aws

User Guide

Incident Manager

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Incident Manager: User Guide

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

..... viii
Was ist AWS Systems Manager Incident Manager? 1
Hauptkomponenten und Funktionen 1
Vorteile der Verwendung von Incident Manager 3
Zugehörige Services 5
Zugriff auf Incident Manager 5
Regionen und Kontingente für Incident Manager 5
Preise für Incident Manager 6
Lebenszyklus eines Vorfalls 6
Alarmierung und Interaktion 7
Triage 8
Untersuchung und Schadensbegrenzung 9
Analyse nach dem Vorfall 10
AWS Systems Manager Incident Manager Änderung der Verfügbarkeit 12
Migrationshandbücher 12
Migration zu AWS Systems Manager OpsCenter 13
Migration zu Jira Service Management 27
Migration zu ServiceNow 28
Migration zu PagerDuty 29
Incident Manager-Daten exportieren 30
Was können Sie exportieren 30
Voraussetzungen 31
Erforderliche IAM-Berechtigungen 31
Struktur exportieren 32
Das Exportskript wird ausgeführt 32
Struktur der Ausgabedatei 34
Aufräumen der Incident Manager-Ressourcen 36
Löschen des Replikationssatzes 36
Löschen von Ressourcen im Zusammenhang mit Incident Manager 24
Einrichtung 38
Melden Sie sich an für ein AWS-Konto 38
Erstellen eines Benutzers mit Administratorzugriff 39
Erteilen programmgesteuerten Zugriffs 40
Erforderliche Rolle für die Einrichtung von Incident Manager 42

Erste Schritte ... 43
Voraussetzungen ... 43
Assistent zur Vorbereitung ... 43
Verwaltung von Vorfällen über Regionen hinweg AWS-Konten ... 51
Regionsübergreifendes Vorfallmanagement ... 51
Kontoübergreifendes Incident-Management ... 52
Best Practices ... 52
Richten Sie das kontenübergreifende Incident-Management ein und konfigurieren Sie es ... 53
Einschränkungen ... 55
Vorbereitung auf Vorfälle ... 56
Überwachen ... 58
Konfiguration von Replikationssätzen und Ergebnissen ... 59
Replikationssatz ... 59
Tags für einen Replikationssatz verwalten ... 61
Verwaltung der Funktion „Ergebnisse“ ... 61
Kontakte erstellen und konfigurieren ... 62
Kontaktkanäle ... 63
Einsatzpläne ... 64
So erstellen Sie einen Kontakt ... 64
Importieren Sie Kontaktinformationen in Ihr Adressbuch ... 66
Verwaltung der Rotationen von Einsatzkräften mit Bereitschaftszeitplänen ... 66
Erstellung eines Bereitschaftszeitplans und einer Rotation ... 67
Verwaltung eines bestehenden Bereitschaftszeitplans ... 72
Erstellung eines Eskalationsplans für die Einbindung der Einsatzkräfte ... 78
Stufen ... 79
Erstellen Sie einen Eskalationsplan ... 79
Chat-Kanäle für Einsatzkräfte erstellen und integrieren ... 80
Aufgabe 1: Amazon SNS SNS-Themen für Ihren Chat-Kanal erstellen oder aktualisieren ... 81
Aufgabe 2: Einen Chat-Kanal in Amazon Q Developer in Chat-Anwendungen erstellen ... 82
Aufgabe 3: Fügen Sie den Chat-Kanal zu einem Reaktionsplan in Incident Manager hinzu ... 85
Interaktion über den Chat-Kanal ... 86
Integration von Systems Manager Automation-Runbooks zur Behebung von Vorfällen ... 87
Zum Starten und Ausführen von Runbook-Workflows sind IAM-Berechtigungen erforderlich ... 88
Arbeiten mit Runbook-Parametern ... 91
Definieren Sie ein Runbook ... 93

