Sie mit einer zu großen Verteilerliste oder mit den falschen Teams zusammenarbeiten, können Sie während eines Vorfalls Verwirrung stiften und Reaktionszeit verschwenden.
- Zuverlässige Eskalation — Für Ihre Engagements im Rahmen eines Reaktionsplans empfehlen wir, einen Einsatzplan anstelle von Kontakten oder Bereitschaftszeiten zu wählen. Der Einsatzplan sollte die einzelnen Ansprechpartner oder Bereitschaftszeitpläne (die mehrere wechselnde Ansprechpartner enthalten) angeben, die bei Vorfällen aktiv werden sollen. Da die in Ihrem Einsatzplan angegebenen Einsatzkräfte manchmal nicht erreichbar sein können, sollten Sie in Ihrem Reaktionsplan Ersatzkräfte einrichten, um diese Szenarien abzudecken. Wenn die primären und sekundären Ansprechpartner nicht verfügbar sind oder andere ungeplante Lücken in der Abdeckung bestehen, benachrichtigt Incident Manager dennoch einen Kontakt über den Vorfall.
- Runbooks — Verwenden Sie Runbooks, um wiederholbare, verständliche Schritte bereitzustellen, die den Stress reduzieren, dem ein Einsatzkräfte während eines Vorfalls ausgesetzt ist.
- Zusammenarbeit — Nutzen Sie Chat-Kanäle, um die Kommunikation bei Vorfällen zu optimieren. Chat-Kanäle helfen den Einsatzkräften, über Informationen auf dem Laufenden zu bleiben. Über diese Kanäle können sie auch Informationen mit anderen Respondern teilen.

Erstellung eines Reaktionsplans

Gehen Sie wie folgt vor, um einen Reaktionsplan zu erstellen und die Reaktion auf Vorfälle zu automatisieren.

Um einen Reaktionsplan zu erstellen

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie im Navigationsbereich Reaktionspläne aus.
2. Wählen Sie Reaktionsplan erstellen aus.
3. Geben Sie unter Name einen eindeutigen und identifizierbaren Namen für den Reaktionsplan ein, der im Amazon-Ressourcennamen (ARN) für den Reaktionsplan verwendet werden soll.
4. (Optional) Geben Sie unter Displayname einen besser lesbaren Namen ein, um den Reaktionsplan leichter identifizieren zu können, wenn Sie Incidents erstellen.
5. Fahren Sie fort, indem Sie Standardwerte für Incident-Datensätze angeben.

Standardwerte für Vorfälle angeben

Damit Sie Vorfälle effektiver verwalten können, können Sie Standardwerte angeben. Incident Manager wendet diese Werte auf alle Vorfälle an, die einem Reaktionsplan zugeordnet sind.

Um Standardwerte für Vorfälle anzugeben

1. Geben Sie unter Titel einen Titel für diesen Vorfall ein, damit Sie ihn auf der Incident Manager-Startseite leichter identifizieren können.
2. Wählen Sie unter Auswirkung eine Auswirkungsstufe aus, um den potenziellen Umfang eines Vorfalls anzugeben, der auf der Grundlage dieses Reaktionsplans ausgelöst wurde, z. B. Kritisch oder Niedrig. Informationen zu den Einstufungen der Auswirkungen in Incident Manager finden Sie unterTriage.
3. (Optional) Geben Sie unter Zusammenfassung eine kurze Zusammenfassung der Art der Vorfälle ein, die anhand dieses Reaktionsplans erstellt wurden.
4. (Optional) Geben Sie für Deduplizierungszeichenfolge eine Deduplizierungszeichenfolge ein. Incident Manager verwendet diese Zeichenfolge, um zu verhindern, dass dieselbe Grundursache mehrere Vorfälle in demselben Konto verursacht.

   Eine Deduplizierungszeichenfolge ist ein Begriff oder ein Ausdruck, den das System verwendet, um nach doppelten Vorfällen zu suchen. Wenn Sie eine Deduplizierungszeichenfolge angeben, sucht Incident Manager bei der Erstellung des Vorfalls nach offenen Vorfällen, die dieselbe Zeichenfolge in dem `dedupeString` Feld enthalten. Wenn ein Duplikat erkannt wird, dedupliziert Incident Manager den neueren Vorfall in den vorhandenen Incident.

   > **Note**
   >
   > Standardmäßig dedupliziert Incident Manager automatisch mehrere Vorfälle, die durch denselben CloudWatch Amazon-Alarm oder dasselbe Amazon-Ereignis verursacht wurden. EventBridge Sie müssen keine eigene Deduplizierungszeichenfolge eingeben, um eine Duplizierung für diese Ressourcentypen zu verhindern.

5. (Optional) Fügen Sie unter Incident-Tags Tag-Schlüssel und Werte hinzu, die Sie Incidents zuweisen möchten, die anhand dieses Reaktionsplans erstellt wurden.

   Sie müssen über die `TagResource` Berechtigung für die Incident-Datensatzressource verfügen, um Incident-Tags innerhalb des Reaktionsplans festzulegen.

6. Geben Sie anschließend einen optionalen Chat-Kanal an, über den die Problemlöser miteinander über Vorfälle kommunizieren können.

(Optional) Angabe eines Chat-Kanals zur Reaktion auf Vorfälle

Wenn Sie einen Chat-Kanal in einen Reaktionsplan aufnehmen, erhalten die Einsatzkräfte über diesen Kanal aktuelle Informationen zum Vorfall. Mithilfe von Chat-Befehlen können sie direkt vom Chat-Kanal aus mit dem Vorfall interagieren.

Mithilfe AWS Chatbot können Sie einen Channel für Slack oder Amazon Chime erstellen, den Sie in Ihren Reaktionsplänen verwenden können. Informationen zum Erstellen eines Chat-Kanals in finden Sie im AWS Chatbot AWS ChatbotAdministratorhandbuch.

> **Important**
>
> Der Incident Manager muss berechtigt sein, Beiträge im Amazon Simple Notification Service (Amazon SNS) -Thema eines Chat-Kanals zu veröffentlichen. Wenn Sie nicht berechtigt sind, dieses SNS-Thema zu veröffentlichen, können Sie es nicht zum Reaktionsplan hinzufügen. Incident Manager veröffentlicht eine Testbenachrichtigung zum SNS-Thema, um die Berechtigungen zu überprüfen.

Weitere Informationen zu Chat-Kanälen finden Sie unterArbeiten mit Chat-Kanälen in Incident Manager.

So geben Sie einen Chat-Kanal zur Reaktion auf Vorfälle an

1. Wählen Sie unter Chat-Kanal einen AWS Chatbot Chat-Kanal aus, über den die Einsatzkräfte während eines Vorfalls kommunizieren können.

   > **Tip**
   >
   > Um einen neuen Chat-Kanal zu erstellenAWS Chatbot, wählen Sie Neuen Chatbot-Client konfigurieren.

2. Wählen Sie für SNS-Themen für Chat-Kanäle zusätzliche SNS-Themen aus, zu denen Sie während des Vorfalls etwas veröffentlichen möchten. Wenn mehrere SNS-Themen hinzugefügt werden, AWS-Regionen erhöht sich die Redundanz für den Fall, dass eine Region zum Zeitpunkt des Vorfalls nicht verfügbar ist.

3. Wählen Sie anschließend die Ansprechpartner, Bereitschaftszeiten und Eskalationspläne aus, die während eines Vorfalls hinzugezogen werden sollen.

(Optional) Wählen Sie die Ressourcen aus, die für die Reaktion auf Vorfälle zuständig sind

Es ist wichtig, die am besten geeigneten Ansprechpartner zu finden, wenn ein Vorfall eintritt. Als bewährte Methode empfehlen wir, dass Sie wie folgt vorgehen:

1. Fügen Sie Kontakte und Bereitschaftszeiten als Eskalationskanäle in einem Eskalationsplan hinzu.
2. Wählen Sie einen Eskalationsplan als Engagement in einem Reaktionsplan.

Weitere Informationen zu Kontakten und Eskalationsplänen finden Sie unter Mit Kontakten im Incident Manager arbeiten und. Arbeiten mit Eskalationsplänen im Incident Manager

Um Ressourcen für die Reaktion auf Vorfälle auszuwählen

1. Wählen Sie für Engagements eine beliebige Anzahl von Eskalationsplänen, Bereitschaftszeiten und individuellen Kontakten aus.
2. Fahren Sie fort, indem Sie optional ein Runbook angeben, das im Rahmen Ihrer Schadensbegrenzung ausgeführt werden soll.

(Optional) Geben Sie ein Runbook zur Schadensbegrenzung an

Sie können Runbooks von AWS Systems ManagerAutomation, einer Funktion von, verwendenAWS Systems Manager, um allgemeine Anwendungs- und Infrastrukturaufgaben in Ihrer Umgebung zu automatisieren. AWS Cloud

Jedes Runbook definiert einen Runbook-Workflow. Ein Runbook-Workflow umfasst die Aktionen, die Systems Manager auf Ihren verwalteten Knoten oder anderen AWS Ressourcentypen ausführt. In Incident Manager steuert ein Runbook die Reaktion auf Vorfälle und deren Behebung.

Weitere Informationen zur Verwendung von Runbooks in Reaktionsplänen finden Sie unter. Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager

So geben Sie ein Runbook zur Minderung von Vorfällen an:

1. Führen Sie für Runbook einen der folgenden Schritte aus:

- Wählen Sie Runbook aus Vorlage klonen, um eine Kopie des standardmäßigen Incident Manager-Runbooks zu erstellen. Geben Sie unter Runbook-Name einen aussagekräftigen Namen für das neue Runbook ein.
- Wählen Sie Bestehendes Runbook auswählen aus. Wählen Sie den Besitzer, das Runbook und die Version aus, die Sie verwenden möchten.

> **Tip**
>
> Um ein Runbook von Grund auf neu zu erstellen, wählen Sie Neues Runbook konfigurieren.
> Weitere Informationen zum Erstellen eines Runbooks finden Sie unter Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager.

2. Geben Sie im Bereich Parameter alle angeforderten Parameter für das von Ihnen ausgewählte Runbook ein.

   Die verfügbaren Parameter sind die vom Runbook angegebenen. Ein Runbook benötigt möglicherweise andere Parameter als ein anderes. Einige Parameter sind möglicherweise erforderlich und andere optional.

   In vielen Fällen können Sie einen statischen Wert für einen Parameter manuell eingeben, z. B. eine Liste von Amazon EC2 EC2-Instance-IDs. Sie können Incident Manager auch die Parameterwerte bereitstellen lassen, die durch einen Incident dynamisch generiert wurden.

3. (Optional) Geben Sie für AutomationAssumeRoledie zu AWS Identity and Access Management verwendende (IAM-) Rolle an. Diese Rolle muss über die erforderlichen Berechtigungen verfügen, um die einzelnen Befehle auszuführen, die im Runbook angegeben sind.

   > **Note**
   >
   > Wenn nichts angegeben `AssumeRole` ist, versucht Incident Manager, die Runbook-Dienstrolle zu verwenden, um die einzelnen Befehle auszuführen, die im Runbook angegeben sind.

   Wählen Sie eine der folgenden Optionen aus:

- ARN-Wert eingeben — Geben Sie den Amazon-Ressourcennamen (ARN) eines AssumeRole manuell im Format ein`arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`*. Zum Beispiel **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
- Bestehende Servicerolle verwenden — Wählen Sie eine Rolle mit den erforderlichen Berechtigungen aus einer Liste vorhandener Rollen in Ihrem Konto aus.
- Neue Servicerolle erstellen — Wählen Sie aus den AWS verwalteten Richtlinien, die Sie Ihrer hinzufügen möchten AssumeRole. Nachdem Sie diese Option ausgewählt haben, wählen Sie für AWSverwaltete Richtlinien eine oder mehrere Richtlinien aus der Liste aus.

  Sie können den vorgeschlagenen Standardnamen für die neue Rolle akzeptieren oder einen Namen Ihrer Wahl eingeben.

  > **Note**
  >
  > Diese neue Runbook-Dienstrolle ist dem spezifischen Runbook zugeordnet, das Sie ausgewählt haben. Sie kann nicht mit verschiedenen Runbooks verwendet werden. Das liegt daran, dass der Ressourcenbereich der Richtlinie keine anderen Runbooks unterstützt.

4. Geben Sie für die Runbook-Dienstrolle die IAM-Rolle an, die verwendet werden soll, um die Berechtigungen bereitzustellen, die für den Zugriff auf das Runbook selbst und den Start des Workflows erforderlich sind.

   Die Rolle muss mindestens die `ssm:StartAutomationExecution` Aktion für Ihr spezielles Runbook zulassen. Damit das Runbook kontenübergreifend funktioniert, muss die Rolle auch die `sts:AssumeRole` Aktion für die Rolle zulassen, die Sie in der `AWS-SystemsManager-AutomationExecutionRole` Rolle erstellt haben. Regions- und kontenübergreifendes Incident-Management im Incident Manager

   Wählen Sie eine der folgenden Optionen aus:

   - Neue Servicerolle erstellen — Incident Manager erstellt für Sie eine Runbook-Servicerolle, die die zum Starten des Runbook-Workflows erforderlichen Mindestberechtigungen umfasst.

     Als Rollenname können Sie den vorgeschlagenen Standardnamen akzeptieren oder einen Namen Ihrer Wahl eingeben. Wir empfehlen, den vorgeschlagenen Namen zu verwenden oder den Namen des Runbooks im Namen beizubehalten. Das liegt daran, dass das neue Runbook

mit dem von Ihnen ausgewählten Runbook verknüpft AssumeRole ist und möglicherweise nicht die für andere Runbooks erforderlichen Berechtigungen enthält.

- Vorhandene Servicerolle verwenden — Eine IAM-Rolle, die Sie oder Incident Manager zuvor erstellt haben, gewährt die erforderlichen Berechtigungen.

  Wählen Sie unter Rollenname den Namen der vorhandenen Rolle aus, die Sie verwenden möchten.

5. Erweitern Sie Zusätzliche Optionen und wählen Sie eine der folgenden Optionen aus, um anzugebenAWS-Konto, wo der Runbook-Workflow ausgeführt werden soll.

   - Konto des Eigentümers des Reaktionsplans — Startet den Runbook-Workflow in demAWS-Konto, der ihn erstellt hat.
   - Betroffenes Konto — Startet den Runbook-Workflow in dem Konto, das den Vorfall ausgelöst oder gemeldet hat.

     Wählen Sie Betroffenes Konto, wenn Sie Incident Manager für kontenübergreifende Szenarien verwenden und das Runbook auf Ressourcen im betroffenen Konto zugreifen muss, um diese zu beheben.

6. Fahren Sie fort, indem Sie optional einen PagerDuty Service in den Reaktionsplan integrieren.

(Optional) Integrieren eines PagerDuty Dienstes in den Reaktionsplan

Um einen PagerDuty Service in den Reaktionsplan zu integrieren

Wenn Sie Incident Manager mit integrieren PagerDuty, PagerDuty erstellt jedes Mal, wenn Incident Manager einen Incident erstellt, einen entsprechenden Incident. Der Incident PagerDuty verwendet den Paging-Workflow und die Eskalationsrichtlinien, die Sie dort zusätzlich zu denen in Incident Manager definiert haben. PagerDuty fügt Timeline-Ereignisse aus Incident Manager als Notizen zu Ihrem Vorfall hinzu.

1. Erweitern Sie Integrationen von Drittanbietern und aktivieren Sie dann das Kontrollkästchen PagerDuty Integration aktivieren.
2. Wählen Sie unter Geheim auswählen das Geheimnis aus, in AWS Secrets Manager dem Sie die Anmeldeinformationen für den Zugriff auf Ihr PagerDuty Konto speichern.

Hinweise zum Speichern Ihrer PagerDuty Anmeldeinformationen in einem Secrets Manager Secret finden Sie unterSpeichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret.

3. Wählen Sie unter PagerDuty Service den Service aus Ihrem PagerDuty Konto aus, für den Sie den PagerDuty Incident erstellen möchten.
4. Fahren Sie fort, indem Sie optionale Tags hinzufügen und den Reaktionsplan erstellen.

Hinzufügen von Tags und Erstellen des Reaktionsplans

Um Tags hinzuzufügen und den Reaktionsplan zu erstellen

1. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere Tag-Schlüsselname/Wert-Paare auf den Reaktionsplan an.

   Tags sind optionale Metadaten, die Sie einer Ressource zuweisen. Mithilfe von Stichwörtern können Sie eine Ressource auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Möglicherweise möchten Sie einen Reaktionsplan taggen, um die Art des Vorfalls, den er eindämmen soll, die Arten von Eskalationskanälen, die er enthält, oder den Eskalationsplan, der damit verknüpft wird, zu identifizieren. Weitere Informationen zur Kennzeichnung von Incident Manager-Ressourcen finden Sie unter. Taggen von Ressourcen in Incident Manager
2. Wählen Sie Reaktionsplan erstellen aus.

Arbeiten mit Ergebnissen in Incident Manager

In Incident Manager handelt es sich bei einem Befund um Informationen über AWS CodeDeploy Bereitstellungen oder AWS CloudFormation Stack-Updates, die etwa zum Zeitpunkt eines Vorfalls aufgetreten sind und an denen eine oder mehrere Ressourcen beteiligt waren, die wahrscheinlich mit dem Vorfall in Zusammenhang stehen. Jeder Befund kann als mögliche Ursache für den Vorfall untersucht werden. Informationen zu diesen möglichen Ursachen werden der Seite mit den Vorfalldetails für einen Vorfall hinzugefügt. Da Informationen zu diesen Implementierungen und Änderungen sofort zur Hand sind, müssen die Einsatzkräfte nicht manuell nach diesen Informationen suchen. Dadurch wird der Zeitaufwand für die Bewertung potenzieller Ursachen reduziert, wodurch sich die mittlere Wiederherstellungszeit (MTTR) nach einem Vorfall verringern kann.

Derzeit unterstützt Incident Manager das Sammeln von Erkenntnissen aus zwei AWS-Services Bereichen: und. AWS CodeDeployAWS CloudFormation

Findings ist eine optionale Funktion. Sie können sie im Assistenten Get Prepared aktivieren, wenn Sie zum ersten Mal in Incident Manager einsteigen, oder später auf der Seite Einstellungen.

Wenn Sie die Funktion „Ergebnisse“ aktivieren, erstellt Incident Manager eine Servicerolle für Sie. Diese Servicerolle umfasst die Berechtigungen, die zum Abrufen von Ergebnissen aus CodeDeploy und erforderlich sind CloudFormation.

Um mit Ergebnissen in einem kontenübergreifenden Szenario zu arbeiten, aktivieren Sie die Funktion im Verwaltungskonto. Danach muss jedes Anwendungskonto in einer AWS Resource Access Manager (AWS RAM) -Organisation eine entsprechende Servicerolle erstellen.

Weitere Informationen zur Verwendung der Funktion „Ergebnisse“ finden Sie in den folgenden Themen.

Themen

- Aktivieren und erstellen Sie eine Servicerolle für Ergebnisse
- Konfigurieren Sie Berechtigungen für die kontoübergreifende Unterstützung von Ergebnissen

Aktivieren und erstellen Sie eine Servicerolle für Ergebnisse

Wenn Sie die Funktion „Ergebnisse“ aktivieren, erstellt Incident Manager eine Servicerolle, die in `IncidentManagerIncidentAccessServiceRole` Ihrem Namen benannt wird. Diese Servicerolle bietet die Berechtigungen, die Incident Manager benötigt, um Informationen über CodeDeploy Bereitstellungen und CloudFormation Stack-Updates zu sammeln, die ungefähr zu dem Zeitpunkt aufgetreten sind, zu dem ein Incident erstellt wurde.

> **Note**
>
> Wenn Sie Incident Manager mit einer Organisation verwenden, wird die Servicerolle im Verwaltungskonto erstellt. Um mit Ergebnissen aus anderen Konten in der Organisation arbeiten zu können, muss die Servicerolle in jedem Anwendungskonto erstellt werden. Informationen zur Verwendung einer CloudFormation Vorlage zum Erstellen dieser Rolle in Ihren Anwendungskonten finden Sie in Schritt 4 unterRichten Sie das kontenübergreifende Incident-Management ein und konfigurieren Sie es.

Diese Servicerolle ist mit einer AWS verwalteten Richtlinie verknüpft. Informationen zu den Berechtigungen in dieser Richtlinie finden Sie unterAWS verwaltete Richtlinie: AWSIncidentManagerIncidentAccessServiceRolePolicy.

Informationen zur Aktivierung von Ergebnissen während des Onboarding-Prozesses für Incident Manager finden Sie unterErste Schritte mit Incident Manager.

Informationen zur Aktivierung von Ergebnissen nach Abschluss des Onboarding-Prozesses finden Sie unter. Verwaltung der Funktion „Ergebnisse“

Konfigurieren Sie Berechtigungen für die kontoübergreifende Unterstützung von Ergebnissen

Um die Funktion „Ergebnisse“ kontenübergreifend verwenden zu könnenAWS RAM, in denen eine Organisation eingerichtet ist, muss jedes Anwendungskonto die Berechtigungen konfigurieren, damit Incident Manager in seinem Namen die Servicerolle des Verwaltungskontos übernimmt.

Diese Berechtigungen können in einem Anwendungskonto konfiguriert werden, indem eine AWS CloudFormation Vorlage bereitgestellt wird, die von bereitgestellt wirdAWS, wodurch die Rolle erstellt wird`IncidentManagerIncidentAccessServiceRole`.

Informationen zum Herunterladen und Bereitstellen dieser Vorlage in einem Anwendungskonto finden Sie in Schritt 4 unterRegions- und kontenübergreifendes Incident-Management im Incident Manager.

Vorfälle im Incident Manager erstellen

Incident Manager, eine Funktion vonAWS Systems Manager, hilft Ihnen, Vorfälle zu verwalten und schnell darauf zu reagieren. Sie können Amazon CloudWatch und Amazon so konfigurieren EventBridge , dass auf der Grundlage von CloudWatch Alarmen und EventBridge Ereignissen automatisch Vorfälle erstellt werden. Sie können Incidents auch manuell auf der Incident-Listenseite oder mithilfe der StartIncidentAPI-Aktion aus demAWS CLI oder demAWS SDK erstellen. Incident Manager dedupliziert Vorfälle, die aufgrund desselben CloudWatch Alarms oder EventBridge Ereignisses entstanden sind, in denselben Vorfall.

Bei Vorfällen, die automatisch durch CloudWatch Alarme oder EventBridge Ereignisse ausgelöst werden, versucht Incident Manager, einen Vorfall zu erstellen, der der Ereignisregel oder dem Alarm entsprichtAWS-Region. Falls Incident Manager in der nicht verfügbar istAWS-Region, CloudWatch oder erstellen Sie den Incident EventBridge automatisch in einer der verfügbaren Regionen, die in Ihrem Replikationssatz angegeben sind. Weitere Informationen finden Sie unter Regions- und kontenübergreifendes Incident-Management im Incident Manager.

Wenn das System einen Incident erstellt, sammelt Incident Manager automatisch Informationen über die an dem Vorfall beteiligtenAWS Ressourcen und fügt diese Informationen der Registerkarte Verwandte Elemente hinzu. Wenn Sie in Ihrem Reaktionsplan ein Runbook angegeben haben, kann Incident Manager, wenn das System einen Incident erstellt, die Informationen über die an dem Vorfall beteiligtenAWS Ressourcen an das Runbook senden. Das System kann diese Ressourcen dann gezielt einsetzen, wenn es das Runbook initiiert und versucht, das Problem zu beheben.

Wenn das System einen Vorfall erstellt, erstellt es auch ein übergeordnetes operativesOpsItem Workitem () OpsCenter, einer Komponente von Systems Manager, und verknüpft es als zugehöriges Element mit dem Vorfall. Sie können dies verwenden OpsItem , um verwandte Arbeiten und future Vorfallanalysen zu verfolgen. Anrufe, um OpsCenter Kosten zu verursachen. Weitere Informationen zur OpsCenter Preisgestaltung finden Sie unter Systems Manager Manager-Preise.

Important

Beachten Sie die folgenden wichtigen Details.

- Falls Incident Manager nicht verfügbar ist, kann das System nur dann einen Failover durchführen und Incidents in anderen erstellen,AWS-Regionen wenn Sie in Ihrem Replikationssatz mindestens zwei Regionen angegeben haben. Hinweise zur Konfiguration eines Replikationssatzes finden Sie unterErste Schritte mit Incident Manager.

- Incidents, die durch einen regionsübergreifenden Failover verursacht wurden, rufen keine in den Reaktionsplänen angegebenen Runbooks auf.

Automatisches Erstellen von Vorfällen mit CloudWatch Alarmen

CloudWatch verwendet Ihre CloudWatch Metriken, um Sie über Änderungen in Ihrer Umgebung zu informieren und automatisch die Aktion „Incident starten“ durchzuführen. CloudWatch arbeitet mit Systems Manager und Incident Manager zusammen, um anhand einer Vorlage für einen Reaktionsplan einen Vorfall zu erstellen, wenn ein Alarm in den Alarmzustand übergeht. Dies erfordert die folgenden Voraussetzungen:

- Incident Manager konfiguriert und Replikationssatz erstellt. In diesem Schritt wird die mit dem Service verknüpfte Incident Manager-Rolle in Ihrem Konto erstellt und die erforderlichen Berechtigungen bereitgestellt.
- Ein konfigurierter Incident-Manager-Reaktionsplan. Informationen zur Konfiguration von Incident Manager-Reaktionsplänen finden SieArbeiten mit Reaktionsplänen in Incident Manager im Abschnitt zur Vorbereitung von Vorfällen in diesem Handbuch.
- Konfigurierte CloudWatch Metriken zur Überwachung Ihrer Anwendung. Bewährte Methoden zur Überwachung finden SieÜberwachen im Abschnitt zur Vorbereitung von Vorfällen in diesem Leitfaden.

So erstellen Sie einen Alarm mit der Aktion „Vorfall starten“

1. Erstellen Sie einen Alarm in CloudWatch. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.
2. Wählen Sie bei der Auswahl der Aktion, die der Alarm ausführen soll, die Option Systemmanager-Aktion hinzufügen aus.
3. Wählen Sie Incident erstellen und wählen Sie den Reaktionsplan für diesen Incident aus.
4. Führen Sie die verbleibenden Schritte in der Anleitung für Ihren ausgewählten Alarmtyp aus.

> **Tip**
>
> Sie können die Aktion „Vorfall erstellen“ auch zu jedem vorhandenen Alarm hinzufügen.

Automatisches Erstellen von Vorfällen mit EventBridge Ereignissen

EventBridge Regeln achten auf Ereignismuster. Wenn das Ereignis dem definierten Muster entspricht, erstellt Incident Manager mithilfe des ausgewählten Reaktionsplans einen Incident.

Ereignisse mithilfe von SaaS-Partnerereignissen erstellen

Sie können so konfigurieren EventBridge , dass Ereignisse von Software-as-a-Service (SaaS) -Partneranwendungen und -diensten empfangen werden, was die Integration von Drittanbietern ermöglicht. Nach der Konfiguration EventBridge für den Empfang von Ereignissen von Drittanbietern können Sie Regeln erstellen, die auf Partnerereignisse abgestimmt sind, um Vorfälle zu erstellen. Eine Liste der Integrationen von Drittanbietern finden Sie unter Empfangen von Ereignissen von einem SaaS-Partner.

Konfigurieren Sie EventBridge den Empfang von Ereignissen aus einer SaaS-Integration.

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Partner event sources (Partnerereignisquellen) aus.
3. Verwenden Sie die Suchleiste, um den gewünschten Partner zu finden, und wählen Sie Für diesen Partner einrichten aus.
4. Wählen Sie Copy (Kopieren) aus, um Ihre Konto-ID in die Zwischenablage zu kopieren.

   > **Note**
   >
   > Verwenden Sie zur Integration mit Salesforce die im AppFlow Amazon-Benutzerhandbuch beschriebenen Schritte.

5. Rufen Sie die Website des Partners auf und befolgen Sie die Anweisungen zum Erstellen einer Partnerereignisquelle. Verwenden Sie hierzu Ihre -Konto-ID. Die von Ihnen erstellte Ereignisquelle ist nur in Ihrem Konto verfügbar.
6. Gehen Sie zurück zur EventBridge Konsole und wählen Sie im Navigationsbereich Partnerereignisquellen aus.
7. Wählen Sie die Schaltfläche neben der Partnerereignisquelle aus und klicken Sie auf Associate with event bus (Mit Ereignisbus verknüpfen) aus.

Erstellen Sie eine Regel, die bei Vorpaketen eines SaaS-Partners ausgelöst wird

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Create rule (Regel erstellen).
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Wählen Sie für Eventbus den Eventbus aus, der diesem Partner entspricht.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Next (Weiter).
8. Wählen Sie als EreignisquelleAWS Ereignisse oder EventBridge Partnerveranstaltungen aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular aus.
10. Wählen Sie als EventquelleEventBridge Partner
11. Wählen Sie für Partner den Namen des Partners aus.
12. Wählen Sie in Event type (Ereignistyp) die Option All Events (Alle Ereignisse) oder den Ereignistyp aus, der für diese Regel verwendet werden soll. Wenn Sie All Events (Alle Ereignisse) auswählen, stimmen alle Ereignisse, die von dieser Partnerereignisquelle ausgegeben werden, mit der Regel überein.

    Wenn Sie das Ereignismuster anpassen möchten, wählen Sie Sie, wählen Sie Ihre Änderungen vor und wählen Sie Speichern.
13. Wählen Sie Next (Weiter).
14. Wählen Sie unter Ziel auswählen die Option Incident Manager-Reaktionsplan und dann einen Reaktionsplan aus.

    > **Note**
    >
    > Wenn Sie einen Reaktionsplan auswählen, werden alle Reaktionspläne, die Sie besitzen und die mit Ihrem Konto geteilt wurden, in der Dropdown-Liste Antwortplan angezeigt.
15. EventBridge kann die IAM-Rolle erstellen, die zum Ausführen Ihrer Regel erforderlich ist:

- Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Create a new role for this specific resource (Eine neue Rolle für diese spezifische Ressource erstellen).
- Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden).

16. Wählen Sie Next (Weiter).
17. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridgeAmazon-Tags im EventBridge Amazon-Benutzerhandbuch.
18. Wählen Sie Next (Weiter).
19. Überprüfe deine Regel und wähle dann Regel erstellen.

Vorfälle mithilfe vonAWS Serviceereignissen erstellen

EventBridge empfängt auch Ereignisse von denAWS Diensten, die unter Ereignisse von unterstütztenAWS Diensten aufgeführt sind. Ähnlich wie Sie Regeln für SaaS-Partner konfigurieren, können Sie sie fürAWS Dienste konfigurieren.

Erstellen Sie eine Regel, die bei Vorpaketen einesAWS Dienstes ausgelöst wird

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Create rule (Regel erstellen).
4. Geben Sie einen Namen und eine Beschreibung für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Next (Weiter).
8. Wählen Sie als EreignisquelleAWS Ereignisse oder EventBridge Partnerveranstaltungen aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular aus.
10. Als Event source (Ereignisquelle) wählen Sie AWS-Services aus.
11. Wählen Sie als Dienstname den Dienst aus, der einen Vorfall überwacht.

12. Wählen Sie in Event type (Ereignistyp) die Option All Events (Alle Ereignisse) oder den Ereignistyp aus, der für diese Regel verwendet werden soll. Wenn Sie All Events (Alle Ereignisse) auswählen, stimmen alle Ereignisse, die von dieser Partnerereignisquelle ausgegeben werden, mit der Regel überein.

    Wenn Sie das Ereignismuster anpassen möchten, wählen Sie Sie, wählen Sie Ihre Änderungen vor und wählen Sie Speichern.
13. Wählen Sie Next (Weiter).
14. Wählen Sie unter Ziel auswählen die Option Incident Manager-Reaktionsplan und dann einen Reaktionsplan aus.

    > **Note**
    >
    > Wenn Sie einen Reaktionsplan auswählen, werden alle Reaktionspläne, die Sie besitzen und die mit Ihrem Konto geteilt wurden, in der Dropdown-Liste Antwortplan angezeigt.
15. EventBridge kann die IAM-Rolle erstellen, die zum Ausführen Ihrer Regel erforderlich ist:

    - Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Create a new role for this specific resource (Eine neue Rolle für diese spezifische Ressource erstellen).
    - Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden).
16. Wählen Sie Next (Weiter).
17. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein. Weitere Informationen finden Sie unter EventBridgeAmazon-Tags im EventBridge Amazon-Benutzerhandbuch.
18. Wählen Sie Next (Weiter).
19. Überprüfe deine Regel und wähle dann Regel erstellen.

Erstellen von Vorpakpaketen

Einsatzkräfte können einen Vorfall mithilfe der Incident Manager-Konsole manuell verfolgen, indem sie einen vordefinierten Reaktionsplan verwenden. Führen Sie die folgenden Schritte aus, um einen Vorfall zu erstellen.

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie Incident starten aus.

3. Wählen Sie unter Reaktionsplan einen Reaktionsplan aus der Liste aus.
4. (Optional) Um den Titel des definierten Reaktionsplans zu überschreiben, geben Sie einen Incident-Titel ein.
5. (Optional) Um die Auswirkungen des definierten Reaktionsplans zu überschreiben, geben Sie die Auswirkung des Vorfalls ein.

Nachverfolgung von Vorfällen im Incident Manager

AWSSystems Manager Incident Manager verfolgt Ihre Vorfälle vom Moment ihrer Entdeckung über die Behebung bis hin zur Analyse nach dem Vorfall. Sie finden alle Vorfälle auf der Seite mit der Liste der Vorfälle in der Incident Manager-Konsole. Dort finden Sie Links direkt zu den Incident-Details.

Themen

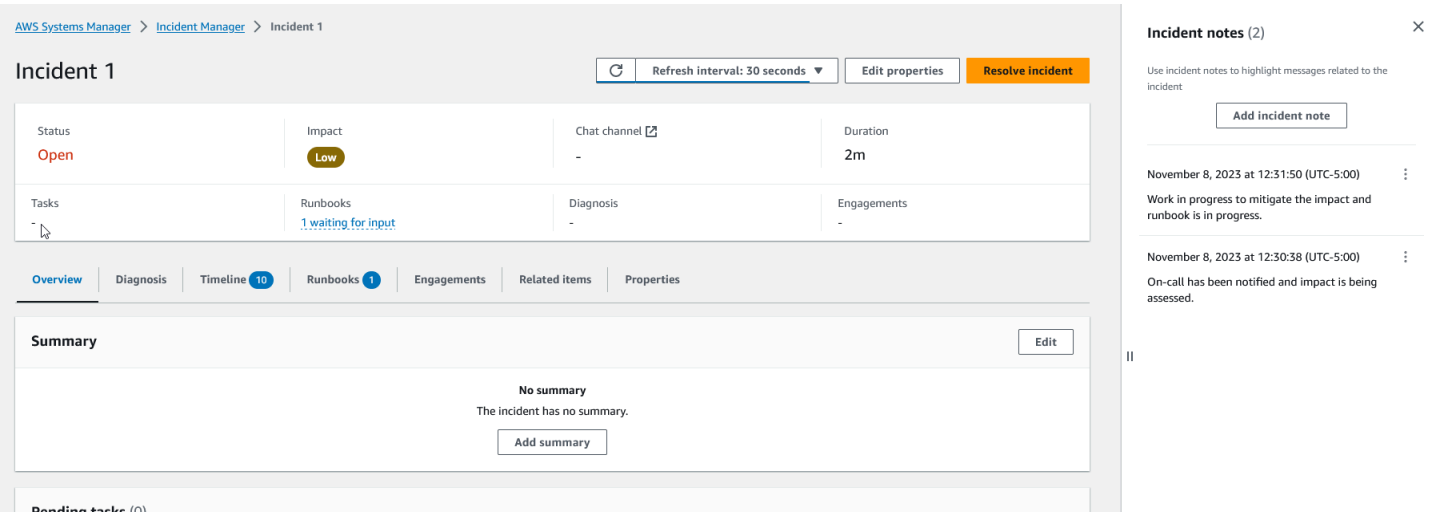
Liste der Vorfälle

Die Seite mit der Liste der Vorfälle besteht aus drei Abschnitten: Offene Vorfälle, Behobene Vorfälle und Analysen. Auf dieser Seite können Sie neue Vorfälle manuell verfolgen und Analysen erstellen. Weitere Informationen zur manuellen Nachverfolgung eines Vorfalls finden Sie Erstellen von Vorpakpaketen im Abschnitt zur Erstellung von Vorfällen in diesem Leitfaden. Weitere Informationen zur Analyse nach einem Vorfall finden Sie im Durchführung einer Analyse nach einem Vorfall im Incident-Manager Abschnitt dieses Handbuchs.

In den Vorfalldetails werden offene Vorfälle in Kacheln mit dem Titel, der Auswirkung, der Dauer und dem Chat-Kanal für den Vorfall angezeigt. Nachdem Sie einen Vorfall gelöst haben, wird er in die Liste Gelöste Vorfälle verschoben. Analysen befinden sich auf der zweiten Registerkarte.

Einzelheiten zum Vorfall

Die Seite mit den Vorfalldetails bietet detaillierte Einblicke und Tools, mit denen Sie einen Vorfall verwalten können. Auf dieser Seite können Sie Runbooks starten, um einen Vorfall einzudämmen, Hinweise zu Vorfällen hinzuzufügen, andere Problemlöser hinzuzuziehen und Vorfalldetails wie Zeitpläne, Kennzahlen, Eigenschaften und zugehörige Ressourcen einzusehen. Die Seite mit den Incident-Details umfasst die folgenden Abschnitte: Top-Banner, Incident-Notizen und sieben Tabs mit zusätzlichen Informationen und Ressourcen. Standardmäßig werden die Abschnitte „Top-Banner“ und „Hinweise zum Vorfall“ auf der Seite mit allen Incident-Details angezeigt.



In diesem Thema werden Elemente der Seite mit den Incident-Details und Aktionen erklärt, die Sie von der Seite aus ausführen können.

Oberes Banner

Das obere Banner auf jeder Seite mit den Vorfalldetails enthält die folgenden Informationen:

- Status — Der aktuelle Status eines Vorfalls kann „Offen“ oder „Gelöst“ lauten.
- Auswirkung — Die Auswirkungen des Vorfalls auf Ihre Umgebung. Sie kann hoch, mittel und niedrig sein. Um die Auswirkungen eines Vorfalls zu ändern, wählen Sie Eigenschaften bearbeiten.
- Chat-Kanal — Ein Link, über den Sie auf den Chat-Kanal zugreifen können, über den Sie Updates und Benachrichtigungen zu Vorfällen einsehen können.
- Dauer — Die Zeit, die verstrichen ist, bis ein Responder den Vorfall behoben hat.
- Runbooks — Der Status der Runbooks, die mit diesem Vorfall verknüpft sind. Der Status kann „Wartet auf Eingabe“, „Erfolgreich“ oder „Nicht erfolgreich“ lauten. Wenn der Status eines Runbooks auf Eingabe wartet, können Sie das Runbook auswählen, um die Aktionsdetails anzuzeigen. Sie können „Nicht erfolgreich“ auswählen, um Runbooks mit Timeout, Fehlgeschlagen oder Storniert anzuzeigen.
- Interaktionen — Die Gesamtzahl der Interaktionen und der Status jedes Engagements. Wenn Sie ein Engagement erstellen, lautet sein Status Engagiert. Sobald Sie das Engagement bestätigt haben, ändert sich der Status von Engagiert zu Bestätigt. Incident Manager unterstützt keine Bestätigung von Interaktionen durch Dritte. Solche Engagements behalten den Status Engagiert.

Sie können den Titel, die Auswirkung und den Chat-Kanal des Vorfalls bearbeiten, indem Sie in der oberen rechten Ecke des Banners „Bearbeiten“ wählen.

Hinweise zum Vorfall

Auf der rechten Seite des Bildschirms wird der Abschnitt „Hinweise zu Vorfällen“ angezeigt. Mithilfe von Notizen können Sie mit anderen Benutzern, die an einem Vorfall arbeiten, zusammenarbeiten und mit ihnen kommunizieren. Sie können die von Ihnen ergriffenen Abhilfemaßnahmen, eine mögliche Ursache, die Sie identifiziert haben, oder den aktuellen Status des Vorfalls erläutern. Es hat sich bewährt, den Abschnitt „Hinweise zu Vorfällen“ zu verwenden, um Statusaktualisierungen und Maßnahmen zu veröffentlichen, die Sie oder andere aufgrund eines Vorfalls ergreifen. Wenn Sie in Echtzeit mit anderen Resolvern kommunizieren möchten, verwenden Sie den Chat-Kanal, der in Incident Manager verfügbar ist.

Um eine Notiz hinzuzufügen, wählen Sie die Schaltfläche Vorfallnotiz hinzufügen und geben Sie dann Ihre Notiz ein. Notizen können Aktualisierungen zum Status des Vorfalls oder andere relevante Informationen enthalten, die für andere Benutzer sichtbar sind. Bei Bedarf können Sie auch Notizen zu Vorfällen bearbeiten oder löschen.

> **Note**
>
> Jeder Benutzer mit IAM-Berechtigungen zur Ausführung der `ssm-incidents:UpdateTimelineEvent` `ssm-incidents:DeleteTimelineEvent` AND-Aktionen kann Notizen bearbeiten und löschen. Wenn Sie jedoch einen Vorfall mit einem anderen Konto teilen, ist die `ssm-incidents:DeleteTimelineEvent` Aktion in der Ressourcenrichtlinie nicht enthalten. Dadurch wird verhindert, dass der Benutzer, mit dem Sie den Vorfall teilen, die Notiz löscht. Sie können den Prüfpfad für eine Notiz aus Incident Manager-Ereignissen in der AWS CloudTrail Konsole einsehen.

Registerkarten

Die Seite mit den Vorfalldetails umfasst sieben Registerkarten, sodass die Einsatzkräfte während eines Vorfalls Informationen leichter finden und einsehen können. Auf den Registerkarten wird im Namen der Registerkarte ein Zähler angezeigt, der die Anzahl der Aktualisierungen für die Registerkarte angibt. Weitere Informationen zum Inhalt der einzelnen Tabs sowie zu den verfügbaren Aktionen finden Sie in diesem Artikel.

Übersicht

Die Registerkarte „Übersicht“ ist die Landingpage für Responder. Sie enthält die Zusammenfassung des Vorfalls, eine Liste der jüngsten Ereignisse auf der Zeitleiste und den aktuellen Runbook-Schritt.

Mithilfe der Zusammenfassung können sich die Einsatzkräfte darüber catch, welche Maßnahmen ergriffen wurden, welche Änderungen sich ergeben haben, welche nächsten Schritte möglich sind und welche Auswirkungen der Vorfall hatte. Um die Zusammenfassung zu aktualisieren, wählen Sie in der oberen rechten Ecke des Abschnitts Zusammenfassung die Option Bearbeiten aus.

> **Important**
>
> Wenn mehrere Antwortende das Zusammenfassungsfeld gleichzeitig bearbeiten, überschreibt der Responder, der ihre Änderungen zuletzt eingereicht hat, alle anderen Eingaben.

Der Abschnitt Aktuelle Ereignisse in der Zeitleiste enthält eine von Incident Manager aufgefüllte Zeitleiste mit den fünf neuesten Ereignissen. Verwenden Sie diesen Abschnitt, um den Status des Vorfalls und die jüngsten Ereignisse zu verstehen. Um eine vollständige Zeitleiste einzusehen, fahren Sie mit der Registerkarte Zeitleiste fort.

Auf der Übersichtsseite wird auch der Schritt Current Runbook angezeigt. Dieser Schritt kann ein automatischer Schritt sein, der in Ihrer AWS Umgebung ausgeführt wird, oder es kann sich um eine Reihe manueller Anweisungen für Responder handeln. Um das vollständige Runbook, einschließlich früherer und bevorstehender Schritte, anzuzeigen, wählen Sie die Registerkarte Runbook.

Diagnose

Die Registerkarte Diagnose enthält wichtige Informationen zu Ihren AWS gehosteten Anwendungen und Systemen, einschließlich Informationen zu Kennzahlen und, falls aktiviert, Ergebnissen.

Mit Metriken arbeiten

Incident Manager verwendet Amazon CloudWatch , um die Metriken und Alarmdiagramme auf dieser Registerkarte zu füllen. Weitere Informationen zu den bewährten Methoden des Incident-Managements zur Definition von Alarmen und Kennzahlen finden Sie Überwachen im Abschnitt Planung von Vorfällen in diesem Benutzerhandbuch.

Um Metriken hinzuzufügen

- Wählen Sie in der oberen rechten Ecke dieses Tabs Hinzufügen aus.
  - Um eine Metrik aus einem vorhandenen CloudWatch Dashboard hinzuzufügen, wählen Sie Aus vorhandenem CloudWatch Dashboard.

    a. Wählen Sie ein Dashboard aus. Dadurch werden alle Metriken und Alarme hinzugefügt, die Teil des ausgewählten Dashboards sind.

    b. (Optional) Sie können auch Metriken aus dem Dashboard auswählen, um bestimmte Metriken anzuzeigen.
  - Fügen Sie eine einzelne Metrik hinzu, indem Sie Von auswählen CloudWatch und eine Metrikquelle einfügen. So kopieren Sie eine Metrikquelle:

    a. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.

    b. Wählen Sie im Navigationsbereich Metriken aus.

    c. Geben Sie auf der Registerkarte Alle Metriken einen Suchbegriff in das Suchfeld ein, z. B. einen Metriknamen oder einen Ressourcennamen, und wählen Sie Enter.

    Wenn Sie beispielsweise nach der `CPUUtilization` Metrik suchen, werden Ihnen die Namespaces und Dimensionen angezeigt, die dieser Metrik zugeordnet sind.

    d. Wählen Sie eines der Ergebnisse aus Ihrer Suche aus, um die Metriken anzuzeigen.

    e. Wählen Sie den Tab Quelle und kopieren Sie die Quelle.

Metrische Alarmdiagramme können den Incident-Details nur über den entsprechenden Reaktionsplan hinzugefügt werden oder indem beim Hinzufügen einer Metrik die Option Aus vorhandenem CloudWatch Dashboard ausgewählt wird.