Runbook-Vorlage für Incident Manager 94
Reaktionspläne erstellen und konfigurieren 96
Erstellung eines Reaktionsplans 97
Identifizierung potenzieller Ursachen für Vorfälle aus anderen Diensten 104
Aktivieren und erstellen Sie eine Servicerolle für Ergebnisse 105
Konfigurieren Sie Berechtigungen für die kontoübergreifende Unterstützung von Ergebnissen 106
Automatisches oder manuelles Erstellen von Vorfällen 107
Automatisches Erstellen von Vorfällen mit Alarmen CloudWatch 108
Automatisches Erstellen von Vorfällen mit EventBridge Ereignissen 109
Erstellen von Vorfällen mithilfe von SaaS-Partnerereignissen 109
Vorfälle mithilfe von AWS Serviceereignissen erstellen 111
Manuelles Erstellen von Vorfällen 112
Erforderliche IAM-Berechtigungen für das manuelle Starten von Incidents 113
Vorfalldetails in der Konsole anzeigen 116
Die Liste der Vorfälle in der Konsole anzeigen 116
Vorfalldetails in der Konsole anzeigen 116
Oberes Banner 117
Hinweise zum Vorfall 118
Registerkarten 118
-Übersicht 119
Diagnose 119
Zeitplan 121
Runbooks 121
Engagements 122
Verwandte Elemente 123
Eigenschaften 124
Durchführung einer Analyse nach dem Vorfall 125
Einzelheiten der Analyse 125
Übersicht 125
Metriken 126
Zeitplan 126
Fragen 127
Aktionen 127
Checkliste 127
Vorlagen für Analysen 128

AWS Standardvorlage ... 128
Erstellen Sie eine Analysevorlage ... 128
Erstellen Sie eine Analyse ... 129
Drucken Sie eine formatierte Vorfallanalyse ... 129
Lernprogramme ... 131
Verwenden von Runbooks mit Incident Manager ... 131
Aufgabe 1: Das Runbook erstellen ... 132
Aufgabe 2: Eine IAM-Rolle erstellen ... 135
Aufgabe 3: Verbinden Sie das Runbook mit Ihrem Reaktionsplan ... 138
Aufgabe 4: Ihrem Reaktionsplan einen CloudWatch Alarm zuordnen ... 138
Aufgabe 5: Überprüfung der Ergebnisse ... 139
Verwaltung von Sicherheitsvorfällen ... 140
Taggen von -Ressourcen ... 143
Sicherheit ... 145
Datenschutz ... 146
Datenverschlüsselung ... 147
Identitäts- und Zugriffsverwaltung ... 149
Zielgruppe ... 150
Authentifizierung mit Identitäten ... 150
Verwalten des Zugriffs mit Richtlinien ... 152
Wie AWS Systems Manager Incident Manager funktioniert mit IAM ... 153
Beispiele für identitätsbasierte Richtlinien ... 160
Beispiele für eine ressourcenbasierte Richtlinie ... 165
Serviceübergreifende Confused-Deputy-Prävention ... 167
Verwenden von servicegebundenen Rollen ... 168
AWS verwaltete Richtlinien für Incident Manager ... 171
Fehlerbehebung ... 177
Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen in Incident Manager ... 179
Voraussetzungen für den Austausch von Kontakten und Reaktionsplänen ... 180
Zugehörige Services ... 180
Einen Kontakt- oder Reaktionsplan teilen ... 181
Beenden Sie das Teilen eines geteilten Kontakt- oder Antwortplans ... 182
Identifizieren eines gemeinsam genutzten Kontakt- oder Antwortplans ... 182
Geteilte Kontakt- und Antwortplanberechtigungen ... 183
Fakturierung und Messung ... 183
Instance-Limits ... 183