Um Metriken zu entfernen, wählen Sie Entfernen und dann die Metriken, die Sie entfernen möchten, aus der bereitgestellten Metrik-Dropdown-Liste aus.

Ergebnisse von AWS CodeDeploy und anzeigen AWS CloudFormation

Nachdem Findings aktiviert und alle erforderlichen Berechtigungen konfiguriert wurden, werden alle Ergebnisse, die sich auf einen bestimmten Vorfall beziehen könnten, dem Vorfall zugeordnet. Responder können Informationen zu diesen Ergebnissen auf der Seite mit den Incident-Details einsehen.

Um Ergebnisse von und einzusehen CodeDeploy CloudFormation

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie den Namen eines zu untersuchenden Vorfalls.
3. Vergleichen Sie auf der Registerkarte Diagnose im Bereich Ergebnisse die Startzeiten aller gemeldeten Ergebnisse mit der Startzeit des Vorfalls.
4. Um weitere Details zu einem Befund anzuzeigen, wählen Sie in der Spalte Referenz den Link zum CloudFormation Befund CodeDeploy oder aus.

Zeitplan

Verwenden Sie die Registerkarte Zeitleiste, um Ereignisse zu verfolgen, die während eines Vorfalls auftreten. Incident Manager füllt automatisch Ereignisse in der Zeitleiste aus, anhand derer signifikante Ereignisse während des Vorfalls identifiziert werden. Responder können benutzerdefinierte Ereignisse hinzufügen, die auf Ereignissen basieren, die manuell erkannt werden. Während der Analyse nach dem Vorfall bietet der Tab „Zeitleiste“ wertvolle Erkenntnisse darüber, wie Sie sich in future besser auf Vorfälle vorbereiten und darauf reagieren können. Weitere Informationen zur Analyse nach einem Vorfall finden Sie unter. Durchführung einer Analyse nach einem Vorfall im Incident-Manager

Um ein benutzerdefiniertes Timeline-Ereignis hinzuzufügen, wählen Sie Hinzufügen. Wählen Sie mithilfe des Kalenders ein Datum aus und geben Sie dann eine Uhrzeit ein. Alle Zeiten werden in Ihrer lokalen Zeitzone angezeigt. Geben Sie eine kurze Beschreibung des Ereignisses ein, das in der Timeline angezeigt wird.

Um ein vorhandenes benutzerdefiniertes Ereignis zu bearbeiten, wählen Sie das Ereignis auf der Timeline aus und wählen Sie Bearbeiten. Sie können Uhrzeit, Datum und Beschreibung von benutzerdefinierten Ereignissen ändern. Sie können nur benutzerdefinierte Ereignisse bearbeiten.

Runbooks

Auf der Registerkarte Runbooks der Seite mit den Incident-Details können sich Einsatzkräfte die Runbook-Schritte ansehen und neue Runbooks starten.

Um ein neues Runbook zu starten, wählen Sie im Abschnitt Runbooks die Option Runbook starten aus. Verwenden Sie das Suchfeld, um das Runbook zu finden, das Sie starten möchten. Geben Sie alle erforderlichen Parameter und die Version des Runbooks an, die Sie beim Starten des Runbooks

verwenden möchten. Runbooks, die während eines Vorfalls über die Registerkarte Runbooks gestartet wurden, verwenden die Berechtigungen des aktuell angemeldeten Kontos.

Um zu einer Runbook-Definition in Systems Manager zu navigieren, wählen Sie unter Runbooks den Titel des Runbooks aus. Um zur laufenden Instanz des Runbooks in Systems Manager zu navigieren, wählen Sie die Ausführungsdetails unter Ausführungsdetails aus. Auf diesen Seiten werden die Vorlage angezeigt, die zum Starten des Runbooks verwendet wurde, sowie die spezifischen Details der aktuell ausgeführten Instanz des Automatisierungsdokuments.

Im Abschnitt Runbook-Schritte wird die Liste der Schritte angezeigt, die das ausgewählte Runbook automatisch ausführt oder die Responder manuell ausführen. Die Schritte werden erweitert, wenn sie zum aktuellen Schritt werden, und es werden Informationen angezeigt, die zum Abschließen des Schritts erforderlich sind, oder Details zu den Aufgaben des Schritts. Automatische Runbook-Schritte werden nach Abschluss der Automatisierung aufgelöst. Bei manuellen Schritten müssen die Responder am Ende jedes Schritts die Option Nächster Schritt auswählen. Nachdem ein Schritt abgeschlossen ist, wird die Schrittausgabe als Dropdownmenü angezeigt.

Um die Ausführung eines Runbooks abzubrechen, wählen Sie Runbook abbrechen. Dadurch wird die Ausführung des Runbooks gestoppt und es werden keine weiteren Schritte im Runbook abgeschlossen.

Engagements

Der Tab Engagements in den Incident-Details fördert das Engagement von Einsatzkräften und Teams. Auf dieser Registerkarte können Sie sehen, wer engagiert wurde, wer geantwortet hat und welche Einsatzkräfte im Rahmen eines Eskalationsplans hinzugezogen werden. Responder können andere Kontakte direkt von diesem Tab aus kontaktieren. Weitere Informationen zum Erstellen von Kontakten und Eskalationsplänen finden Sie in den Arbeiten mit Eskalationsplänen im Incident Manager Abschnitten Mit Kontakten im Incident Manager arbeiten und in diesem Leitfaden.

Sie können Reaktionspläne mit Kontakten und Eskalationsplänen so konfigurieren, dass der Kontakt zu Beginn eines Vorfalls automatisch gestartet wird. Weitere Informationen zur Konfiguration von Reaktionsplänen finden Sie im Arbeiten mit Reaktionsplänen in Incident Manager Abschnitt dieses Handbuchs.

Informationen zu den einzelnen Kontakten finden Sie in der Tabelle. Diese Tabelle enthält die folgenden Informationen:

- Name — Links zur Seite mit den Kontaktdaten, auf der die Kontaktmethoden und der Kontaktplan angezeigt werden.

- Eskalationsplan — Links zu dem Eskalationsplan, mit dem der Kontakt beauftragt wurde.
- Kontaktquelle — Identifiziert den Service, der diesen Kontakt kontaktiert hat, z. B. AWS Systems Manager oder. PagerDuty
- Engagiert — Zeigt an, wann der Plan einen Kontakt beauftragt hat oder wann ein Kontakt im Rahmen eines Eskalationsplans hinzugezogen werden sollte.
- Bestätigt — Zeigt an, ob der Kontakt den Kontakt bestätigt hat.

Um ein Engagement zu bestätigen, kann der Antwortende einen der folgenden Schritte ausführen:

- Telefonanruf — Geben Sie ein, **1** wenn Sie dazu aufgefordert werden.
- SMS — Beantworten Sie die Nachricht mit dem bereitgestellten Code oder geben Sie den bereitgestellten Code auf der Registerkarte Interaktionen des Vorfalls ein.
- E-Mail — Geben Sie den bereitgestellten Code auf der Registerkarte Engagements des Vorfalls ein.

Verwandte Elemente

Auf der Registerkarte „Verwandte Artikel“ werden Ressourcen gesammelt, die sich auf die Minderung von Vorfällen beziehen. Bei diesen Ressourcen kann es sich um ARNs, Links zu externen Ressourcen oder Dateien handeln, die in Amazon S3 S3-Buckets hochgeladen wurden. In der Tabelle werden ein beschreibender Titel und entweder ein ARN, ein Link oder Bucket-Details angezeigt. Bevor Sie S3-Buckets verwenden, lesen Sie die bewährten Sicherheitsmethoden für Amazon S3 im Amazon S3 S3-Benutzerhandbuch.

Beim Hochladen von Dateien in einen Amazon S3 S3-Bucket ist die Versionierung für diesen Bucket entweder aktiviert oder ausgesetzt. Wenn die Versionsverwaltung für den Bucket aktiviert ist, werden Dateien, die mit demselben Namen wie eine bestehende Datei hochgeladen wurden, als neue Version der Datei hinzugefügt. Wenn die Versionierung unterbrochen ist, überschreiben Dateien, die denselben Namen wie eine bestehende Datei haben, die vorhandene Datei. Weitere Informationen zur Versionierung finden Sie unter Verwenden der Versionierung in S3-Buckets im Amazon S3 S3-Benutzerhandbuch.

Wenn Sie ein dateibezogenes Element entfernen, wird die Datei aus dem Vorfall entfernt, aber nicht aus dem Amazon S3 S3-Bucket entfernt. Weitere Informationen zum Entfernen von Objekten aus einem Amazon S3 S3-Bucket finden Sie unter Löschen von Amazon S3 S3-Objekten im Amazon S3 S3-Benutzerhandbuch.

Eigenschaften

Die Registerkarte „Eigenschaften“ enthält die folgenden Informationen zu dem Vorfall.

Im Abschnitt mit den Incident-Eigenschaften können Sie Folgendes einsehen:

- Status — Beschreibt den aktuellen Status des Vorfalls. Der Vorfall kann „Offen“ oder „Gelöst“ sein.
- Startzeit — Die Uhrzeit, zu der der Incident Manager erstellt wurde.
- Behobene Zeit — Der Zeitpunkt, zu dem der Vorfall in Incident Manager behoben wurde.
- Amazon Resource Name (ARN) — Der ARN des Vorfalls. Verwenden Sie den ARN, wenn Sie im Chat oder mit den Befehlen AWS Command Line Interface (AWS CLI) auf den Vorfall verweisen.
- Reaktionsplan — Identifiziert den Reaktionsplan für den ausgewählten Vorfall. Wenn Sie den Reaktionsplan auswählen, wird die Detailseite des Reaktionsplans geöffnet.
- Übergeordnetes Element OpsItem — Identifiziert die OpsItem Person, die erstellt wurde, als übergeordnetes Element des Vorfalls. Ein Elternteil OpsItem kann mehrere zusammenhängende Vorfälle und Folgemaßnahmen haben. Wenn Sie das Elternteil auswählen, OpsItem wird die OpsItems Detailseite in geöffnet OpsCenter.
- Analyse — Identifiziert die Analyse, die aufgrund dieses Vorfalls erstellt wurde. Erstellen Sie anhand eines gelösten Vorfalls eine Analyse, um Ihren Prozess zur Reaktion auf Vorfälle zu verbessern. Wählen Sie die Analyse aus, um die Seite mit den Analysedetails zu öffnen.
- Besitzer — Das Konto, in dem der Vorfall erstellt wurde.

Im Abschnitt „Tags“ können Sie die Tag-Schlüssel und -Werte, die mit dem Incident-Datensatz verknüpft sind, einsehen und bearbeiten. Weitere Informationen zu Tags in Incident Manager finden Sie unterTaggen von Ressourcen in Incident Manager.

Durchführung einer Analyse nach einem Vorfall im Incident-Manager

Die Post-Incident-Analyse führt Sie durch die Identifizierung von Verbesserungen Ihrer Reaktion auf Vorfälle und führt Sie durch die Identifizierung von Verbesserungen Ihrer Reaktion auf Vorfälle. Eine Analyse kann Ihnen auch helfen, die Grundursache der Vorfälle zu verstehen. Incident Manager erstellt Handlungsempfehlungen, um Ihre Reaktion auf Vorfälle zu verbessern.

Vorteile einer Analyse nach einem Vorfall

- Verbesserung der Reaktion auf Vorfälle
- Verstehen Sie die Grundursache des Problems
- Behandeln Sie die Grundursachen mit umsetzbaren Maßnahmen
- Analysieren Sie die Auswirkungen von Vorfällen
- Erfassen und teilen Sie Erkenntnisse innerhalb einer Organisation

Wofür Sie eine Analyse nicht verwenden sollten

Eine Analyse ist tadellos und nennt die Leute nicht beim Namen.

„Unabhängig davon, was wir herausfinden, verstehen wir und sind fest davon überzeugt, dass jeder die bestmögliche Arbeit geleistet hat, wenn man bedenkt, was er zu diesem Zeitpunkt wusste, seine Fähigkeiten und Fertigkeiten, die verfügbaren Ressourcen und die aktuelle Situation.“ - Norm Kerth, Projektrückblicke: Ein Handbuch zur Teamüberprüfung

Details zur Analyse

Die Seite mit den Analysedetails führt Sie durch das Sammeln von Informationen, die Bewertung von Verbesserungen und die Erstellung von Aktionspunkten. Die Seite mit den Analysedetails ähnelt den Vorfalldetails, weist jedoch einige wichtige Unterschiede auf, z. B. historische Kennzahlen, einen editierbaren Zeitplan und Fragen zur Verbesserung future Vorfälle.

Übersicht

Die Übersicht ist eine Zusammenfassung des Vorfalls. Diese Zusammenfassung enthält Hintergrundinformationen, was passiert ist, warum es passiert ist, wie es gemildert wurde, wie es dauert und wichtige Maßnahmen, um zu verhindern, dass sich der Vorfall erneut ereignet. Die

Übersicht ist auf hohem Niveau. Weitere Informationen finden Sie auf der Registerkarte „Fragen“ der Analyse.

Metriken

Verwenden Sie die Registerkarte „Metriken“, um wichtige Kennzahlen in Ihrer Anwendung über die Dauer des Vorfalls zu visualisieren. Sie können hier metrische Grafiken hinzufügen, bei denen eine oder mehrere Metriken in derselben Grafik dargestellt sind. Metriken, die während eines Vorfalls verwendet wurden, werden auf dieser Registerkarte automatisch eingetragen. Wir empfehlen Ihnen, eine Beschreibung, einen Titel und Anmerkungen zu wichtigen Zeitpunkten während des Vorfalls hinzuzufügen.

Einige wichtige Zeitpunkte, die Sie bei der Analyse eines metrischen Diagramms berücksichtigen können:

- Änderung des Einsatzes
- Konfigurationsänderung
- Startzeit des Ereignisses
- Uhrzeit des Weckers
- Zeitpunkt des Engagements
- Startzeit des Ereignisses
- Zeit zur Behebung des Vorfalls

Einschränkungen

- CloudWatch Alarme und metrische Ausdrücke werden nicht aus einem Vorfall importiert.
- Metriken, die sich in einer Region befinden, die Incident Manager nicht unterstützt, werden nicht aus dem Incident importiert.
- Metriken in Anwendungskonten müssen`CloudWatch-CrossAccountSharingRole` vor der Erstellung der Analyse konfiguriert werden. Weitere Informationen zur Rolle finden Sie unter Account CloudWatch Cross-Region-Konsole im CloudWatch Benutzerhandbuch.

Zeitplan

Beschreiben Sie wichtige Zeitpunkte auf der Zeitleiste, während Sie sich eingehender mit dem Verständnis des Vorfalls befassen. Die Zeitleiste der Vorfälle wird automatisch auf dieser

Registerkarte aufgefüllt. Sie können Zeitpunkte löschen, die für die Analyse nicht relevant sind. Sie können auch Zeitpunkte hinzufügen und bearbeiten, um den Vorfall und seine Auswirkungen genauer zu beschreiben.

Verwenden Sie die Registerkarte „Zeitleiste“, um Fragen zu beantworten, die Sie auf der Registerkarte „Fragen“ zur Reaktion auf den Vorfall finden.

Fragen

Verwenden Sie Incident Manager-Fragen, um die Zeit bis zur Behebung von Vorfällen in Ihrer Anwendung zu verkürzen und das Auftreten von Vorfällen zu reduzieren. Aktualisieren Sie bei der Beantwortung von Fragen die Tabs „Metriken“ und „Zeitleiste“, um die Genauigkeit zu gewährleisten. Die Fragen konzentrieren sich auf diese Schlüsselaspekte der Reaktion auf Vorfälle:

- Erkennung — Könnten Sie die Zeit bis zur Erkennung verkürzen? Gibt es Aktualisierungen der Kennzahlen und Alarme, mit denen der Vorfall früher erkannt werden könnte?
- Diagnose — Können Sie die Zeit bis zur Diagnose verkürzen? Gibt es Aktualisierungen Ihrer Reaktionspläne oder Eskalationspläne, durch die die richtigen Ansprechpartner früher eingebunden werden könnten?
- Schadensbegrenzung — Können Sie die Zeit bis zur Schadensbegrenzung verkürzen? Gibt es Runbook-Schritte, die Sie hinzufügen oder verbessern könnten?
- Prävention — Können Sie future Vorfälle verhindern? Um die Grundursachen eines Vorfalls zu ermitteln, verwendet Amazon bei der Problemuntersuchung den 5-Whys-Ansatz.

Aktionen

Incident Manager erstellt Handlungsempfehlungen, die Sie beim Beantworten der Fragen überprüfen können. Auf dieser Registerkarte können Sie wählen, ob Sie diese Aktionen akzeptieren und abschließen möchten, oder Sie können sie ablehnen. Sie können abgewiesene Aktionspunkte überprüfen, indem Sie Abgelehnte Aktionspunkte wählen. Bei Aktionspunkten handelt es sich um eine Art von Maßnahmen OpsItem , die mit der Analyse und dem Vorfall in verknüpft sind OpsCenter.

Checkliste

Bevor Sie eine Analyse abschließen, überprüfen Sie anhand der Checkliste, welche Maßnahmen ein Responder ergreifen sollte. Wenn die Responder Aktionen in der Checkliste abgeschlossen haben, ändert sich das Symbol neben der Aktion von einer Ellipse in ein Häkchen, was darauf hinweist, dass die Aktion abgeschlossen ist. Wenn Sie die Checklistenelemente nicht abgeschlossen haben, zeigt

Incident Manager eine Meldung an, um zu bestätigen, dass der Responder die Analyse abschließen möchte, ohne sie abzuschließen.

Analyseschemas

Eine Analysevorlage enthält eine Reihe von Fragen, die sich eingehend mit der Grundursache von Vorfällen befassen. Sie können Ihre Antworten auf diese Fragen verwenden, um die Anwendungsleistung und die Reaktion auf Vorfälle zu verbessern.

AWSStandardvorlage

Incident Manager bietet eine Standardvorlage für Fragen, die auf bewährten Methoden zur Reaktion aufAWS Vorfälle und zur Problemanalyse basieren, mit dem Titel`AWSIncidents-PostIncidentAnalysisTemplate`.

Erstellen einer Analysevorlage

Wir empfehlen Ihnen, die`AWSIncidents-PostIncidentAnalysisTemplate` Standardvorlage zu verwenden und zusätzliche Fragen oder Abschnitte hinzuzufügen, die für Ihre Anwendungsfälle geeignet sind. Erstellen Sie Analysevorlagen auf der Grundlage der Standardvorlage Verwenden Sie diese Vorlage als Ausgangspunkt, um Analysevorlagen in Ihrem Verwaltungskonto zu erstellen. Anschließend können Sie Ihre Analysevorlagen für jede Region duplizieren, in der Sie Incident Manager aktiviert haben.

Erstellen einer Analysevorlage

1. Rufen Sie die`GetDocument` Aktion auf und verwenden Sie ihren`Name` Parameter zum Herunterladen`AWSIncidents-PostIncidentAnalysisTemplate`. Weitere Informationen zur`GetDocument` Syntax finden Sie unter Systems Manager Manager-API-Referenz.
2. Der Inhalt der Antwort enthält die JSON-Bausteine für die Analyse. Verwenden Sie die Fragenbausteine, um zusätzliche Fragen in die Analyse einzufügen. Wir empfehlen Ihnen, dem`Incident questions` Abschnitt Fragen oder Abschnitte hinzuzufügen.
3. Verwenden Sie zum Erstellen der neuen Vorlage den`CreateDocument` Vorgang mit dem aktualisierten JSON aus dem vorherigen Schritt. Sie müssen Folgendes angeben, wo der Name Ihrer Vorlage*`Analysis_Template_Name`* ist,

   - `DocumentFormat: "JSON"`
   - `DocumentType: "ProblemAnalysisTemplate"`

- `Name: "Analysis_Template_Name"`

Erstellen einer Analyse

1. Um eine Analyse zu erstellen, wählen Sie auf der Seite mit den Incident-Details eines abgeschlossenen Incidents die Option Analyse erstellen aus.
2. Wählen Sie die Analysevorlage aus, aus der diese Analyse erstellt werden soll, und geben Sie einen beschreibenden Namen für die Analyse ein.
3. Wählen Sie Create (Erstellen) aus.

Drucken Sie eine formatierte Vorfallanalyse

Sie können eine Kopie einer vollständigen oder unvollständigen Analyse erstellen, die für den Druck formatiert ist. Sie können diese Kopie auch als PDF speichern. Sie können eine Analyse nach der anderen drucken. Batch-Drucken von mehreren Analysen wird derzeit nicht unterstützt.

Um eine formatierte Analyse zu drucken

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie die Registerkarte Analyse.
3. Wählen Sie den Titel der Analyse, die Sie drucken möchten.
4. Wählen Sie im Feld oben rechts auf der Seite mit den Analysedetails auf Drucken.
5. Löschen Sie im Dialogfeld Vorfallanalyse drucken die Abschnitte der Analyse, die nicht in der gedruckten Version enthalten sein sollen. Standardmäßig sind alle Abschnitte ausgewählt.
6. Wählen Sie Drucken, um die lokalen Drucksteuerungen für Ihr Gerät zu öffnen.
7. Wählen Sie Ihr Druckziel oder Format. Sie können einen lokalen Drucker oder einen Netzwerkdrucker auswählen, oder Sie können die Analyse als PDF speichern. Nehmen Sie, falls gewünscht, Änderungen an den verbleibenden Druckoptionen vor, und wählen Sie dann Drucken.

> **Note**
>
> Local Print Controls bezieht sich auf die Benutzeroberfläche, die von Ihrem Webbrowser und Gerät bereitgestellt wird.

Druckziele sind diejenigen, die für Ihr Gerät konfiguriert sind und auf die von Ihrem Gerät aus zugegriffen werden kann.

Tutorials zum Incident Manager

Diese Tutorials zu AWS Systems Manager Incident Manager helfen Ihnen beim Aufbau eines robusteren Incident-Management-Systems. Diese Tutorials behandeln allgemeine Aktivitäten, die während eines Vorfalls oder der Reaktion auf Support-Vorfälle auftreten.

Themen

Verwenden von Systems Manager Automation-Runbooks mit Incident Manager

Sie können AWS Systems Manager Automation-Runbooks verwenden, um allgemeine Wartungs-, Bereitstellungs- und Problembehebungsaufgaben für Services zu vereinfachen. AWS In diesem Tutorial erstellen Sie ein benutzerdefiniertes Runbook, um die Reaktion auf Vorfälle in Incident Manager zu automatisieren. Das Szenario für dieses Tutorial beinhaltet einen CloudWatch Amazon-Alarm, der einer Amazon EC2-Metrik zugewiesen ist. Wenn die Instance in einen Zustand übergeht, der den Alarm auslöst, führt Incident Manager automatisch die folgenden Aufgaben aus:

1. Erzeugt einen Vorfall in Incident Manager.
2. Initiiert ein Runbook, das versucht, das Problem zu beheben.
3. Veröffentlicht die Runbook-Ergebnisse auf der Seite mit den Incident-Details in Incident Manager.

Der in diesem Tutorial beschriebene Prozess kann auch mit EventBridge Amazon-Events und anderen Arten von AWS Ressourcen verwendet werden. Indem Sie Ihre Reaktion auf Alarme und Ereignisse automatisieren, können Sie die Auswirkungen eines Vorfalls auf Ihr Unternehmen und dessen Ressourcen reduzieren.

In diesem Tutorial wird beschrieben, wie Sie einen CloudWatch Alarm bearbeiten, der einer Amazon EC2 EC2-Instance für einen Incident Manager-Reaktionsplan zugewiesen ist. Wenn Sie keinen Alarm, keine Instance oder keinen Reaktionsplan konfiguriert haben, empfehlen wir Ihnen, diese Ressourcen zu konfigurieren, bevor Sie beginnen. Weitere Informationen finden Sie unter den folgenden Themen:

- Verwenden von CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch
- Amazon EC2 EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch
- Amazon EC2 EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch
- Arbeiten mit Reaktionsplänen in Incident Manager

> **Important**
>
> Durch die Erstellung von AWS Ressourcen und die Verwendung von Runbook-Automatisierungsschritten entstehen Ihnen Kosten. Weitere Informationen finden Sie unter AWS Preise.

Themen

Aufgabe 1: Das Runbook erstellen

Gehen Sie wie folgt vor, um ein Runbook in der Systems Manager Manager-Konsole zu erstellen. Wenn das Runbook von einem Incident Manager-Incident aus aufgerufen wird, startet es eine Amazon EC2 EC2-Instance neu und aktualisiert den Incident mit Informationen über die Runbook-Ausführung. Bevor Sie beginnen, stellen Sie sicher, dass Sie berechtigt sind, ein Runbook zu erstellen. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Automatisierung einrichten.

> **Important**
>
> Lesen Sie die folgenden wichtigen Informationen zur Erstellung des Runbooks für dieses Tutorial:
>
> - Das Runbook ist für einen Vorfall vorgesehen, der durch eine CloudWatch Alarmquelle ausgelöst wurde. Wenn Sie dieses Runbook für andere Arten von Incidents verwenden,

z. B. für manuell erstellte Incidents, wird das Timeline-Ereignis im ersten Runbook-Schritt nicht gefunden und das System gibt einen Fehler zurück.

- Das Runbook erfordert, dass der CloudWatch Alarm eine Dimension namens enthält. `InstanceId` Alarme für Amazon EC2 EC2-Instance-Metriken haben diese Dimension. Wenn Sie dieses Runbook mit anderen Metriken (oder mit anderen Vorfallquellen wie EventBridge) verwenden, müssen Sie den `JsonDecode2` Schritt so ändern, dass er mit den in Ihrem Szenario erfassten Daten übereinstimmt.
- Das Runbook versucht, das Problem, das den Alarm ausgelöst hat, durch einen Neustart der Amazon EC2 EC2-Instance zu beheben. Bei einem echten Vorfall möchten Sie die Instance möglicherweise nicht neu starten. Aktualisieren Sie das Runbook mit den spezifischen Behebungsmaßnahmen, die das System ergreifen soll.

Weitere Informationen zum Erstellen von Runbooks finden Sie im Benutzerhandbuch unter Arbeiten mit Runbooks.AWS Systems Manager

So erstellen Sie ein Runbook

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Documents (Dokumente) aus.
3. Wählen Sie Automatisierung.
4. Geben Sie unter Name einen beschreibenden Namen für das Runbook ein, z. B. **`IncidentResponseRunbook`**
5. Wählen Sie die Registerkarte Editor und wählen Sie Edit (Bearbeiten) aus.
6. Fügen Sie folgenden Inhalt in den Editor ein:

```
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. Wählen Sie Create automation (Automation erstellen).

Aufgabe 2: Eine IAM-Rolle erstellen

Verwenden Sie das folgende Tutorial, um eine AWS Identity and Access Management (IAM-) Rolle zu erstellen, die Incident Manager die Berechtigung erteilt, ein in einem Reaktionsplan spezifiziertes Runbook zu initiieren. Das Runbook in diesem Tutorial startet eine Amazon EC2 EC2-Instance neu. Sie geben diese IAM-Rolle in der nächsten Aufgabe an, wenn Sie das Runbook mit Ihrem Reaktionsplan verbinden.

Erstellen Sie eine IAM-Rolle, die ein Runbook aus einem Reaktionsplan initiiert

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).
3. Vergewissern Sie sich, dass unter Vertrauenswürdiger Entitätstyp der Dienst ausgewählt ist.AWS
4. Geben Sie unter Anwendungsfall in das Feld Anwendungsfälle für andere AWS Dienste den Wert ein**`Incident Manager`**.
5. Wählen Sie Incident Manager und dann Weiter aus.
6. Wählen Sie auf der Seite „Berechtigungen hinzufügen“ die Option Richtlinie erstellen aus. Der Berechtigungseditor wird in einem neuen Browserfenster oder einer neuen Registerkarte geöffnet.
7. Wählen Sie im Editor die Registerkarte JSON.
8. Kopieren Sie die folgende Berechtigungsrichtlinie und fügen Sie sie in den JSON-Editor ein. Ersetzen Sie *`Account_ID`* durch Ihre AWS-Konto ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:account_ID: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. Wählen Sie Weiter: Markierungen.
10. (Optional) Fügen Sie Ihrer Richtlinie bei Bedarf Tags hinzu.
11. Wählen Sie Weiter: Prüfen aus.
12. Geben Sie im Feld Name einen Namen ein, anhand dessen Sie erkennen können, ob diese Rolle für dieses Tutorial verwendet wird.
13. (Optional) Geben Sie eine Beschreibung in das Feld Beschreibung ein.
14. Wählen Sie Richtlinie erstellen aus.
15. Navigieren Sie zurück zum Browserfenster oder der Registerkarte für die Rolle, die Sie gerade erstellen. Die Seite „Berechtigungen hinzufügen“ wird angezeigt.
16. Wählen Sie die Schaltfläche „Aktualisieren“ (neben der Schaltfläche „Richtlinie erstellen“) und geben Sie dann den Namen der von Ihnen erstellten Berechtigungsrichtlinie in das Filterfeld ein.
17. Wählen Sie die von Ihnen erstellte Berechtigungsrichtlinie aus, und klicken Sie dann auf Weiter.
18. Geben Sie auf der Seite Name, Überprüfung und Erstellung in das Feld Rollenname einen Namen ein, anhand dessen Sie erkennen können, ob diese Rolle für dieses Tutorial verwendet wird.
19. (Optional) Geben Sie eine Beschreibung in das Feld Beschreibung ein.
20. Überprüfen Sie die Rollendetails, fügen Sie bei Bedarf Tags hinzu und wählen Sie Rolle erstellen aus.

Aufgabe 3: Verbinden Sie das Runbook mit Ihrem Reaktionsplan

Indem Sie das Runbook mit Ihrem Incident Manager-Reaktionsplan verbinden, stellen Sie einen konsistenten, wiederholbaren und zeitnahen Abhilfeprozess sicher. Das Runbook dient den Resolvern auch als Ausgangspunkt für die Festlegung ihrer nächsten Vorgehensweise.

Um das Runbook Ihrem Reaktionsplan zuzuweisen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie Reaktionspläne aus.
3. Wählen Sie für Reaktionsplan einen vorhandenen Reaktionsplan aus und klicken Sie auf Bearbeiten. Wenn Sie noch keinen Reaktionsplan haben, wählen Sie Reaktionsplan erstellen aus, um einen neuen Plan zu erstellen.

   Füllen Sie die folgenden Felder aus:

   a. Wählen Sie im Abschnitt Runbook die Option Existierendes Runbook auswählen aus.
   b. Vergewissern Sie sich, dass für Besitzer die Option Mein Eigentum ausgewählt ist.
   c. Wählen Sie für Runbook das Runbook aus, in dem Sie es erstellt haben. Aufgabe 1: Das Runbook erstellen
   d. Wählen Sie bei der Ausführung als Version die Option Standard aus.
   e. Wählen Sie im Abschnitt Eingaben für den Parameter IncidentRecordArn die Option Incident ARN aus.
   f. Wählen Sie im Abschnitt Ausführungsberechtigungen die IAM-Rolle aus, in Aufgabe 2: Eine IAM-Rolle erstellen der Sie sie erstellt haben.
4. Speichern Sie Ihre Änderungen.

Aufgabe 4: Ihrem Reaktionsplan einen CloudWatch Alarm zuordnen

Gehen Sie wie folgt vor, um Ihrem Reaktionsplan einen CloudWatch Alarm für eine Amazon EC2 EC2-Instance zuzuweisen.

Um Ihrem CloudWatch Reaktionsplan einen Alarm zuzuweisen

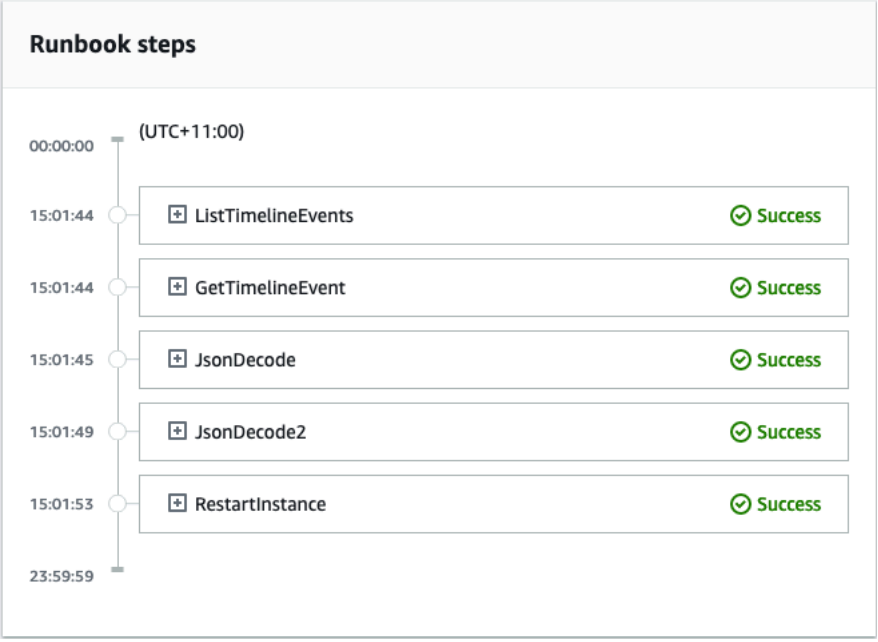
1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich unter Alarme die Option Alle Alarme aus.
3. Wählen Sie einen Alarm für eine Amazon EC2 EC2-Instance aus, die Sie mit Ihrem Reaktionsplan verbinden möchten.
4. Wählen Sie Actions und anschließend Bearbeiten. Stellen Sie sicher, dass die Metrik eine Dimension namens `InstanceId` hat.
5. Wählen Sie Weiter aus.

6. Wählen Sie für den Assistenten zum Konfigurieren von Aktionen die Option Systems Manager Manager-Aktion hinzufügen aus.
7. Wählen Sie Incident erstellen aus.
8. Wählen Sie den Reaktionsplan aus, in dem Sie ihn erstellt habenAufgabe 3: Verbinden Sie das Runbook mit Ihrem Reaktionsplan.
9. Wählen Sie Update Alarm (Alarm bearbeiten) aus.

Aufgabe 5: Überprüfung der Ergebnisse

Um zu überprüfen, ob der CloudWatch Alarm einen Vorfall verursacht und anschließend das in Ihrem Reaktionsplan angegebene Runbook verarbeitet, müssen Sie den Alarm auslösen. Nachdem Sie den Alarm ausgelöst haben und die Verarbeitung des Runbooks abgeschlossen ist, können Sie die Ergebnisse des Runbooks mithilfe des folgenden Verfahrens überprüfen. Informationen zum Auslösen eines Alarms finden Sie unter set-alarm-state in der Befehlsreferenz.AWS CLI

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie den Vorfall aus, der durch den CloudWatch Alarm ausgelöst wurde.
3. Wählen Sie die Registerkarte Runbooks.
4. Sehen Sie sich die auf Ihrer Amazon EC2 EC2-Instance ausgeführten Aktionen im Abschnitt Runbook-Schritte an. Die folgende Abbildung zeigt ein Beispiel, das die Schritte zeigt, die das Runbook unternommen hat, das Sie in diesem Tutorial erstellt haben. Jeder Schritt wird mit einem Zeitstempel und einer Statusmeldung aufgeführt.



Um alle Details des CloudWatch Alarms anzuzeigen, erweitern Sie den Schritt JsonDecode2 und dann Ausgabe.

> **Important**
>
> Sie müssen alle Ressourcenänderungen bereinigen, die Sie in diesem Tutorial vorgenommen haben und die Sie nicht behalten möchten. Dazu gehören Änderungen an Incident Manager-Ressourcen wie Ressourcenplänen und Incidents, Änderungen an CloudWatch Alarmen und die IAM-Rolle, die Sie für dieses Tutorial erstellt haben.

Verwaltung von Sicherheitsvorfällen im Incident Manager

Sie können Amazon und Incident Manager zusammen verwenden AWS Security Hub EventBridge, um Sicherheitsvorfälle in Ihren AWS gehosteten Anwendungen zu identifizieren und zu verwalten. In diesem Tutorial erfahren Sie, wie Sie eine EventBridge Regel konfigurieren, die auf automatisch gesendeten Ergebnissen von Security Hub basiert, einen Vorfall erstellt.

> **Note**
>
> In diesem Tutorial wird EventBridge Security Hub verwendet. Durch die Nutzung dieser Dienste können Ihnen Kosten entstehen.

Voraussetzungen

- Richten Sie Security Hub ein. Weitere Informationen finden Sie unter Einrichten von AWS Security Hub.
- Erstellen oder aktualisieren Sie Ergebnisse in Security Hub. Weitere Informationen finden Sie unter Ergebnisse in AWS Security Hub.
- Konfigurieren Sie einen Reaktionsplan, den Incident Manager bei der Erstellung Ihres Sicherheitsvorfalls als Vorlage verwendet. Weitere Informationen finden Sie unter Vorbereitung auf Vorfälle im Incident Manager.

In diesem Tutorial verwenden wir ein vordefiniertes Muster, um die EventBridge Regel zu erstellen. Informationen zum Erstellen der Regel mithilfe eines benutzerdefinierten Musters finden Sie im AWS

Security Hub Benutzerhandbuch unter Verwenden eines benutzerdefinierten Musters zum Erstellen der Regel.

Erstellen Sie eine EventBridge Regel

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules aus.
3. Wählen Sie Regel erstellen aus.
4. Geben Sie einen Name (Namen) und eine Description (Beschreibung) für die Regel ein.

   Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
5. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus.
6. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie als Eventquelle AWS Events oder EventBridge Partnerevents aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie als AWS Service Security Hub.
12. Wählen Sie als Ereignistyp die Option Security Hub Findings — Importiert aus.
13. Standardmäßig EventBridge konfiguriert das Ereignismuster ohne Filterwerte. Für jedes Attribut ist die Option Beliebiger ***Attributname*** ausgewählt. Aktualisieren Sie diese Filter, um Vorfälle zu erstellen, die auf den Sicherheitsergebnissen basieren, die sich am stärksten auf Ihre Umgebung auswirken.
14. Klicken Sie auf Weiter.
15. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
16. Wählen Sie unter Ziel auswählen die Option Incident Manager-Reaktionsplan aus.
17. Wählen Sie unter Reaktionsplan einen Reaktionsplan aus, der als Vorlage für erstellte Vorfälle verwendet werden soll.
18. EventBridge kann die IAM-Rolle erstellen, die für die Ausführung Ihrer Regel erforderlich ist.

    - Um eine IAM-Rolle automatisch zu erstellen, wählen Sie Neue Rolle für die spezifische Ressource erstellen aus.

- Um eine IAM-Rolle zu verwenden, die bereits in Ihrem Konto vorhanden ist, wählen Sie Bestehende Rolle verwenden.

19. (Optional) Geben Sie ein oder mehrere Tags für die Regel ein.
20. Wählen Sie Weiter aus.
21. Überprüfen Sie die Details der Regel und wählen Sie dann Create rule (Regel erstellen) aus.

Nachdem Sie diese EventBridge Regel erstellt haben, führen Sicherheitsergebnisse, die den von Ihnen definierten Attributwerten entsprechen, zu Vorfällen in Incident Manager. Sie können diese Vorfälle nach dem Vorfall sortieren, verwalten, überwachen und Analysen nach dem Vorfall erstellen.

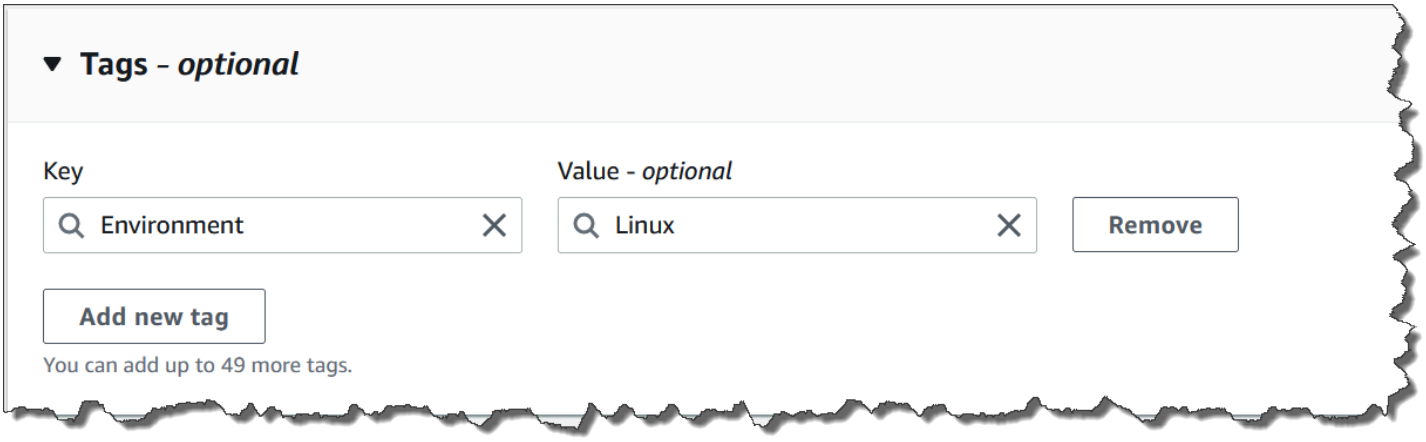
Taggen von Ressourcen in Incident Manager

Tags sind optionale Metadaten, die Sie Ihren -Incident-Manager-Ressourcen in der jeweiligenAWS-Regionen Replikationsgruppe zuweisen können. Sie können Reaktionsplänen, Vorfallaufzeichnungen und Kontakten Stichwörter zuweisen. Sie können Bereitschaftsplänen und Rotationen auch Stichwörter hinzufügen. Sie können auch dem Replikationssatz selbst Stichwörter hinzufügen. Mit Tags können Sie -Ressourcen auf unterschiedliche Weise kategorisieren und den Zugriff auf diese Ressourcen zuweisen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Wir empfehlen die Verwendung von Tag-Schlüsseln, die Anforderungen der jeweiligen Ressourcentypen erfüllen. Eine Anzahl einheitlicher Tag-Schlüssel vereinfacht das Verwalten der Ressourcen und den Zugriff auf sie zuweisen. Sie können die Ressourcen auf Grundlage von Tags durchsuchen und filtern. Weitere Informationen zur Steuerung des Zugriffs auf Ressourcen mithilfe von Tags finden Sie im IAM-Benutzerhandbuch unter Steuern des Zugriffs aufAWS Ressourcen mithilfe von Tags.

Bei der Erstellung eines Reaktionsplans können Sie im Standardabschnitt Incident Tags angeben. Diese Tags werden auf den Incident-Datensatz angewendet, wenn ein Incident mithilfe des Reaktionsplans erstellt wird.

> **Note**
>
> Tags haben keine semantische Bedeutung. Sie werden streng als Zeichenfolge interpretiert.

Sie können die Tags über die Incident-Manager-Konsole hinzufügen oder entfernen. Der folgende Screenshot zeigt den Abschnitt mit den Tags bei der Erstellung eines neuen Reaktionsplans.



Um programmgesteuert mit Tags zu arbeiten, verwenden Sie die folgenden API-Aktionen:

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> Stichwörter, die auf Reaktionspläne, Vorfalldatensätze, Kontakte, Bereitschaftspläne und Rotationen sowie Replikationssätze angewendet wurden, können nur vom Konto des Ressourcenbesitzers aus angezeigt und geändert werden.

Sicherheit in AWS Systems Manager Incident Manager

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Systems Manager Incident Manager, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Incident Manager anwenden können. In den folgenden Themen erfahren Sie, wie Sie Incident Manager so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen helfen, Ihre Incident Manager-Ressourcen zu überwachen und zu schützen.

Themen

- Konfiguration und Schwachstellenanalyse in Incident Manager
- Bewährte Sicherheitsmethoden in AWS Systems Manager Incident Manager

Datenschutz im Incident Manager

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Systems Manager Incident Manager. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit

Incident Manager oder anderen Geräten arbeiten und die Konsole, die API oder SDKs AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Standardmäßig verschlüsselt Incident Manager Daten während der Übertragung mit SSL/TLS.

Datenverschlüsselung

Incident Manager verwendet AWS Key Management Service (AWS KMS) -Schlüssel, um Ihre Incident Manager-Ressourcen zu verschlüsseln. Weitere Informationen zu AWS KMS finden Sie im AWS KMS Entwicklerhandbuch. AWS KMS kombiniert sichere, hochverfügbare Hardware und Software zu einem für die Cloud skalierten Schlüsselverwaltungssystem. Incident Manager verschlüsselt Ihre Daten mit Ihrem angegebenen Schlüssel und verschlüsselt Metadaten mit einem AWS eigenen Schlüssel. Um Incident Manager verwenden zu können, müssen Sie Ihren Replikationssatz einrichten, der auch die Verschlüsselung einschließt. Für die Verwendung von Incident Manager ist eine Datenverschlüsselung erforderlich.

Sie können einen AWS eigenen Schlüssel verwenden, um Ihren Replikationssatz zu verschlüsseln, oder Sie können Ihren eigenen, vom Kunden verwalteten Schlüssel verwenden, den Sie erstellt haben, AWS KMS um die Regionen in Ihrem Replikationssatz zu verschlüsseln. Incident Manager unterstützt nur symmetrische AWS KMS Verschlüsselungsschlüssel zur Verschlüsselung Ihrer darin erstellten Daten. AWS KMS Incident Manager unterstützt keine AWS KMS Schlüssel mit importiertem Schlüsselmaterial, benutzerdefinierte Schlüsselspeicher, Hash-basierter Nachrichtenauthentifizierungscode (HMAC) oder andere Schlüsseltypen. Wenn Sie vom Kunden verwaltete Schlüssel verwenden, verwenden Sie die AWS KMS Konsole oder AWS KMS APIs, um die vom Kunden verwalteten Schlüssel zentral zu erstellen und die wichtigsten Richtlinien zu definieren, die steuern, wie Incident Manager die vom Kunden verwalteten Schlüssel verwenden kann. Wenn Sie einen vom Kunden verwalteten Schlüssel für die Verschlüsselung mit Incident Manager verwenden, muss sich der vom AWS KMS Kunden verwaltete Schlüssel in derselben Region wie die Ressourcen befinden. Weitere Informationen zur Einrichtung der Datenverschlüsselung in Incident Manager finden Sie unterAssistent zur Vorbereitung.

Für die Verwendung von vom AWS KMS Kunden verwalteten Schlüsseln fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter AWS KMS Konzepte — KMS-Schlüssel im AWS Key Management Service Entwicklerhandbuch und unter AWS KMS Preise.

> **Important**
>
> Wenn Sie einen vom Kunden verwalteten Schlüssel (CMK) verwenden, um Ihren Replikationssatz und die Incident Manager-Daten zu verschlüsseln, sich aber später dazu entschließen, den Replikationssatz zu löschen, müssen Sie den Replikationssatz löschen, bevor Sie den CMK deaktivieren oder löschen.

Damit Incident Manager Ihren vom Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Daten verwenden kann, müssen Sie der Schlüsselrichtlinie Ihres vom Kunden verwalteten Schlüssels die folgenden Richtlinienerklärungen hinzufügen. Weitere Informationen zum Einrichten und Ändern der wichtigsten Richtlinien in Ihrem Konto finden Sie im AWS KMSAWS Key Management Service Entwicklerhandbuch unter Verwenden wichtiger Richtlinien. Die Richtlinie bietet die folgenden Berechtigungen:

- Ermöglicht Incident Manager, schreibgeschützte Operationen durchzuführen, um den CMK für Incident Manager in Ihrem Konto zu finden.
- Ermöglicht es Incident Manager, den CMK zur Erstellung von Zuschüssen und zur Beschreibung des Schlüssels zu verwenden, aber nur, wenn der CMK im Namen von Principals im Account handelt, die berechtigt sind, Incident Manager zu verwenden. Wenn die in der Richtlinienerklärung angegebenen Principals nicht berechtigt sind, die KMS-Schlüssel zu verwenden und Incident Manager zu verwenden, schlägt der Anruf fehl, auch wenn er vom Incident Manager-Service stammt.