Compliance-Validierung 184
Ausfallsicherheit 184
Sicherheit der Infrastruktur 185
Arbeiten mit VPC-Endpunkten ()AWS PrivateLink 185
Überlegungen zu Incident Manager-VPC-Endpunkten 186
Erstellen eines VPC-Schnittstellen-Endpunkts für Incident Manager 186
Erstellen einer VPC-Endpunktrichtlinie für Incident Manager 187
Konfigurations- und Schwachstellenanalyse 188
Bewährte Methoden für die Gewährleistung der Sicherheit 188
Bewährte Methoden zur präventiven Sicherheit für Incident Manager 188
Bewährte Methoden zur Detektivsicherheit für Incident Manager 190
Überwachen 192
Metriken mit Amazon überwachen CloudWatch 193
Incident Manager-Metriken auf der CloudWatch Konsole anzeigen 195
Dimensionen für Metriken 195
Protokollieren von API-Aufrufen mit AWS CloudTrail 196
Ereignisse zur Verwaltung von Incident Manager in CloudTrail 198
Beispiele für Incident Manager-Ereignisse 198
Produkt- und Service-Integrationen 201
Integration mit AWS-Services 201
Integration in andere Produkte und Services 207
Speichern von PagerDuty Zugangsdaten in einem geheimen Ordner AWS Secrets Manager ... 213
Fehlerbehebung 219
Fehlermeldung: `ValidationException – We were unable to validate the AWS Secrets Manager secret` 219
Fehlerbehebung bei anderen Problemen 221
Dokumentverlauf 222

AWS Systems Manager Incident Manager steht neuen Kunden nicht mehr offen. Bestandskunden können den Service weiterhin wie gewohnt nutzen. Weitere Informationen finden Sie unter Änderung der AWS Systems Manager Incident Manager Verfügbarkeit.

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.

Was ist AWS Systems Manager Incident Manager?

Incident Manager, ein Tool in AWS Systems Manager, soll Ihnen helfen, Vorfälle, die Ihre gehosteten Anwendungen betreffen, zu minimieren und diese zu AWS 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 CloudTrail AWS 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 durch die Integration mit dem Amazon Q Developer in Chat Applications Client. Amazon Q Developer in Chat-Anwendungen unterstützt die Erstellung von Chat-Kanälen für Incident Manager, die Slack, Microsoft Teams, oder Amazon Chime. Einsatzkräfte können direkt miteinander kommunizieren, automatische Benachrichtigungen über Vorfälle erhalten und — in Slack and Microsoft Teams— führt einige Incident Manager-Befehlszeilenschnittstellenoperationen (CLI) direkt aus.

Diagnose eines Vorfalls

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 Grundursache 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 bei ungeplanten Unterbrechungen oder Qualitätseinbußen Ihrer Services automatisch zu Vorfällen führen.

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 Sehenswürdigkeiten gehören:

- Ein CloudWatch Alarm oder eine EventBridge Regel verursacht einen Vorfall.
- Kennzahlen zu Vorfällen 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. Verwendung eines Amazon Q Developer in Chat-Anwendungen, für die der Client eingerichtet ist Slack, Microsoft Teams, oder Amazon Chime, Sie können die Einsatzkräfte in ihrem bevorzugten verbundenen Chat-Kanal zusammenbringen, wo sie direkt mit dem Vorfall und miteinander interagieren. 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 Interface Benutzerhandbuch. Informationen zu CLI-Befehlen für Incident Manager finden Sie unter ssm-incidents und ssm-contactsin der AWS CLI Befehlsreferenz.
- Incident Manager API — Weitere Informationen finden Sie in der AWS Systems Manager Incident Manager API-Referenz.
- AWS SDKs— Weitere Informationen finden Sie unter Tools, auf denen Sie aufbauen können AWS.

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 Manager Endpunkte 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 AWS Systems 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.