```
{
"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.amazonaws.com",
            "ssm-contacts.amazonaws.com"
          ]
        }
      }
    }
```

Ersetzen Sie den `Principal` Wert durch den IAM-Prinzipal, der Ihren Replikationssatz erstellt hat.

Incident Manager verwendet bei allen Anfragen an kryptografische Operationen einen Verschlüsselungskontext. AWS KMS Sie können diesen Verschlüsselungskontext verwenden, um CloudTrail Protokollereignisse zu identifizieren, bei denen Incident Manager Ihre KMS-Schlüssel verwendet. Incident Manager verwendet den folgenden Verschlüsselungskontext:

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

Identity and Access Management für AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Incident Manager-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Problembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Incident Manager ausführen.

Dienstbenutzer — Wenn Sie den Incident Manager-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Incident Manager-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Incident Manager nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterProblembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Incident Manager-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Incident Manager. Es ist Ihre Aufgabe, zu bestimmen, auf welche Incident Manager-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Incident Manager nutzen kann, finden Sie unterWie AWS Systems Manager Incident Manager funktioniert mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Incident Manager zu verwalten. Beispiele für identitätsbasierte Incident Manager-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie

sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services

könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer

Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Systems Manager Incident Manager funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf Incident Manager verwenden, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Incident Manager verfügbar sind.

IAM-Funktionen, die Sie mit verwenden können AWS Systems Manager Incident Manager

IAM-Feature	Unterstützung durch Incident Manager
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Nein

IAM-Feature	Unterstützung durch Incident Manager
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Incident Manager und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Incident Manager unterstützt keine Richtlinien, die den Zugriff auf gemeinsam genutzte Ressourcen verweigern. AWS RAM

Identitätsbasierte Richtlinien für Incident Manager

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Incident Manager

Beispiele für identitätsbasierte Richtlinien von Incident Manager finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager

Ressourcenbasierte Richtlinien in Incident Manager

Unterstützt ressourcenbasierte Richtlinien	Ja

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Der Incident Manager-Dienst unterstützt nur zwei Arten von ressourcenbasierten Richtlinien, die entweder über die AWS RAM Konsole oder über die PutResourcePolicy Aktion aufgerufen werden, die an einen Reaktionsplan oder Kontakt angehängt ist. Diese Richtlinie legt fest, welche Principals Aktionen im Zusammenhang mit den Reaktionsplänen, Kontakten, Eskalationsplänen und Vorfällen durchführen können. Incident Manager verwendet ressourcenbasierte Richtlinien, um Ressourcen für mehrere Konten gemeinsam zu nutzen.

Incident Manager unterstützt keine Richtlinien, die den Zugriff auf gemeinsam genutzte Ressourcen verweigern AWS RAM.

Informationen zum Anhängen einer ressourcenbasierten Richtlinie an einen Reaktionsplan oder Kontakt finden Sie unter. Regions- und kontenübergreifendes Incident-Management im Incident Manager

Beispiele für ressourcenbasierte Richtlinien in Incident Manager

Beispiele für ressourcenbasierte Richtlinien von Incident Manager finden Sie unter. Beispiele für ressourcenbasierte Richtlinien für AWS Systems Manager Incident Manager

Richtlinienaktionen für Incident Manager

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Incident Manager-Aktionen finden Sie unter Aktionen definiert von AWS Systems Manager Incident Manager in der Service Authorization Reference.

Bei Richtlinienaktionen in Incident Manager werden vor der Aktion die folgenden Präfixe verwendet:

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

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Get` beginnen, einschließlich der folgenden Aktion:

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

Beispiele für identitätsbasierte Richtlinien von Incident Manager finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager

Incident Manager verwendet Aktionen in zwei verschiedenen Namespaces: SSM-Incidents und SSM-Contacts. Achten Sie beim Erstellen von Richtlinien für Incident Manager darauf, den richtigen Namespace für die Aktion zu verwenden. SSM-Incidents wird für Reaktionspläne und Maßnahmen im Zusammenhang mit Vorfällen verwendet. SSM-Contacts wird für Aktionen im Zusammenhang mit Kontakten und Kontaktbindung verwendet. Beispielsweise:

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

Richtlinienressourcen für Incident Manager

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen

(ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Incident Manager-Ressourcentypen und ihrer ARNs finden Sie unter Ressourcen definiert von AWS Systems Manager Incident Manager in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Systems Manager Incident Manager definierte Aktionen.

Beispiele für identitätsbasierte Incident Manager-Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager

Incident Manager-Ressourcen werden verwendet, um Vorfälle zu erstellen, in Chat-Kanälen zusammenzuarbeiten, Vorfälle zu lösen und Einsatzkräfte einzubeziehen. Wenn ein Benutzer Zugriff auf einen Reaktionsplan hat, hat er Zugriff auf alle daraus erstellten Incidents. Wenn ein Benutzer Zugriff auf einen Kontakt- oder Eskalationsplan hat, kann er den Kontakt oder die Kontakte im Eskalationsplan einbeziehen.

Schlüssel zur Richtlinienbedingung für Incident Manager

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Zugriffskontrolllisten (ACLs) in Incident Manager

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Incident Manager

Unterstützt ABAC (Tags in Richtlinien)	Nein

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Incident Manager

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipalberechtigungen für Incident Manager

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Incident Manager

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Incident Manager beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Incident Manager Sie dazu anleitet.

Auswahl einer IAM-Rolle in Incident Manager

Wenn Sie eine Reaktionsplanressource in Incident Manager erstellen, müssen Sie eine Rolle auswählen, damit Incident Manager in Ihrem Namen ein Systems Manager Manager-Automatisierungsdokument ausführen kann. Wenn Sie zuvor eine Servicerolle oder eine dienstbezogene Rolle erstellt haben, stellt Ihnen Incident Manager eine Liste von Rollen zur Auswahl zur Verfügung. Es ist wichtig, eine Rolle auszuwählen, die den Zugriff auf die Ausführung Ihrer Automatisierungsdokumentinstanzen ermöglicht. Weitere Informationen finden Sie unter Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager. Wenn Sie einen AWS Chatbot Chat-Kanal erstellen, der während eines Vorfalls verwendet werden soll, können Sie eine Servicerolle auswählen, mit der Sie Befehle direkt aus dem Chat verwenden können. Weitere Informationen zum Erstellen von Chat-Kanälen für die Zusammenarbeit bei Vorfällen finden Sie unterArbeiten

mit Chat-Kanälen in Incident Manager. Weitere Informationen zu IAM-Richtlinien finden Sie unter Verwaltung von Berechtigungen für die Ausführung von Befehlen mithilfe AWS Chatbot des AWS Chatbot Administratorhandbuchs. AWS Chatbot

Dienstbezogene Rollen für Incident Manager

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Informationen zum Erstellen oder Verwalten von dienstbezogenen Rollen in Incident Manager finden Sie unter. Verwenden von serviceverknüpften Rollen für Incident Manager

Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Incident Manager-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von Incident Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Systems Manager Incident Manager in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien

- Verwenden der Incident Manager-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Zugriff auf einen Reaktionsplan

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Incident Manager-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue

und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Incident Manager-Konsole

Um auf die AWS Systems Manager Incident Manager Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Incident Manager-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen den Vorfall mithilfe der Incident Manager-Konsole lösen können, fügen Sie den Entitäten auch die `IncidentManagerResolverAccess` AWS verwaltete Incident Manager-Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

```
IncidentManagerResolverAccess
```

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder 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": "*"
        }
    ]
}
```

Zugriff auf einen Reaktionsplan

In diesem Beispiel möchten Sie einem IAM-Benutzer in Ihrem Amazon Web Services Services-Konto Zugriff auf einen Ihrer Incident Manager-Reaktionspläne gewähren. `exampleplan` Sie möchten dem Benutzer auch ermöglichen, den Reaktionsplan hinzuzufügen, zu aktualisieren und zu löschen.

Die Richtlinie gewährt `ssm-incidents:ListResponsePlans` dem Benutzer die `ssm-incident:ListResponsePlan` Berechtigungen`ssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` und.

```
{
   "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/*"
      }
   ]
}
```

Beispiele für ressourcenbasierte Richtlinien für AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager unterstützt ressourcenbasierte Berechtigungsrichtlinien für Reaktionspläne und Kontakte von Incident Manager.

Incident Manager unterstützt keine ressourcenbasierten Richtlinien, die den Zugriff auf gemeinsam genutzte Ressourcen verweigern. AWS RAM

Informationen zum Erstellen eines Reaktionsplans oder Kontakts finden Sie unter Arbeiten mit Reaktionsplänen in Incident Manager und. Mit Kontakten im Incident Manager arbeiten

Beschränken des Zugriffs auf den Reaktionsplan von Incident Manager nach Organisation

Im folgenden Beispiel werden Benutzern in der Organisation mit der Organisations-ID: Berechtigungen erteilt, um auf Vorfälle `o-abc123def45` zu reagieren, die mithilfe des Reaktionsplans `myplan` erstellt wurden.

Der `Condition` Block verwendet die `StringEquals` Bedingungen und den `aws:PrincipalOrgID` Bedingungsschlüssel, der ein AWS Organizations bestimmter Bedingungsschlüssel ist. Weitere Informationen zu diesen Bedingungsschlüsseln finden Sie unter Bedingungen in einer Richtlinie angeben.

```
{
  "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/*"
      ]
    }
  ]
}
```

Bereitstellung von Kontaktzugriff für Incident Manager für einen Principal

Im folgenden Beispiel wird dem Principal mit dem ARN die Erlaubnis erteilt, Engagements für den Kontakt `arn:aws:iam::999988887777:root` `mycontact` zu erstellen.

```
{
    "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/*"
            ]
        }
    ]
}
```

Dienstübergreifende Vermeidung verwirrter stellvertretender Mitarbeiter in Incident Manager

Das Problem des verwirrten Stellvertreters ist ein Problem der Informationssicherheit, das auftritt, wenn eine Entität, die nicht berechtigt ist, eine Aktion auszuführen, eine Entität mit mehr Rechten zur Ausführung der Aktion aufruft. Auf diese Weise können böswillige Akteure Befehle ausführen oder Ressourcen ändern, zu deren Ausführung oder Zugriff sie sonst nicht berechtigt wären.

In AWS kann ein dienstübergreifendes Identitätswechsels zu einem verwirrten Szenario für Stellvertreter führen. Ein dienstübergreifender Identitätswechsel liegt vor, wenn ein Dienst (der anrufende Dienst) einen anderen Dienst (den angerufenen Dienst) anruft. Ein böswilliger Akteur kann den anrufenden Dienst verwenden, um Ressourcen in einem anderen Dienst mithilfe von Berechtigungen zu ändern, über die er normalerweise nicht verfügen würde.

AWS bietet Dienstprinzipalen verwalteten Zugriff auf Ressourcen in Ihrem Konto, um Sie beim Schutz Ihrer Ressourcen zu unterstützen. Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ihren Ressourcenrichtlinien zu verwenden. Diese Schlüssel schränken die Berechtigungen ein, AWS Systems Manager Incident Manager die dieser Ressource einen anderen Dienst gewähren. Wenn Sie beide Kontextschlüssel für globale Bedingungen verwenden, müssen der `aws:SourceAccount` Wert und das Konto, auf das im `aws:SourceArn` Wert verwiesen wird, dieselbe Konto-ID verwenden, wenn sie in derselben Richtlinienanweisung verwendet werden.

Der Wert von `aws:SourceArn` muss der ARN des betroffenen Incident-Datensatzes sein. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den `aws:SourceArn` globalen Kontextbedingungsschlüssel mit dem * Platzhalter für die unbekannten Teile des ARN. Sie können beispielsweise festlegen `aws:SourceArn` auf`arn:aws:ssm-incidents::111122223333:*`.

Im folgenden Beispiel für eine Vertrauensrichtlinie verwenden wir den `aws:SourceArn` Bedingungsschlüssel, um den Zugriff auf die Servicerolle auf der Grundlage des ARN des Incident-Datensatzes einzuschränken. Nur Incident-Datensätze, die anhand des Reaktionsplans `myresponseplan` erstellt wurden, können diese Rolle verwenden.

```
{
  "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/*"
      }
    }
  }
}
```

Verwenden von serviceverknüpften Rollen für Incident Manager

AWS Systems Manager Incident Manager verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit Incident Manager verknüpft ist. Servicebezogene Rollen sind von Incident Manager vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von Incident Manager, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Incident Manager definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Incident Manager seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Incident Manager-Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Mit dem Dienst verknüpfte Rollenberechtigungen für Incident Manager

Incident Manager verwendet die dienstbezogene Rolle mit dem Namen AWSServiceRoleforIncidentManager— ermöglicht es Incident Manager, Incident Manager-Incident-Aufzeichnungen und zugehörige Ressourcen in Ihrem Namen zu verwalten.

Die AWSServiceRoleforIncidentManager dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `ssm-incidents.amazonaws.com`

Die Richtlinie für Rollenberechtigungen `AWSIncidentManagerServiceRolePolicy`ermöglicht es Incident Manager, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion: für alle Ressourcen, die sich `ssm-incidents:ListIncidentRecords` auf die Aktion beziehen.

- Maßnahme: `ssm-incidents:CreateTimelineEvent` für alle Ressourcen im Zusammenhang mit der Aktion.
- Maßnahme: `ssm:CreateOpsItem` für alle Ressourcen im Zusammenhang mit der Aktion.
- Aktion: `ssm:AssociateOpsItemRelatedItem` für `all resources related to the action.`
- Maßnahme: `ssm-contacts:StartEngagement` für alle Ressourcen im Zusammenhang mit der Aktion.
- Aktion: `cloudwatch:PutMetricData` für CloudWatch Metriken innerhalb des `AWS/IncidentManager` Namespace

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

Eine dienstbezogene Rolle für Incident Manager erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen Replikationssatz in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt Incident Manager die serviceverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie einen Replikationssatz erstellen, erstellt Incident Manager die serviceverknüpfte Rolle erneut für Sie.

Eine serviceverknüpfte Rolle für Incident Manager bearbeiten

Incident Manager erlaubt es Ihnen nicht, die AWSServiceRoleforIncidentManager dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Incident Manager

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise ist keine ungenutzte Entität vorhanden, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Um die serviceverknüpfte Rolle zu löschen, müssen Sie zuerst den Replikationssatz löschen. Beim Löschen des Replikationssatzes werden alle in Incident Manager erstellten und gespeicherten Daten gelöscht, einschließlich Reaktionsplänen, Kontakten und Eskalationsplänen. Außerdem gehen alle zuvor erstellten Incidents verloren. Alarme und EventBridge Regeln, die auf gelöschte Reaktionspläne verweisen, führen nicht mehr zu einem Vorfall, wenn ein Alarm oder eine Regelübereinstimmung vorliegt. Um den Replikationssatz zu löschen, müssen Sie jede Region im Satz löschen.

> **Note**
>
> Wenn der Incident Manager-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die Regionen in der Replikationsgruppe zu löschen, die von AWSServiceRoleforIncidentManager

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie eine Region im Replikationssatz aus.
3. Wählen Sie Löschen aus.
4. Um das Löschen der Region zu bestätigen, geben Sie den Namen der Region ein und wählen Sie Löschen.
5. Wiederholen Sie diese Schritte, bis Sie alle Regionen in Ihrem Replikationssatz gelöscht haben. Wenn Sie die letzte Region löschen, werden Sie von der Konsole darüber informiert, dass auch der Replikationssatz gelöscht wird.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleforIncidentManager serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Incident Manager-Rollen

Incident Manager unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und Endpunkte.

AWS verwaltete Richtlinien für AWS Systems Manager Incident Manager

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSIncidentManagerIncidentAccessServiceRolePolicy

Sie können `AWSIncidentManagerIncidentAccessServiceRolePolicy` an Ihre IAM-Entitäten anhängen. Incident Manager ordnet diese Richtlinie auch einer Incident-Manager-Rolle zu, die es Incident Manager ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Diese Richtlinie gewährt nur Leseberechtigungen, die es Incident Manager ermöglichen, Ressourcen in bestimmten anderen Bereichen zu lesen, AWS-Services um Ergebnisse im Zusammenhang mit Vorfällen in diesen Diensten zu identifizieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `cloudformation`— Ermöglicht Prinzipalen die Beschreibung von Stacks. AWS CloudFormation Dies ist erforderlich, damit Incident Manager CloudFormation Ereignisse und Ressourcen im Zusammenhang mit einem Vorfall identifizieren kann.
- `codedeploy`— Ermöglicht Prinzipalen das Lesen von AWS CodeDeploy Bereitstellungen. Dies ist erforderlich, damit Incident Manager CodeDeploy Bereitstellungen und Ziele im Zusammenhang mit einem Vorfall identifizieren kann.
- `autoscaling`— Ermöglicht Prinzipalen festzustellen, ob eine Amazon Elastic Compute Cloud (EC2) -Instance Teil einer Auto Scaling Scaling-Gruppe ist. Dies ist erforderlich, damit Incident Manager Ergebnisse für EC2-Instances bereitstellen kann, die Teil von Auto Scaling Scaling-Gruppen sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie AWSIncidentManagerIncidentAccessServiceRolePolicyim AWS Managed Policy Reference Guide.

Von AWS verwaltete Richtlinie: **`AWSIncidentManagerServiceRolePolicy`**

Sie können `AWSIncidentManagerServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es Incident Manager ermöglicht,

Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Incident Manager.

Diese Richtlinie gewährt Incident Manager die Berechtigung, Vorfälle aufzulisten, Zeitplanereignisse zu erstellen, zugehörige Elemente zu erstellen OpsItems, ihnen zuzuordnen OpsItems, Interaktionen zu starten und CloudWatch Metriken zu veröffentlichen, die sich auf einen Vorfall beziehen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ssm-incidents`— Ermöglicht Principals, Vorfälle aufzulisten und Zeitplanereignisse zu erstellen. Dies ist erforderlich, damit die Einsatzkräfte während eines Vorfalls im Incident-Dashboard zusammenarbeiten können.
- `ssm`— Ermöglicht Prinzipalen das Erstellen OpsItems und Zuordnen verwandter Elemente. Dies ist erforderlich, um ein übergeordnetes Element zu erstellen OpsItem , wenn ein Vorfall beginnt.
- `ssm-contacts`— Ermöglicht es Schulleitern, Engagements zu beginnen. Dies ist erforderlich, damit Incident Manager während eines Vorfalls mit Kontakten Kontakt aufnehmen kann.
- `cloudwatch`— Ermöglicht Prinzipalen die Veröffentlichung von CloudWatch Metriken. Dies ist erforderlich, damit Incident Manager Kennzahlen zu einem Vorfall veröffentlichen kann.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/IncidentManager"
                }
            }
        }
    ]
}
```

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie AWSIncidentManagerServiceRolePolicyim Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: **`AWSIncidentManagerResolverAccess`**

Sie können eine Verbindung `AWSIncidentManagerResolverAccess` zu Ihren IAM-Entitäten herstellen, damit diese Incidents starten, anzeigen und aktualisieren können. Auf diese Weise können sie auch Ereignisse in der Kundenzeitleiste und zugehörige Elemente im Incident-Dashboard erstellen. Sie können diese Richtlinie auch der AWS Chatbot Servicerolle oder direkt Ihrer vom Kunden verwalteten Rolle hinzufügen, die einem beliebigen Chat-Kanal zugeordnet ist, der für die Zusammenarbeit bei Vorfällen verwendet wird. Weitere Informationen zu IAM-Richtlinien finden Sie unter Verwaltung von Berechtigungen für die Ausführung von Befehlen mithilfe AWS Chatbot des AWS Chatbot Administratorhandbuchs. AWS Chatbot

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ssm-incidents`— Ermöglicht es Ihnen, Incidents zu starten, Reaktionspläne aufzulisten, Incidents aufzulisten, Incidents zu aktualisieren, Timeline-Ereignisse aufzulisten, benutzerdefinierte Timeline-Ereignisse zu erstellen, benutzerdefinierte Timeline-Ereignisse zu aktualisieren, benutzerdefinierte Timeline-Ereignisse zu löschen, verwandte Elemente aufzulisten, verwandte Elemente zu erstellen und zugehörige Elemente zu aktualisieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
```

```
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zur Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie AWSIncidentManagerResolverAccessim Referenzhandbuch für AWS verwaltete Richtlinien.

Incident Manager aktualisiert AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Incident Manager an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite Incident Manager-Dokumentenverlauf.

Änderung	Beschreibung	Datum
AWSIncidentManagerIncidentAccessServiceRolePolicy — Aktualisierung der Richtlinie	Incident Manager hat zur Unterstützung der `AWSIncidentManagerIncidentAccessServiceRolePolicy` Findings-Funktion eine neue Berechtigung hinzugefügt, mit der geprüft werden kann, ob eine EC2-Instance Teil einer Auto Scaling Scaling-Gruppe ist.	20. Februar 2024
`AWSIncidentManagerIncidentAccessServ`	Incident Manager hat eine neue Richtlinie hinzugefü	17. November 2023

Änderung	Beschreibung	Datum
iceRolePolicy – Neue Richtlinie.	gt, die Incident Manager berechtigt, im Rahmen der Verwaltung eines Vorfalls andere AWS-Services Personen anzurufen.	
AWSIncidentManager ServiceRolePolicy — Aktualisierung der Richtlinie	Incident Manager hat eine neue Berechtigung hinzugefü gt, die es Incident Manager ermöglicht, Metriken in Ihrem Konto zu veröffentlichen.	16. Dezember 2022
AWSIncidentManager ResolverAccess – Neue Richtlinie.	Incident Manager hat eine neue Richtlinie hinzugefügt, mit der Sie Incidents starten, Reaktionspläne auflisten, Incidents auflisten, Incidents aktualisieren, Timeline-Ereignisse auflisten, benutzerd efinierte Timeline-Ereignisse erstellen, benutzerdefinierte Timeline-Ereignisse aktualisi eren, benutzerdefinierte Timeline-Ereignisse löschen, verwandte Elemente auflisten, verwandte Elemente erstellen und verwandte Elemente aktualisieren können.	26. April 2021

Änderung	Beschreibung	Datum
AWSIncidentManagerServiceRolePolicy – Neue Richtlinie.	Incident Manager hat eine neue Richtlinie hinzugefügt, mit der Incident Manager berechtigt ist, Vorfälle aufzulisten, Zeitplanereignisse zu erstellen OpsItems, zugehörige Elemente zu erstellen OpsItems, zugehörige Elemente zu erstellen und Interaktionen im Zusammenhang mit einem Vorfall zu starten.	26. April 2021
Incident Manager hat damit begonnen, Änderungen nachzuverfolgen	Incident Manager begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	26. April 2021

Problembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Incident Manager und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Incident Manager durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines Amazon Web Services Services-Kontos den Zugriff auf meine Incident Manager-Ressourcen ermöglichen

Ich bin nicht autorisiert, eine Aktion in Incident Manager durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `ssm-incidents:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `ssm-incidents:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Incident Manager übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Incident Manager auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines Amazon Web Services Services-Kontos den Zugriff auf meine Incident Manager-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Incident Manager diese Funktionen unterstützt, finden Sie unterWie AWS Systems Manager Incident Manager funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in IAM.

Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen in Incident Manager

Mit der Kontaktfreigabe können Sie als Kontaktinhaber Kontaktinformationen, Eskalationspläne und Interaktionen mit anderen Personen AWS-Konten oder innerhalb einer AWS Organisation teilen. Sie können Kontakte und Eskalationspläne zentral erstellen und verwalten und so sicherstellen, dass andere während eines Vorfalls die richtigen Ansprechpartner kontaktieren können.

Durch die gemeinsame Nutzung von Reaktionsplänen können Sie als Verantwortlicher für den Reaktionsplan einen Reaktionsplan und die damit verbundenen Vorfälle mit anderen AWS-Konten

oder innerhalb einer AWS Organisation teilen. Sie können Reaktionspläne zentral erstellen und verwalten, sodass Einsatzkräfte in Kundenkonten auf Vorfälle reagieren können, sobald sie auftreten.

Ein Kontakt- oder Reaktionsplaninhaber kann Kontakte und Reaktionspläne mit folgenden Personen teilen:

- AWS-Konten Spezifisch innerhalb oder außerhalb seiner Organisation in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations
- Ihre gesamte Organisation ist in AWS Organizations

Inhalt

Voraussetzungen für den Austausch von Kontakten und Reaktionsplänen

So teilen Sie einen Kontakt- oder Antwortplan mit Ihrer Organisation oder Organisationseinheit in AWS Organizations:

- Sie müssen die Ressource in Ihrem besitzen AWS-Konto. Sie können keinen Kontakt- oder Antwortplan teilen, der mit Ihnen geteilt wurde.
- Sie müssen das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM -Benutzerhandbuch.

Zugehörige Services

Die gemeinsame Nutzung von Kontakt- und Reaktionsplänen ist in AWS Resource Access Manager (AWS RAM) integriert. Mit AWS RAM können Sie Ihre AWS Ressourcen mit anderen

teilen AWS-Konto oder über AWS Organizations. Sie können Ressourcen, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Bei Verbrauchern kann es sich um einzelne Personen AWS-Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Einen Kontakt- oder Reaktionsplan teilen

Nachdem Sie einen Reaktionsplan geteilt haben, haben die Verbraucher Zugriff auf alle vergangenen, aktuellen und future Vorfälle, die mit diesem Reaktionsplan erstellt wurden.

Nachdem Sie einen Kontakt geteilt haben, haben die Verbraucher Zugriff auf die Kontaktinformationen, den Interaktionsplan, die Eskalationspläne und die Interaktionen, die während eines Vorfalls auftreten. Verbraucher können während eines Vorfalls auch einen Kontakt- oder Eskalationsplan in Anspruch nehmen.

Wenn Sie Teil einer Organisation sind AWS Organizations und das Teilen innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf den gemeinsamen Kontakt- oder Antwortplan. Andernfalls erhalten Verbraucher eine Einladung zur Teilnahme an Resource Share und erhalten Zugriff auf den gemeinsamen Kontakt- oder Antwortplan, nachdem sie die Einladung angenommen haben.

Sie können einen Kontakt- oder Antwortplan, den Sie besitzen, mit anderen teilen, indem Sie die AWS RAM Konsole oder die verwenden AWS CLI.

Um einen Kontakt- oder Antwortplan, den Sie besitzen, mithilfe der AWS RAM Konsole zu teilen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um einen Kontakt- oder Antwortplan, den Sie besitzen, mit der AWS CLI

Verwenden Sie den Befehl create-resource-share.

Beenden Sie das Teilen eines geteilten Kontakt- oder Antwortplans

Wenn ein Ressourcenbesitzer aufhört, einen Kontakt- oder Reaktionsplan mit einem Verbraucher zu teilen, werden die Kontakte, Reaktionspläne, Eskalationspläne, Interaktionen und Vorfälle nicht mehr in der Konsole des Verbrauchers angezeigt.

> **Note**
>
> Der Kunde sieht die Kontakte, Reaktionspläne, Eskalationspläne, Interaktionen oder Vorfälle weiterhin ohne Aktualisierung, wenn er sie in der Konsole aufruft, bis er die Seite aktualisiert oder die Seite verlässt.

Wenn Sie einen geteilten Kontakt- oder Reaktionsplan, dessen Eigentümer Sie sind, nicht mehr teilen möchten, müssen Sie ihn aus der Ressourcenfreigabe entfernen. Sie können dies mit der AWS RAM Konsole oder dem tun AWS CLI.

So beenden Sie die Weitergabe eines geteilten Kontakt- oder Antwortplans, dessen Eigentümer Sie sind, mithilfe der AWS RAM Konsole

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

So beenden Sie die gemeinsame Nutzung eines geteilten Kontakt- oder Antwortplans, dessen Eigentümer Sie sind, indem Sie AWS CLI

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren eines gemeinsam genutzten Kontakt- oder Antwortplans

Eigentümer und Verbraucher können gemeinsam genutzte Kontakte und Reaktionspläne mithilfe der Incident Manager-Konsole und identifizieren AWS CLI.

Um mithilfe der Incident Manager-Konsole einen gemeinsamen Kontakt oder einen gemeinsamen Reaktionsplan zu identifizieren

> **Note**
>
> Kontakte, Reaktionspläne, Eskalationspläne, Engagements und Vorfälle lassen sich in der Incident Manager-Konsole im Allgemeinen nicht als gemeinsam genutzte Ressource identifizieren. An Stellen, an denen der Amazon-Ressourcenname (ARN) sichtbar ist, enthält der ARN die Konto-ID des Besitzers.

Um einen gemeinsamen Kontakt oder einen gemeinsamen Antwortplan zu identifizieren, verwenden Sie AWS CLI

Verwenden Sie die ListResponsePläne oder ListContactsBefehle. Der Befehl gibt die Kontakte und Reaktionspläne zurück, die Ihnen gehören, sowie die Kontakte und Reaktionspläne, die mit Ihnen geteilt wurden. Die ARN zeigt die AWS-Konto ID des Kontakts- oder Antwortplanbesitzers.

Geteilte Kontakt- und Antwortplanberechtigungen

Berechtigungen für Besitzer

Inhaber können Kontakte und Antwortpläne aktualisieren, ansehen, teilen, das Teilen beenden und verwenden. Kontakte und Reaktionspläne beinhalten damit verbundene Interaktionen und Vorfälle.

Berechtigungen für Konsumenten

Verbraucher können nur Reaktionspläne und Kontakte verwenden und einsehen. Kontakte und Reaktionspläne beinhalten entsprechende Einsätze und Vorfälle.

Fakturierung und Messung

Dem Besitzer der Ressource wird die Ressource in Rechnung gestellt. Den Verbrauchern werden Ressourcen, die sie gemeinsam nutzen, nicht in Rechnung gestellt. Mit der gemeinsamen Nutzung einer Ressource sind keine zusätzlichen Kosten verbunden.

Instance-Limits

Die gemeinsame Nutzung einer Ressource hat keinen Einfluss auf die Limits der Ressource im Konto des Eigentümers oder Verbrauchers. Nur das Konto des Besitzers wird verwendet, um die Limits der Ressource zu berechnen.

Überprüfung der Einhaltung der Vorschriften für AWS Systems Manager Incident Manager

Externe Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften im AWS Systems Manager Incident Manager Rahmen mehrerer AWS Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services

unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu

überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.

- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Systems Manager Incident Manager

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Incident Manager ist ein globaler und regionaler Service und unterstützt derzeit keine Availability Zones.

Zusätzlich zur AWS globalen Infrastruktur bietet Incident Manager mehrere Funktionen, die Sie bei der Erfüllung Ihrer Datenausfallsicherheit und Ihrer Backup-Anforderungen unterstützen. Im Assistenten zur Vorbereitung werden Sie aufgefordert, einen Replikationssatz einzurichten. Dieser regionale Replikationssatz stellt sicher, dass auf Ihre Daten und Ressourcen von mehreren Regionen aus zugegriffen werden kann, wodurch das Incident-Management in einem Cloud-Netzwerk einfacher verwaltet werden kann. Diese Replikation stellt außerdem sicher, dass Ihre Daten sicher und zugänglich sind, falls eine Ihrer Regionen ausfällt.

Weitere Informationen zur Verwendung des Incident Manager-Replikationssatzes finden Sie unterVerwenden Sie den Incident Manager-Replikationssatz.

Sicherheit der Infrastruktur in AWS Systems Manager Incident Manager

Als verwalteter Dienst AWS Systems Manager Incident Manager ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Incident Manager zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Arbeiten mit VPC-Endpunkten AWS Systems Manager Incident Manager und Schnittstellen ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC herstellen und AWS Systems Manager Incident Manager einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von unterstütz AWS PrivateLink. Mit AWS PrivateLink können Sie privat auf Incident Manager-API-Operationen zugreifen, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Incident Manager-API-Vorgängen zu kommunizieren. Der Verkehr zwischen Ihrer VPC und dem Incident Manager verbleibt im Amazon-Netzwerk.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter Interface VPC Endpoints (AWS PrivateLink) im Amazon VPC-Benutzerhandbuch.

Überlegungen zu Incident Manager-VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Incident Manager einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen und AWS PrivateLink Kontingente der Schnittstellen-Endpunkte im Amazon VPC-Benutzerhandbuch lesen.

Incident Manager unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus. Um Incident Manager vollständig verwenden zu können, müssen Sie zwei VPC-Endpunkte erstellen: einen für `ssm-incidents` und einen für. `ssm-contacts`

Erstellen eines VPC-Schnittstellen-Endpunkts für Incident Manager

Sie können einen VPC-Endpunkt für Incident Manager entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für Incident Manager mit den folgenden Dienstnamen:

- `com.amazonaws.`*`region`*`.ssm-incidents`
- `com.amazonaws.`*`region`*`.ssm-contacts`

Wenn Sie privates DNS für den Endpunkt verwenden, können Sie API-Anfragen an Incident Manager stellen, indem Sie dessen Standard-DNS-Namen für die Region verwenden. Sie können beispielsweise die Namen `ssm-incidents.us-east-1.amazonaws.com` oder verwendenssm-contacts.us-east-1.amazonaws.com.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für Incident Manager

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Incident Manager steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.

- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen diese Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für Incident Manager-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Incident Manager. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Principals auf allen Ressourcen Zugriff auf die aufgelisteten Incident Manager-Aktionen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Konfiguration und Schwachstellenanalyse in Incident Manager

Konfiguration und IT-Kontrollen fallen in die gemeinsame AWS Verantwortung von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Bewährte Sicherheitsmethoden in AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager bietet viele Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden stellen allgemeine Richtlinien und keine vollständige

Sicherheitslösung dar. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Themen

Bewährte Methoden zur präventiven Sicherheit für Incident Manager

Implementieren des Zugriffs mit geringsten Berechtigungen

Bei der Erteilung von Berechtigungen entscheiden Sie, wer welche Berechtigungen für welche Incident Manager-Ressourcen erhält. Sie aktivieren die spezifischen Aktionen, die daraufhin für die betreffenden Ressourcen erlaubt sein sollen. Erteilen Sie daher nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Die Implementierung der geringstmöglichen Zugriffsrechte ist eine grundlegende Voraussetzung zum Reduzieren des Sicherheitsrisikos und der Auswirkungen, die aufgrund von Fehlern oder böswilligen Absichten entstehen könnten.

Die folgenden Tools stehen zur Implementierung der geringstmöglichen Zugriffsrechte zur Verfügung:

- Steuern des Zugriffs auf AWS Ressourcen mithilfe von Richtlinien und Berechtigungsgrenzen für IAM-Entitäten
- Service-Kontrollrichtlinien

Kontakte erstellen und verwalten

Bei der Aktivierung von Kontakten kontaktiert Incident Manager das Gerät, um die Aktivierung zu bestätigen. Stellen Sie sicher, dass die Geräteinformationen korrekt sind, bevor Sie das Gerät aktivieren. Dadurch wird die Wahrscheinlichkeit verringert, dass Incident Manager während der Aktivierung das falsche Gerät oder die falsche Person kontaktiert.

Überprüfen Sie regelmäßig Ihre Kontakte und Eskalationspläne, um sicherzustellen, dass nur Kontakte kontaktiert werden, die während eines Vorfalls kontaktiert werden müssen. Überprüfen Sie die Kontakte regelmäßig, um veraltete oder falsche Informationen zu entfernen. Wenn ein Kontakt nicht mehr informiert werden soll, wenn ein Vorfall eintritt, entfernen Sie ihn aus den entsprechenden Eskalationsplänen oder entfernen Sie ihn aus dem Incident Manager.

Machen Sie Chat-Kanäle privat

Sie können Ihre Chat-Kanäle für Vorfälle privat machen, um den Zugriff mit den geringsten Rechten zu implementieren. Erwägen Sie, für jede Vorlage für den Reaktionsplan einen anderen Chat-Kanal mit einer eingeschränkten Benutzerliste zu verwenden. Dadurch wird sichergestellt, dass nur die richtigen Antwortenden in einen Chat-Kanal geleitet werden, der möglicherweise vertrauliche Informationen enthält.

AWS Chatbot aktivierte Slack-Channels erben die Berechtigungen der IAM-Rolle, die für die Konfiguration verwendet wurde. AWS Chatbot Auf diese Weise können Responder in einem AWS Chatbot aktivierten Slack-Channel jede Aktion aufrufen, auf der eine Zulassungsliste steht, z. B. Incident Manager-APIs und das Abrufen von Metrikdiagrammen.

AWS Halten Sie die Tools auf dem neuesten Stand

AWS veröffentlicht regelmäßig aktualisierte Versionen von Tools und Plugins, die Sie in Ihren AWS Abläufen verwenden können. Wenn Sie diese Ressourcen auf dem neuesten Stand halten, wird sichergestellt, dass Benutzer und Instances in Ihrem Konto Zugriff auf die neuesten Funktionen und Sicherheitsfunktionen dieser Tools haben.

- AWS CLI — The AWS Command Line Interface (AWS CLI) ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Um AWS CLI zu aktualisieren, führen Sie denselben Befehl aus, mit dem Sie den AWS CLI installiert haben. Wir empfehlen, mindestens alle zwei Wochen eine geplante Aufgabe auf Ihrem lokalen Rechner zu erstellen, um den für Ihr Betriebssystem geeigneten Befehl auszuführen. Informationen zu Installationsbefehlen finden Sie unter Installation der AWS Befehlszeilenschnittstelle im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.
- AWS Tools for Windows PowerShell — Die Tools für Windows PowerShell sind eine Reihe von PowerShell Modulen, die auf den Funktionen des AWS SDK for .NET aufbauen. Mit den Tools für Windows PowerShell können Sie über die PowerShell Befehlszeile Skripts für Operationen auf Ihren AWS Ressourcen erstellen. Wenn aktualisierte Versionen der Tools für Windows veröffentlicht PowerShell werden, sollten Sie regelmäßig die Version aktualisieren, die Sie lokal ausführen. Weitere Informationen finden Sie unter Aktualisieren AWS Tools for Windows PowerShell unter Windows oder Aktualisieren von AWS Tools for Windows PowerShell unter Linux oder macOS.

Verwandter Inhalt

Bewährte Sicherheitsmethoden für Systems Manager

Bewährte Methoden zur Detektivsicherheit für Incident Manager

Identifizieren und prüfen Sie alle Ihre Incident Manager-Ressourcen

Die Identifikation Ihrer IT-Assets ist ein wichtiger Aspekt von Governance und Sicherheit. Identifizieren Sie Ihre Systems Manager Manager-Ressourcen, um deren Sicherheitslage zu beurteilen und Maßnahmen zu ergreifen, um potenzielle Schwachstellen zu beheben. Erstellen Sie Ressourcengruppen für Ihre Incident Manager-Ressourcen. Weitere Informationen finden Sie unter Was sind Ressourcengruppen? im AWS Resource Groups -Benutzerhandbuch.

Verwenden AWS CloudTrail

AWS CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Incident Manager ausgeführt wurden. Anhand der von AWS CloudTrail gesammelten Informationen können Sie die Anfrage an Incident Manager, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen finden Sie unter Protokollierung von -API-Aufrufen mitAWS CloudTrail.

Überwachen Sie die AWS Sicherheitsempfehlungen

Überprüfen Sie regelmäßig die Trusted Advisor für Sie veröffentlichten Sicherheitshinweise. AWS-Konto Sie können dies auch programmgesteuert mit describe-trusted-advisor-checks durchführen.

Überwachen Sie außerdem aktiv die primäre E-Mail-Adresse, die für jeden von Ihnen AWS-Konten registriert ist. AWS wird Sie unter Verwendung dieser E-Mail-Adresse über neu auftretende Sicherheitsprobleme kontaktieren, die Sie betreffen könnten.

AWS Betriebsprobleme mit weitreichenden Auswirkungen werden im AWS Service Health Dashboard veröffentlicht. Operative Probleme werden über AWS Health Dashboard auch in den einzelnen Konten veröffentlicht. Weitere Informationen finden Sie in der AWS Health -Dokumentation.

Verwandter Inhalt

Amazon Web Services: Übersicht über Sicherheitsverfahren (Whitepaper)

Erste Schritte: Halten Sie sich bei der Konfiguration Ihrer AWS Ressourcen an bewährte Sicherheitsmethoden (AWS Sicherheitsblog)

IAM Best Practices

Bewährte Sicherheitsmethoden in AWS CloudTrail

Protokollierung und Überwachung im Incident Manager

AWSSystems Manager Incident Manager lässt sich in die folgenden Dienste integrieren, die Überwachungs- und Protokollierungsfunktionen bieten:

CloudWatch -Metriken

BenutzenCloudWatchMetriken zum Abrufen von Statistiken über Datenpunkte für IhreAWSSystems Manager Incident Manager arbeitet als geordneter Satz von Zeitreihendaten, bekannt alsMetriken. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken im Incident Manager.

CloudTrail Protokolle

BenutzenAWS CloudTrailum detaillierte Informationen über die Anrufe zu erfassenAWSAPIs. Sie können diese Aufrufe als Protokolldateien in Amazon Simple Storage Service speichern. Sie können diese verwendenCloudTrailprotokolliert, um Informationen wie den getätigten Anruf, die Quell-IP-Adresse, von der der Anruf kam, wer den Anruf getätigt hat und wann der Anruf getätigt wurde, zu ermitteln. DerCloudTrailLogs enthalten Informationen über die Aufrufe von API-Aktionen für Incident Manager. lWeitere Informationen finden Sie unterProtokollierung von -API-Aufrufen mitAWS CloudTrail.

Trusted Advisor

AWS Trusted Advisor kann Ihnen helfen, Ihre AWS Ressourcen zu überwachen, um Leistung, Zuverlässigkeit, Sicherheit und Kosteneffektivität zu verbessern. Vier Trusted Advisor-Prüfungen stehen allen Benutzern zur Verfügung; mehr als 50 Überprüfungen stehen Benutzern mit einem Business- oder Enterprise-Supportplan zur Verfügung. Für Incident ManagerTrusted Advisorprüft, ob die Konfiguration eines Replikationssatzes mehr als einen verwendetAWS-Regionum regionale Ausfallsicherheit und Reaktion zu unterstützen. Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

CloudWatch Amazon-Metriken im Incident Manager

Incident Manager bietet aggregierte Kennzahlen, die Sie in Amazon überwachen können CloudWatch. Sie können diese Metriken verwenden, um Trends bei Vorfällen und Reaktionsplänen zu identifizieren.

Zu diesen Metriken gehören:

- Anzahl der Incidents, die in einem bestimmten Zeitraum entstanden sind
- Die Zeit, um auf diese Vorfälle zu reagieren und sie zu lösen
- Anzahl der gelösten Vorfälle

Sie können die Kennzahlen von Incident Manager überwachen, um Ihren Betriebsstatus besser zu verstehen, und sinnvolle Maßnahmen ergreifen, um die betriebliche Exzellenz Ihrer Incident-Reaktion zu steigern. Incident Manager-Metriken sind in allen Incident Manager-Regionen verfügbar. Ihre Metriken können in Amazon CloudWatch für alle Regionen eingesehen werden, die Sie beim Onboarding in Incident Manager in Ihrem Replikationssatz angegeben haben. Sie können die veröffentlichten Kennzahlen in der Region einsehen, in der Maßnahmen für den Vorfall ergriffen wurden. Für diese Kennzahlen fallen keine zusätzlichen Gebühren an.

Auf der CloudWatch Konsole können Sie Dashboards mit diesen Metriken erstellen, um:

- Messen und überprüfen Sie Ihre aktuelle Anzahl an Vorfällen
- Verfolgen Sie, ob Ihre Ereignislast zunimmt, abnimmt oder gleich bleibt
- Nutzen Sie Incident Manager effektiver, um die Häufigkeit, Dauer und Auswirkungen Ihrer Vorfälle zu reduzieren

Auf dieser Seite werden die auf der CloudWatch Konsole verfügbaren Incident Manager-Metriken beschrieben.

> **Important**
>
> Wenn bei einem vom Kunden generierten Ereignis der Quellwert in mit Nicht-ASCII-Zeichen benannt `TriggerDetails` ist, werden die Metriken für das Ereignis nicht in CloudWatch Amazon-Metriken gemeldet, das keinen Nicht-ASCII-Text unterstützt. `source`kann nur programmatisch bereitgestellt werden, z. B. mithilfe eines SDK oder der. AWS CLI

Incident Manager sendet die folgenden Messwerte an CloudWatch.

Kennzahl	Beschreibung
`NumberOfCreateIncidents`	Anzahl der erstellten Vorfälle.

Kennzahl	Beschreibung
	Gültige Dimensionen: [] (Leere Dimension), [ResponsePlan], [Impact], [Source]ResponseP lan , [Impact], [ResponsePlan ,Source] Einheit: Anzahl
NumberOfResolveIncidents	Anzahl der gelösten Vorfälle. Gültige Dimensionen: [] (Leere Dimension), [ResponsePlan], [Impact], [Source]ResponseP lan , [Impact], [ResponsePlan ,Source] Einheit: Anzahl
TimeToFirstAcknowledgement	Zeitunterschied zwischen dem Zeitpunkt der Erstellung des Vorfalls und dem Zeitpunkt, zu dem der Vorfall zum ersten Mal bestätigt wurde. Gültige Dimensionen: [] (Leere Dimension), [ResponsePlan], [Impact], [Source], [,Impact]ResponsePlan , [ResponsePlan ,] Source Einheit: Sekunden
TimeToResolveIncident	Zeitunterschied zwischen dem Zeitpunkt, an dem der Vorfall erstellt wurde, und dem Zeitpunkt, an dem er behoben wurde. Gültige Dimensionen:] (Leere Dimension), [ResponsePlan], [Impact], [Source], [ResponsePlan ,Impact], [ResponseP lan ,Source] Einheit: Sekunden

Incident Manager-Metriken auf der CloudWatch Konsole anzeigen

Um Incident Manager-Metriken in der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den `IncidentManager`-Namespace.
4. Wählen Sie auf der Registerkarte Metriken eine Dimension und dann eine Metrik aus.

Weitere Informationen zur Arbeit mit CloudWatch Metriken finden Sie in den folgenden Themen im CloudWatch Amazon-Benutzerhandbuch:

- Metriken
- Verwenden von CloudWatch Amazon-Metriken

Dimensionen für Metriken

Incident Manager-Metriken verwenden den `IncidentManager` Namespace und stellen Metriken für die folgenden Dimensionen bereit:

Dimension	Beschreibung
`By Response Plan`	Zeigen Sie aggregierte Kennzahlen nach Reaktionsplan an.
`By Impact Level`	Zeigen Sie aggregierte Kennzahlen nach Schweregrad an.
`By Source`	Sehen Sie sich Metriken für manuell, nach CloudWatch Alarm oder EventBridge Ereignis erstellte Vorfälle an.
`Across All Incidents`	Zeigen Sie aggregierte Metriken für alle Vorfälle in der aktuellen AWS Region an.
`Response Plan name and Source`	Zeigen Sie aggregierte Kennzahlen für jede Kombination aus Reaktionsplan und Quelle an.

Dimension	Beschreibung
`Response Plan Name and Impact Level`	Zeigen Sie aggregierte Kennzahlen für jede Kombination aus Reaktionsplan und Schweregrad an.

Protokollierung von -API-Aufrufen mitAWS CloudTrail

AWS Systems Manager Incident Managerist in integriertAWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einemAWS -Service durchgeführten Aktionen in Incident-Manager bereitstellt. CloudTrail erfasst alle API-Aufrufe für Inci-Manager als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe über die -Inci-Manager-Konsole und Codeaufrufe der -Inci-Manager-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignisse für Incident-Manager aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an Inci-Manager gesendete Anforderung, die IP-Adresse, von der die Anforderung stammt, den Initiator der Anforderung, den Zeitpunkt der Anforderung und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

Informationen zum Incident Manager in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Die in Inci-Manager auftretenden Aktivitäten werden als CloudTrail Ereignis zusammen mit anderenAWS -Service-Ereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in IhremAWS-Konto, darunter Ereignisse für Inci-Manager, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von -Protokolldateien in einem Amazon-S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andereAWS -Services konfigurieren, um die in den CloudTrail -

Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail -Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail -Protokolldateien aus mehreren Konten

CloudTrail protokolliert alle Incident Manager-Aktionen und Incident Manager dokumentiert alle Aktionen in der AWS Systems Manager Incident ManagerAPI-Referenz. Beispielsweise generieren Aufrufe der`StartIncident` Aktionen`CreateResponsePlan`, `ActivateDevice`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen von ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter -Element derCloudTrail Benutzeridentität.

Grundlegendes zu -Protokolldateieinträge

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail -Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`StartIncident` Aktion demonstriert.

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2021-04-22T23:20:10Z",
    "eventSource": "gamma-ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-west-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"
}
```

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`DeleteContactChannel` Aktion demonstriert.

```
    {
    "eventVersion":"1.08",
    "userIdentity":{
        "type":"IAMUser",
        "principalId":"1234567890abcdef0",
        "arn":"arn:aws:iam::246873129580111122223333:user/nikki_wolf",
```

```
        "accountId":"abcdef01234567890",
        "accessKeyId":"021345abcdef6789",
        "userName":"nikki_wolf"
    },
    "eventTime":"2021-04-08T02:27:21Z",
    "eventSource":"ssm-contacts.amazonaws.com",
    "eventName":"DeleteContactChannel",
    "awsRegion":"us-east-1",
    "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"
}
```

Produkt- und Serviceintegrationen mit Incident Manager

Incident Manager, eine Funktion von AWS Systems Manager, lässt sich in die folgenden Produkte, Services und Tools integrieren.

Integration mit AWS-Services

Incident Manager lässt sich in die in der folgenden Tabelle beschriebenen Tools AWS-Services und integrieren.

AWS CDK	AWS CDK ist ein Entwicklungs-Framework zur Verwendung von Code zur Definition Ihrer Cloud-Infrastruktur und zur Verwendung von AWS CloudFormation für die Bereitstellung. unterstützt AWS CDK mehrere Programmi ersprachen, darunter TypeScript, JavaScrip tPythonJava, und C#/.Netz. Informationen zur Verwendung von AWS CDK mit Incident Manager finden Sie in den folgenden Abschnitten in der APIAWS CDK - Referenz zu : • @aws-cdk/aws-ssmincidents -Modul • @aws-cdk/aws-ssmcontacts -Modul
AWS Chatbot	AWS Chatbot ermöglicht DevOps es und Softwareentwicklungsteams, Chatrooms für Messaging-Programme zu verwenden, um Betriebsereignisse in ihrem zu überwachen und darauf zu reagieren AWS Cloud. Mit AWS Chatbot Incident Manager können Sie Chat-Kanäle erstellen, mit denen Antworter Vorfälle überwachen und darauf reagieren können. AWS Chatbot unterstützt Slack

	Chatrooms, Microsoft Teams Kanäle und Amazon-Chime-Chatrooms als Chat-Kanäle. Als Teil der Erstellung eines Chat-Kanals erstellen Sie auch ein Thema in Amazon Simple Notification Service (Amazon SNS). Amazon SNS ist ein verwalteter Service, der die Nachrichtenzustellung von Publishern an Abonnenten bereitstellt. Wenn Sie in Plänen zur Reaktion auf Vorfälle einen Chat-Kanal zuordnen, den Sie mit dem Plan erstellt haben, wählen Sie auch ein oder mehrere Themen aus, die Sie dem Chat-Kanal zugeordnet haben. Diese SNS-Themen werden verwendet , um Benachrichtigungen über einen Vorfall an die Vorfallshelfer zu senden. Weitere Informationen finden Sie unter Arbeiten mit Chat-Kanälen in Incident Manager.
AWS CloudFormation	AWS CloudFormation ist ein Service, mit dem Sie eine Vorlage mit allen Ressourcen erstellen können, die Sie für Ihre Anwendung benötigen, und dann die Ressourcen für Sie konfigurieren und bereitstellen können. Außerdem werden alle Abhängigkeiten konfiguriert, sodass Sie sich mehr auf Ihre Anwendung und weniger auf die Verwaltung von -Ressourcen konzentrieren können. Informationen zur Verwendung von AWS CloudFormation mit Incident Manager finden Sie in den folgenden Themen im AWS CloudFormation -Benutzerhandbuch: • Ressourcentypreferenz für Incident Manager • Ressourcentypreferenz für Kontakte Ressourcentypreferenz

Amazon CloudWatch	CloudWatch überwacht Ihre - AWS Ressourcen und die Anwendungen, auf denen Sie ausgeführt werden, AWS in Echtzeit. Sie können verwenden, CloudWatch um Metriken zu erfassen und zu verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können. Sie können CloudWatch Alarme konfigurieren, um Vorfälle in Incident Manager. CloudWatch works mit Systems Manager und Incident Manager zu erstellen, um einen Vorfall aus einer Reaktionsplanvorlage zu erstellen, wenn ein Alarm in den Alarmzustand wechselt. Weitere Informationen finden Sie unter Automatisches Erstellen von Vorfällen mit CloudWatch Alarmen.
Amazon Chime	Amazon Chime ist ein Online-Standort, der Meetings, Chat und Geschäftsanrufe kombiniert. Mit Amazon Chime können Sie Geschäftsanrufe innerhalb und außerhalb Ihrer Organisation tätigen. Sie können einen Amazon-Chime-Raum in Ihre Incident-Manager-Operationen integrieren enAWS Chatbot, indem Sie einen Chat-Kanal für Amazon Chime in erstellen und diesen Kanal dann einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Chat-Kanälen in Incident Manager.

Amazon EventBridge	EventBridge ist ein Serverless-Service, der Ereignisse verwendet, um Anwendungskomponenten zu verbinden, sodass Sie einfacher skalierbare ereignisgesteuerte Anwendungen erstellen können. Sie können EventBridge Regeln konfigurieren, um auf Ereignismuster in Ihren AWS Ressourcen zu achten und einen Vorfall in Incident Manager zu erstellen, wenn ein Ereignis einem von Ihnen definierten Muster entspricht. Ihre Regeln können Ereignisse in Dutzenden von Anwendungen AWS-Services und Services von und Drittanbietern überwachen. Weitere Informationen finden Sie unter Automatisches Erstellen von Vorfällen mit EventBridge Ereignissen.
AWS Secrets Manager	Secrets Manager hilft Ihnen, Datenbankanmeldeinformationen, Anwendungsanmeldeinformationen, OAuth-Token, API-Schlüssel und andere Secrets während ihres gesamten Lebenszyklus zu verwalten, abzurufen und zu rotieren. Wenn Sie Incident Manager in den PagerDuty Service integrieren, erstellen Sie ein Secret in Secrets Manager, das Ihre PagerDuty Anmeldeinformationen enthält. Weitere Informationen finden Sie unter Speichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret.

AWS Systems Manager	Systems Manager ist ein Betriebs-Hub, mit dem Sie Ihre Anwendungsinfrastruktur anzeigen und steuern können, und eine sichere end-to-end Verwaltungslösung für Cloud-Umgebungen. Die folgenden Systems Manager-Funktionen lassen sich direkt in Incident Manager integrieren: • Automatisierung – Ein Automation-Runbook definiert die Aktionen, die Systems Manager für Ihre AWS Ressourcen durchführt. In Incident Manager definiert ein Runbook eine Reihe automatisierter und manueller Schritte zur Behebung Ihrer Vorfälle. Informationen zum Erstellen von Automatio n-Runbooks zur Verwendung mit Incident Manager finden Sie unter Arbeiten mit Systems Manager Automation-Runbooks in Incident Manager. • OpsCenter – OpsCenter bietet einen zentralen Ort, an dem Betriebstechniker und IT-Experten operative Arbeitselemente, genannt OpsItems, im Zusammenhang mit - AWS Ressourcen verwalten können. Sie können direkt aus einer Analyse nach einem Vorfall erstellen OpsItems, um verwandte Arbeiten zu verfolgen. Weitere Informationen finden Sie unter Durchführung einer Analyse nach einem Vorfall im Incident-Manager.

AWS Trusted Advisor	Trusted Advisor ist ein Tool, das AWS Kunden mit einem Basic- oder Developer-Supportp lan zur Verfügung steht. Trusted Advisor überprüft Ihre - AWS Umgebung und gibt dann Empfehlungen, wenn sich Möglichke iten ergeben, Geld zu sparen, die Systemver fügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Trusted Advisor Überprüft für Incident Manager, ob die Konfiguration eines Replikationssatzes mehr als eine verwendet, AWS-Region um regionales Failover und regionale Antworten zu unterstützen.

Integration in andere Produkte und Services

Sie können Incident Manager in die in der folgenden Tabelle beschriebenen Drittanbieterservices integrieren oder verwenden.

Jira Cloud	Mithilfe der können AWS Service Managemen t ConnectorSie Incident Manager in Jura Cloud (Atlassian), eine cloudbasierte Workflow-Plattform von Drittanbietern, integrieren. Nachdem Sie die Integration mit Jura Cloud konfiguriert haben und wenn Sie einen neuen Vorfall in Incident Manager erstellen, erstellt die Integration auch den Vorfall in Jura Cloud. Wenn Sie einen Vorfall in Incident Manager aktualisieren, werden diese Aktualisierungen für den entsprechenden Vorfall in Jura Cloud vorgenommen. Wenn Sie einen Vorfall entweder im Incident Manager oder in der Jura Cloud beheben, löst die Integration den Vorfall

	in beiden Services basierend auf den von Ihnen konfigurierten Einstellungen auf. Weitere Informationen finden Sie unter Integration von AWS Systems Manager Incident Manager (Jura Cloud) im AWS Service Management Connector Administratorhandbuch für .
Verwaltung des Jura-Service	Mit der können AWS Service Management ConnectorSie Incident Manager in Jura Service Management integrieren, eine cloudbasierte Workflow-Plattform eines Drittanbieters. Wenn Sie nach der Konfiguration der Integration mit Jura Service Management einen neuen Vorfall in Incident Manager erstellen, erstellt die Integration auch den Vorfall in Jura Service Management. Wenn Sie einen Vorfall in Incident Manager aktualisieren, werden diese Aktualisierungen für den entsprechenden Vorfall in Jura Service Management vorgenommen. Wenn Sie einen Vorfall entweder in Incident Manager oder Jura Service Management beheben, löst die Integration den Vorfall in beiden Services basierend auf den von Ihnen konfigurierten Einstellungen. Weitere Informationen finden Sie unter Konfigurieren der Jura-Serviceverwaltung im AWS Service Management Connector Administratorhandbuch für .

Microsoft Teams	Microsoft Teams bietet kollaborative Cloud-basierte Tools für Team-Messaging, Audio- und Videokonferenzen sowie Dateifreigabe. Sie können einen Microsoft Teams Kanal in Ihre Incident Manager-Operationen integrieren mitAWS Chatbot, indem Sie einen Chat-Kanal für Microsoft Team in erstellen und diesen Kanal dann einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Chat-Kanälen in Incident Manager.

PagerDuty	PagerDuty ist ein Tool zur Reaktion auf Vorfälle, das Auslagerungsworkflows und Eskalatio nsrichtlinien unterstützt. Wenn Sie Incident Manager in integrieren PagerDuty, können Sie Ihrem Reaktionsplan einen PagerDuty Service hinzufügen. Danach wird ein entsprechender Vorfall in erstellt, PagerDuty wenn ein Vorfall in Incident Manager erstellt wird. Der Vorfall in PagerDuty verwendet den Auslagerungs-Workflow und die Eskalatio nsrichtlinien, die Sie dort zusätzlich zu den in Incident Manager definierten Richtlinien definiert haben. PagerDuty fügt Zeitachsenereignisse aus Incident Manager als Hinweise zu Ihrem Vorfall hinzu. Um Incident Manager in zu integrieren PagerDuty, müssen Sie zunächst ein Secret in AWS Secrets Manager erstellen, das Ihre PagerDuty Anmeldeinformationen enthält. Informationen zum Hinzufügen eines PagerDuty REST-API-Schlüssels und anderer erforderl icher Details zu einem Secret in finden Sie AWS Secrets Managerunter Speichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret. Informationen zum Hinzufügen eines PagerDuty Services aus Ihrem PagerDuty Konto zu einem Reaktionsplan in Incident Manager finden Sie in den Schritten unter Integrieren eines PagerDuty Services in den Reaktionsplan im Thema Erstellung eines Reaktionsplans.

ServiceNow	Mit der können AWS Service Management ConnectorSie Incident Manager in integrier enServiceNow, eine cloudbasierte Workflow-Plattform eines Drittanbieters. Nachdem Sie die Integration mit konfiguriert haben ServiceNow, erstellt die Integration beim Erstellen eines neuen Vorfalls in Incident Manager ServiceNow auch den Vorfall in . Wenn Sie einen Vorfall in Incident Manager aktualisieren, werden diese Aktualisierungen für den entsprechenden Vorfall in vorgenommen ServiceNow. Wenn Sie einen Vorfall entweder in Incident Manager oder beheben ServiceNo w, löst die Integration den Vorfall in beiden Services basierend auf den von Ihnen konfiguri erten Einstellungen. Weitere Informationen finden Sie unter Integrati on AWS Systems Manager Incident Manager in ServiceNow im AWS Service Management Connector Administratorhandbuch für .
Slack	Slack bietet kollaborative Cloud-basierte Tools für Team-Messaging, Audio- und Videokonf erenzen sowie Dateifreigabe. Sie können einen Slack Kanal in Ihre Incident Manager-Operationen integrierenAWS Chatbot, indem Sie einen Chat-Kanal für Slack in erstellen und diesen Kanal dann einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Chat-Kanälen in Incident Manager.

Terraform	HashiCorp Terraform ist ein Open-Source-Softwaretool für Infrastructure as Code (IaC), das einen Befehlszeilenschnittstellen-Workflow (CLI) zur Verwaltung verschiedener Cloud-Services bietet. Für Incident Manager können Sie Terraform verwenden, um Folgendes zu verwalten oder bereitzustellen: SSM Incident Manager Contacts-Ressourcen • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmKontakte_Rotation Datenquellen für SSM Contacts • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmKontakte_Rotation SSM Incident Manager-Ressourcen • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Datenquellen von SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Speichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret

Nachdem Sie die Integration mit PagerDuty für einen Reaktionsplan aktiviert haben, arbeitet Incident Manager wie folgt mit PagerDuty zusammen:

- Incident Manager erstellt einen entsprechenden Vorfall in PagerDuty , wenn Sie einen neuen Vorfall in Incident Manager erstellen.
- Der Auslagerungs-Workflow und die Eskalationsrichtlinien, die Sie in erstellt haben, PagerDuty werden in der PagerDuty Umgebung verwendet. Incident Manager importiert Ihre PagerDuty Konfiguration jedoch nicht.
- Incident Manager veröffentlicht Zeitachsenereignisse als Hinweise auf den Vorfall in PagerDutybis zu maximal 2 000 Notizen.
- Sie können wählen, ob Sie PagerDuty Vorfälle automatisch lösen möchten, wenn Sie den zugehörigen Vorfall in Incident Manager beheben.

Um Incident Manager in zu integrieren PagerDuty, müssen Sie zunächst ein Secret in erstellen AWS Secrets Manager , das Ihre PagerDuty Anmeldeinformationen enthält. Dadurch kann Incident Manager mit Ihrem PagerDuty Service kommunizieren. Anschließend können Sie einen PagerDuty Service in Reaktionspläne aufnehmen, die Sie in Incident Manager erstellen.

Dieses Secret, das Sie in Secrets Manager erstellen, muss im korrekten JSON-Format Folgendes enthalten:

- Ein API-Schlüssel aus Ihrem PagerDuty Konto. Sie können entweder einen REST-API-Schlüssel für allgemeinen Zugriff oder einen REST-API-Schlüssel für Benutzer-Token verwenden.
- Eine gültige Benutzer-E-Mail-Adresse aus Ihrer PagerDuty Subdomäne.
- Die PagerDuty Serviceregion, in der Sie Ihre Subdomäne bereitgestellt haben.

> **Note**
>
> Alle Services in einer PagerDuty Subdomäne werden in derselben Serviceregion bereitgestellt.

Voraussetzungen

Bevor Sie das Secret in Secrets Manager erstellen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen.

KMS-Schlüssel

Sie müssen das von Ihnen erstellte Secret mit einem vom Kunden verwalteten Schlüssel verschlüsseln, den Sie in AWS Key Management Service () erstellt habenAWS KMS. Sie geben diesen Schlüssel an, wenn Sie das Secret erstellen, das Ihre PagerDuty Anmeldeinformationen speichert.

> **Important**
>
> Secrets Manager bietet die Möglichkeit, das Secret mit einem zu verschlüsseln Von AWS verwalteter Schlüssel, aber dieser Verschlüsselungsmodus wird nicht unterstützt.

Der vom Kunden verwaltete Schlüssel muss die folgenden Anforderungen erfüllen:

- Schlüsseltyp : Wählen Sie Symmetrisch aus.
- Schlüsselnutzung: Wählen Sie Verschlüsseln und Entschlüsseln aus.
- Regionalität: Wenn Sie Ihren Reaktionsplan auf mehrere replizieren möchten AWS-Regionen, stellen Sie sicher, dass Sie den multiregionalen Schlüssel auswählen.

Schlüsselrichtlinie

Der Benutzer, der den Reaktionsplan konfiguriert, muss über die Berechtigung für `kms:GenerateDataKey` und `kms:Decrypt` in der ressourcenbasierten Richtlinie des Schlüssels verfügen. Der `ssm-incidents.amazonaws.com` Service-Prinzipal muss über die Berechtigung für `kms:GenerateDataKey` und `kms:Decrypt` in der ressourcenbasierten Richtlinie des Schlüssels verfügen.

Die folgende Richtlinie zeigt diese Berechtigungen. Ersetzen Sie jedes *`Platzhalter für Benutzereingaben`* durch Ihre eigenen Informationen.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
```

```
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id: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": "*"
        }
    ]
}
```

Informationen zum Erstellen eines neuen kundenverwalteten Schlüssels finden Sie unter Erstellen von KMS-Schlüsseln mit symmetrischer Verschlüsselung im AWS Key Management Service - Entwicklerhandbuch. Weitere Informationen zu - AWS KMS Schlüsseln finden Sie unter AWS KMS -Konzepte.

Wenn ein vorhandener kundenverwalteter Schlüssel alle vorherigen Anforderungen erfüllt, können Sie seine Richtlinie bearbeiten, um diese Berechtigungen hinzuzufügen. Informationen zum

Aktualisieren der Richtlinie in einem vom Kunden verwalteten Schlüssel finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch für .

> **Tip**
>
> Sie können einen Bedingungsschlüssel angeben, um den Zugriff noch weiter einzuschränken. Die folgende Richtlinie erlaubt beispielsweise den Zugriff nur über Secrets Manager in der Region USA Ost (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` Berechtigung

Die IAM-Identität (Benutzer, Rolle oder Gruppe), die den Reaktionsplan erstellt, muss über die IAM-Berechtigung verfügen`secretsmanager:GetSecretValue`.

So speichern Sie PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret

1. Folgen Sie den Schritten bis Schritt 3a unter Erstellen eines - AWS Secrets Manager Secrets im AWS Secrets Manager -Benutzerhandbuch.
2. Gehen Sie für Schritt 3b für Schlüssel/Wert-Paare wie folgt vor:
   - Wählen Sie die Registerkarte Klartext aus.
   - Ersetzen Sie den Standardinhalt des Felds durch die folgende JSON-Struktur:

     ```
     {
     ```

```
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
}
```

- Ersetzen Sie im eingefügten JSON-Beispiel die *Platzhalterwerte* wie folgt:
  - *pagerduty-token*: Der Wert eines REST-API-Schlüssels für allgemeinen Zugriff oder eines REST-API-Schlüssels für Benutzer-Token aus Ihrem PagerDuty Konto.

    Weitere Informationen finden Sie unter API-Zugriffsschlüssel in der PagerDuty Wissensdatenbank .
  - *pagerduty-region*: Die Serviceregion des PagerDuty Rechenzentrums, das Ihre PagerDuty Subdomäne hostet.

    Weitere Informationen finden Sie unter Serviceregionen in der PagerDuty Wissensdatenbank .
  - *pagerduty-email*: Die gültige E-Mail-Adresse für einen Benutzer, der zu Ihrer PagerDuty Subdomäne gehört.

    Weitere Informationen finden Sie unter Benutzer verwalten in der PagerDuty Wissensdatenbank .

  Das folgende Beispiel zeigt ein abgeschlossenes JSON-Secret, das die erforderlichen PagerDuty Anmeldeinformationen enthält:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. Wählen Sie in Schritt 3c für Verschlüsselungsschlüssel einen vom Kunden verwalteten Schlüssel aus, der die im vorherigen Abschnitt Voraussetzungen aufgeführten Anforderungen erfüllt.
4. Gehen Sie in Schritt 4c für Ressourcenberechtigungen wie folgt vor:
   - Erweitern Sie Ressourcenberechtigungen .
   - Wählen Sie Berechtigungen bearbeiten aus.
   - Ersetzen Sie den Standardinhalt des Richtlinienfelds durch die folgende JSON-Struktur:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- Wählen Sie Speichern.

5. Gehen Sie in Schritt 4d für Secret replizieren wie folgt vor, wenn Sie Ihren Reaktionsplan auf mehr als ein repliziert haben AWS-Region:
   - Erweitern Sie Geheimnis replizieren.
   - Wählen Sie für die Region ausAWS-Region, in die Sie Ihren Reaktionsplan repliziert haben.
   - Wählen Sie für Verschlüsselungsschlüssel einen kundenverwalteten Schlüssel aus, den Sie in dieser Region erstellt oder repliziert haben und der die im Abschnitt Voraussetzungen aufgeführten Anforderungen erfüllt.
   - AWS-RegionWählen Sie für jede weitere Region hinzufügen und wählen Sie den Namen der Region und den vom Kunden verwalteten Schlüssel aus.
6. Führen Sie die verbleibenden Schritte unter Erstellen eines - AWS Secrets Manager Secrets im AWS Secrets Manager -Benutzerhandbuch aus.

Informationen zum Hinzufügen eines PagerDuty Services zu einem Incident Manager-Vorfall-Workflow finden Sie unter Integrieren eines PagerDuty Services in den Reaktionsplan im Thema Erstellung eines Reaktionsplans.

Ähnliche Informationen

So automatisieren Sie die Reaktion auf Vorfälle mit PagerDuty und AWS Systems Manager Incident Manager (AWS Cloud -Blog für Betrieb und Migrationen)

Secret-Verschlüsselung in AWS Secrets Manager im AWS Secrets Manager -Benutzerhandbuch

Fehlerbehebung beiAWS Systems Manager

Wenn Sie bei der Verwendung vonAWS Systems Manager Incident Manager auf Probleme stoßen, können Sie die folgenden Informationen verwenden, um diese gemäß unseren bewährten Methoden zu lösen. Wenn die Probleme, auf die Sie stoßen, nicht in den Rahmen der folgenden Informationen fallen oder wenn sie weiterhin bestehen, nachdem Sie versucht haben, sie zu lösen, wenden Sie sich an AWS Support.

Themen

Fehlermeldung:`ValidationException – We were unable to validate the AWS Secrets Manager secret`

Problem 1: DieAWS Identity and Access Management (IAM-) Identität (Benutzer, Rolle oder Gruppe), die den Antwortplan erstellt, hat keine`secretsmanager:GetSecretValue` IAM-Berechtigung. IAM-Identitäten müssen über diese Berechtigung verfügen, um Secrets Manager zu validieren.

- Lösung: Fügen Sie der IAM-Richtlinie die fehlende`secretsmanager:GetSecretValue` Berechtigung für die IAM-Identität hinzu, die den Antwortplan erstellt. Weitere Informationen finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) oder Hinzufügen von IAM-Richtlinien (AWS CLI) im IAM-Benutzerhandbuch.

Problem 2: Dem geheimen Schlüssel ist keine ressourcenbasierte Richtlinie angehängt, die es der IAM-Identität ermöglicht, die `GetSecretValue`Aktion auszuführen, oder die ressourcenbasierte Richtlinie verweigert der Identität die Erlaubnis.

- Lösung: Erstellen Sie eine Anweisung oder fügen Sie eine`Allow` Anweisung zur ressourcenbasierten Richtlinie des Geheims hinzu, die der IAM-Identität die Berechtigung erteilt.`secrets:GetSecretValue` Oder, wenn Sie eine`Deny` Anweisung verwenden, die die IAM-Identität enthält, aktualisieren Sie die Richtlinie, damit die Identität die Aktion ausführen kann. Weitere Informationen finden Sie im AWS Secrets ManagerBenutzerhandbuch unter Anhängen einer Berechtigungsrichtlinie an einAWS Secrets Manager Geheimnis.

Problem 3: Den Geheimnissen ist keine ressourcenbasierte Richtlinie beigefügt, die den Zugriff auf den Incident Manager-Serviceprinzip ermöglichtssm-incidents.amazonaws.com.

- Lösung: Erstellen oder aktualisieren Sie die ressourcenbasierte Richtlinie für das Geheimnis und fügen Sie die folgende Berechtigung hinzu:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Problem 4: Der für die Verschlüsselung des geheimen CodesAWS KMS key ausgewählte Schlüssel ist kein vom Kunden verwalteter Schlüssel, oder der vom Kunden verwaltete Schlüssel stellt die IAM-Berechtigungenkms:Decrypt und nicht für den Incident Manager-Serviceprinzipkms:GenerateDataKey* zur Verfügung. Alternativ verfügt die IAM-Identität, die den Antwortplan erstellt, möglicherweise nicht über die IAM-Berechtigung GetSecretValue.

- Lösung: Stellen Sie sicher, dass Sie die im Thema unter Voraussetzungen beschriebenen Anforderungen erfüllenSpeichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret.

Problem 5: Die ID des -Geheimnisses, das den REST-API-Schlüssel für allgemeinen Zugriff oder REST-API-Schlüssel für Benutzertoken und REST-API-Schlüssel für Benutzertoken.

- Lösung: Stellen Sie sicher, dass Sie die ID des Secrets Manager Manager-Geheimnisses korrekt und ohne Leerzeichen eingegeben haben. Sie müssen dasselbe verwendenAWS-Region, das das Geheimnis speichert, das Sie verwenden möchten. Sie können ein gelöschtes Geheimnis nicht verwenden.

Problem 6: In seltenen Fällen kann es beim Secrets Manager Manager-Dienst zu einem Problem kommen, oder Incident Manager hat möglicherweise Probleme, mit ihm zu kommunizieren.

- Lösung: Warten Sie einige Minuten und versuchen Sie dann erneut. Suchen Sie unter AWS Health Dashboardnach Problemen, die sich auf einen der beiden Dienste auswirken könnten.

Andere Probleme zur Fehlerbehebung bei der Fehlerbehebung

Wenn die vorherigen Schritte Ihr Problem nicht gelöst haben, finden Sie zusätzliche Hilfe in den folgenden Ressourcen:

- Informationen zu IAM-Problemen, die sich speziell auf Incident Manager beziehen, wenn Sie auf die Incident Manager-Konsole zugreifen, finden Sie unterProblembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff.
- Allgemeine Authentifizierungs- und Autorisierungsprobleme beim Zugriff aufAWS Management Console finden Sie im IAM-Benutzerhandbuch unter Problembehandlung bei IAM.

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Dokumentverlauf für Incident Manager

Änderung	Beschreibung	Datum
Aktualisierung auf von verwaltete Richtlinie `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Incident Manager hat zur Unterstützung der Funktion Erkenntnisse eine neue Berechtigung zu hinzugefügt `AWSIncidentManagerIncidentAccessServiceRolePolicy`, mit der überprüft werden kann, ob eine EC2-Instance Teil einer Auto Scaling-Gruppe ist. Weitere Informationen finden Sie unter Incident Manager-Updates für - AWS verwaltete Richtlinien.	20. Februar 2024
Zusätzliche HashiCorp Terraform-Unterstützung: Bereitschaftsrotationen	Terraform hat seine Unterstützung für Incident Manager erweitert. Sie können jetzt Incident Manager-Bereitschaftsressourcen mit Terraform bereitstellen oder verwalten. Informationen zu dieser und anderen Drittanbieterintegrationen mit Incident Manager finden Sie unter Integration mit anderen -Produkten und -Services.	2. Februar 2024
Neues Feature: Erkenntnisse aus anderen AWS-Services	Die Erkenntnisse liefern Ihnen Informationen zu Änderungen im Zusammenhang mit AWS CloudFormation Stacks und	15. November 2023

	AWS CodeDeploy Bereitstellungen, die ungefähr zum Zeitpunkt der Erstellung eines Vorfalls in Incident Manager aufgetreten sind. In der Incident Manager-Konsole können Sie zusammenfassende Informationen zu diesen Änderungen anzeigen und in vielen Fällen auf Links zu den - CloudFormation oder - CodeDeploy Konsolen zugreifen, um vollständige Details zu der Änderung zu erhalten. Die Erkenntnisse reduzieren den Zeitaufwand für die Bewertung potenzieller Ursachen von Vorfällen. Sie verringern auch die Wahrscheinlichkeit, dass Angreifer auf das falsche Konto oder die falsche Konsole zugreifen, um die Ursache eines Vorfalls zu untersuchen. Dieses Feature führt auch eine neue verwaltete Richtlinie ein, die es Incident Manager ermöglicht`AWSIncidentManagerIncidentAccessServiceRolePolicy` , Ressourcen in anderen zu lesen, AWS-Services um Erkenntnisse im Zusammenhang mit Vorfällen zu identifizieren. Weitere

	Informationen finden Sie unter den folgenden Themen: • Arbeiten mit Ergebnissen • AWS Von verwaltete Richtlinie: AWSIncidentManagerIncidentAccessServiceRolePolicy	
Aktualisierte Integrationslisten mit Incident Manager	Das Thema Produkt- und Serviceintegrationen mit Incident Manager wurde erweitert, um alle Tools AWS-Services und Drittanbieter aufzulisten und zu beschreiben, die Sie in Incident Manager in Ihre Vorgänge zur Erkennung und Reaktion auf Vorfälle integrieren können.	9. Juni 2023

Integration mit AWS Trusted Advisor	Trusted Advisor überprüft jetzt, ob die Konfiguration eines Replikationssatzes mehr als eine verwendet, AWS-Region um regionale s Failover und regionale Antworten zu unterstützen. Für Vorfälle, die durch CloudWatch Alarme oder EventBridge Ereignisse erstellt wurden, erstellt Incident Manager einen Vorfall in derselben AWS-Region wie der Alarm oder die Ereignisregel. Wenn Incident Manager in dieser Region vorübergehend nicht verfügbar ist, versucht das System, einen Vorfall in einer anderen Region im Replikationssatz zu erstellen . Wenn der Replikationssatz nur eine Region umfasst, kann das System keinen Vorfallsdatensatz erstellen , solange Incident Manager nicht verfügbar ist. Um diese Situation zu vermeiden, Trusted Advisor meldet , wenn ein Replikationssatz nur für eine Region konfiguriert ist. Weitere Informationen zum Arbeiten mit finden Sie Trusted Advisorunter AWS Trusted Advisor im AWS Support - Benutzerhandbuch.	28. April 2023

Microsoft Teams als Chat-Kanal in Reaktionsplänen verwenden	Durch die Integration mit Microsoft Teams und können AWS ChatbotSie jetzt Microsoft Teams für den Chat-Kanal in Ihren Antwortplänen verwenden. Dies wird zusätzlich zur Unterstützung für Slack- und Amazon-Chime-Chat-Kanäle unterstützt. Während eines Vorfalls sendet Incident Manager Statusbenachrichtigungen direkt an einen Chat-Kanal, um alle Mitarbeiter auf dem Laufenden zu halten. Responder können in der Microsoft Teams-Anwendung auch miteinander und mit vorfällenbezogenen AWS CLI Befehlen kommunizieren, um die Vorfälle zu aktualisieren und mit ihnen zu interagieren. Weitere Informationen finden Sie unter Arbeiten mit Chat-Kanälen in Incident Manager.	4. April 2023

Neues Feature: Bereitschaftspläne	Ein Bereitschaftsplan in Incident Manager definiert, wer benachrichtigt wird, wenn ein Vorfall eintritt, der ein Eingreifen des Bedieners erfordert. Ein Bereitschaftsplan besteht aus einer oder mehreren Rotationen, die Sie für den Zeitplan erstellen. Jede Rotation kann bis zu 30 Kontakte enthalten. Nachdem Sie einen Bereitschaftsplan erstellt haben, können Sie ihn als Eskalation in Ihren Eskalationsplan aufnehmen. Wenn ein Vorfall im Zusammenhang mit diesem Eskalationsplan auftritt, benachrichtigt Incident Manager den (oder die Operatoren), die gemäß dem Zeitplan aufgerufen werden. Weitere Informationen finden Sie unter Arbeiten mit Bereitschaftsplänen in Incident Manager.	28. März 2023

Drucken einer formatierten Vorfallanalyse oder Speichern als PDF	Die Seite zur Vorfallanalyse enthält jetzt eine Schaltfläche Drucken, um eine Version der Analyse zu generieren, die zum Drucken formatiert ist. Mithilfe der für Ihr Gerät konfigurierten Druckerziele können Sie die Vorfallanalyse als PDF speichern oder an einen lokalen oder Netzwerk Drucker senden. Weitere Informationen finden Sie unter Drucken einer formatierten Vorfallanalyse.	17. Januar 2023

PagerDuty -Integration: Incident Manager kopiert jetzt Vorfallzeitplanereignisse in PagerDuty Vorfälle	Wenn Sie die Integration mit PagerDuty in einem Reaktionsplan aktivieren, fügt Incident Manager Zeitachsenereignisse, die aus diesem Plan erstellt wurden, dem entsprechenden Vorfalldatensatz in hinzu PagerDuty. PagerDuty fügt Zeitachsenereignisse als Notizen zum Vorfall hinzu, bis zu maximal 2 000 Notizen. Weitere Informationen zu diesen Änderungen finden Sie in den folgenden Themen: • Speichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret • Integrieren eines PagerDuty Services in den Reaktionsplan	15. Dezember 2022
Incident Manager-Integration mit - CloudWatch Metriken.	Sie können jetzt Metriken im Zusammenhang mit Vorfällen in veröffentlichen CloudWatch. Weitere Informationen finden Sie unter -CloudWatchMetriken. Die AWSIncidentManagerServiceRolePolicy hat eine zusätzliche Berechtigung enthalten, damit unser Service Metriken in Ihrem Namen veröffentlichen kann.	15. Dezember 2022

Hinweise zu Vorfällen gestartet und Bildschirm mit den Details zu Vorfällen aktualisiert	Mithilfe von Vorfallhinweisen können Sie mit anderen Benutzern zusammenarbeiten und mit ihnen kommunizieren, die an einem Vorfall arbeiten. Darüber hinaus können Sie den Status von Runbooks und Engagements auf dem Bildschirm mit den Vorfalldetails anzeigen. Weitere Informationen finden Sie unter Details zu Vorfällen.	16. November 2022

Integrieren Sie PagerDuty Eskalationspläne und Auslagerungs-Workflows in Incident Manager-Antwortpläne	Sie können Incident Manager jetzt in integrieren PagerDuty und einem Reaktionsplan einen PagerDuty Service hinzufügen. Nachdem Sie die Integration konfiguriert haben, kann Incident Manager einen entsprechenden Vorfall in PagerDuty für jeden neuen Vorfall erstellen, der in Incident Manager erstellt wurde. PagerDuty verwendet den Paging-Workflow und die Eskalationsrichtlinien, die Sie in der PagerDuty Umgebung definieren. Weitere Informationen finden Sie unter den folgenden Themen: • Produkt- und Serviceintegrationen mit Incident Manager • Speichern von PagerDuty Anmeldeinformationen in einem - AWS Secrets Manager Secret • Integrieren eines PagerDuty Services in den Reaktionsplan im Thema Erstellung eines Reaktionsplans • Fehlersuche	16. November 2022

Hinweise zu Vorfällen gestartet und der Bildschirm mit den Details zu Vorfällen aktualisiert.	Mithilfe von Vorfallhinweisen können Sie mit anderen Benutzern zusammenarbeiten und mit ihnen kommunizieren, die an einem Vorfall arbeiten. Darüber hinaus können Sie den Status von Runbooks und Engagements auf dem Bildschirm mit den Details zu Vorfällen anzeigen. Weitere Informationen finden Sie unter Details zu Vorfällen.	16. November 2022
Tagging-Unterstützung für Replikationssätze	Sie können jetzt Ihrem Replikationssatz in Tags zuweisen AWS Systems Manager Incident Manager. Dies erhöht die bestehende Unterstützung für die Zuweisung von Tags zu Reaktionsplänen, Vorfalldatensätzen und Kontakten in den in Ihrem Replikationssatz AWS-Regionen angegebenen . Weitere Informationen finden Sie unter den folgenden Themen: • Vorbereiten des Assistenten • Markieren von Incident Manager-Ressourcen	02. November 2022

Incident Manager-Integration mit Atlassian Jura Service Management	Sie können Incident Manager mithilfe des AWS Service Management Connectors für Jura Service Management in Jura Service Management integrieren. Nachdem Sie die Integration konfiguriert haben, erstellen neue Vorfälle, die in Incident Manager erstellt wurden, einen entsprechenden Vorfall in JCCP. Wenn Sie einen Vorfall in Incident Manager aktualisieren, werden die Aktualisierungen dem entsprechenden Vorfall in Jura hinzugefügt. Wenn Sie einen Vorfall entweder in Incident Manager oder JSpeed beheben, wird der entsprechende Vorfall ebenfalls auf der Grundlage der konfigurierten Einstellungen behoben. Weitere Informationen finden Sie unter Konfigurieren von Jura Service Management im AWS Service Management Connector Administratorhandbuch.	6. Oktober 2022

Verbesserte Tagging-Unterstützung	Incident Manager unterstützt das Zuweisen von Tags zu Reaktionsplänen, Vorfalldatensätzen und Kontakten in den in Ihrem Replikationssatz AWS-Regionen angegebenen . Incident Manager unterstützt auch das automatische Zuweisen von Tags zu Vorfällen, die aus Reaktionsplänen erstellt wurden. Weitere Informationen finden Sie unter Markieren von Incident Manager-Ressourcen.	28. Juni 2022

Incident Manager-Integration mit ServiceNow	Sie können Incident Manager mit integrieren, ServiceNow indem Sie den AWS Service Management Connector für verwenden ServiceNow. Nachdem Sie die Integration konfiguriert haben, erstellen neue Vorfälle, die in Incident Manager erstellt wurden, einen entsprechenden Vorfall in ServiceNow. Wenn Sie einen Vorfall in Incident Manager aktualisieren, werden die Aktualisierungen dem entsprechenden Vorfall in hinzugefügt ServiceNo w. Wenn Sie einen Vorfall entweder in Incident Manager oder beheben ServiceNo w, wird der entsprechende Vorfall ebenfalls basierend auf den konfigurierten Einstellu ngen behoben. Weitere Informationen finden Sie unter Integration von AWS Systems Manager Incident Manager in ServiceNow.	9. Juni 2022

Importieren von Kontaktdaten	Wenn ein Vorfall erstellt wird, kann Incident Manager die Mitarbeiter mithilfe von Sprach- oder SMS-Benachrichtigungen benachrichtigen. Um sicherzustellen, dass die Antwortenden sehen, dass der Anruf oder die SMS-Benachrichtigung von Incident Manager stammt, empfehlen wir allen Antwortern, die Datei im virtuellen Kartenformat von Incident Manager (.vcf) in das Adressbuch auf ihren Mobilgeräten herunterzuladen. Weitere Informationen finden Sie unter Importieren von Kontaktdaten in Ihr Adressbuch.	18. Mai 2022

Mehrere Funktionsverbesserungen zur Verbesserung der Vorfallerstellung und -behebung	Incident Manager hat die folgenden Funktionsverbesserungen eingeführt, um die Erstellung und Behebung von Vorfällen zu verbessern: • Automatisches Erstellen von Vorfällen in anderen AWS-Regionen: Für den Fall, dass Incident Manager nicht in einem verfügbar ist, AWS-Region wenn Amazon CloudWatch oder Amazon einen Vorfall EventBridge erstellen, erstellen diese Services den Vorfall jetzt automatisch in einer der verfügbaren Regionen, die in Ihrem Replikationssatz angegeben sind. Weitere Informationen finden Sie unter Regionsübergreifen des Vorfallmanagement. • Automatisches Ausfüllen von Runbook-Parametern mit Vorfallmetadaten: Sie können Incident Manager jetzt so konfigurieren, dass Informationen über AWS Ressourcen aus Vorfällen erfasst werden. Incident Manager kann dann Runbook-Parameter mit den gesammelten Informationen füllen. Weitere Informationen finden Sie	17. Mai 2022

	unter Tutorial: Verwenden von Systems Manager Automation-Runbooks mit Incident Manager . • Automatisches Sammeln von AWS Ressource ninformationen: Wenn das System einen Vorfall erstellt, erfasst Incident Manager jetzt automatis ch Informationen über die an dem Vorfall beteiligten AWS Ressourcen. Incident Manager fügt diese Informati onen dann der Registerkarte Verwandte Elemente hinzu.	
Unterstützung für mehrere Runbooks	Incident Manager unterstützt jetzt die Ausführung mehrerer Runbooks während eines Vorfalls auf der Seite mit den Vorfalldetails.	14. Januar 2022
Incident Manager wurde in neuen gestartet AWS-Regio nen	Incident Manager ist jetzt in diesen neuen Regionen verfügbar: us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 und eu-west-3. Weitere Informationen zu Incident Manager-Regionen und -Kontingenten finden Sie im Allgemeine AWS-Referenz - Referenzhandbuch.	8. November 2021

Bestätigung der Konsoleninteraktion	Sie können Engagements jetzt direkt über die Incident Manager-Konsole bestätigen.	05. August 2021
Registerkarte „Eigenschaften“	Incident Manager hat der Seite mit den Details zu Vorfällen eine Registerkarte Eigenschaften hinzugefügt und bietet weitere Informationen zu den Vorfällen, dem übergeordneten OpsItemund der zugehörigen Analyse nach dem Vorfall.	3. August 2021
Incident-Manager-Start	Incident Manager ist eine Vorfallverwaltungskonsole, die Benutzern helfen soll, Vorfälle zu beheben, die ihre AWS gehosteten Anwendungen betreffen.	10. Mai 2021

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.