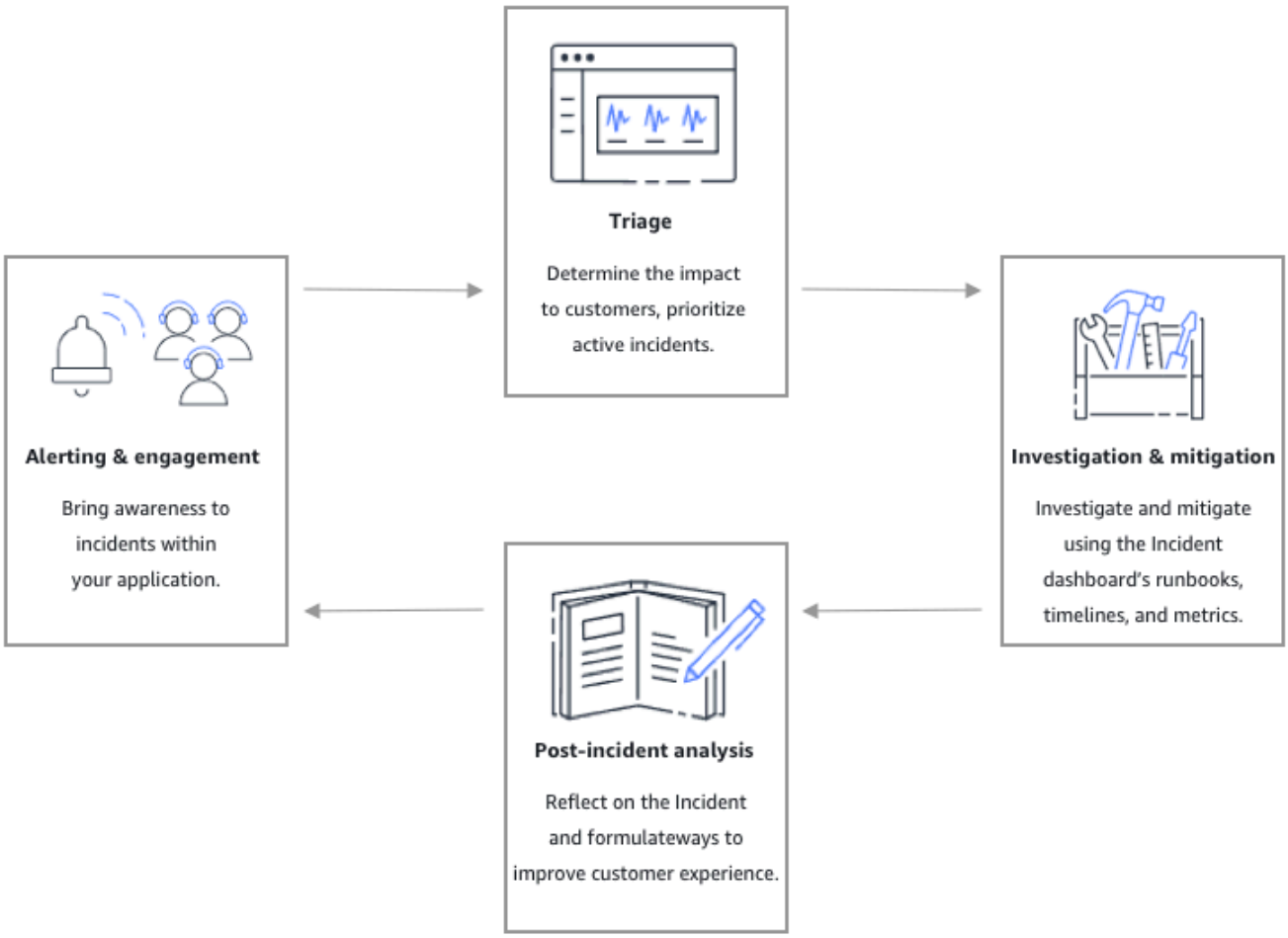
Eine Übersicht über einen Service Trusted Advisor, mit dem Sie die Kosten, die Sicherheit und die Leistung Ihrer AWS Umgebung optimieren können, finden Sie AWS Trusted Advisorim AWS Support Benutzerhandbuch.

Lebenszyklus von Vorfällen in Incident Manager

AWS Systems Manager Incident Manager bietet 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.

Wie in der folgenden Abbildung dargestellt, bietet Incident Manager Tools und bewährte Methoden 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 verwenden, 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 unterErstellung und Konfiguration von 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 unterAutomatisches oder manuelles Erstellen von Vorfällen im Incident Manager.

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 Gleichzeitig benachrichtigt Amazon Q Developer in Chat-Anwendungen die Antwortenden über einen Chat-Kanal und leitet sie zur Detailseite des Vorfalls weiter. Mithilfe des Chat-Kanals und der Vorfalldetails kann das Team einen Vorfall kommunizieren und prüfen. Weitere Informationen zur Einrichtung von Chat-Kanälen in Incident Manager finden Sie unterAufgabe 2: Einen Chat-Kanal in Amazon Q Developer in Chat-Anwendungen erstellen.

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, Lösung und 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. Vorfalldetails in der Konsole anzeigen

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
- CloudFormation Ressourcen verwalten

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

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. Wenn Sie Amazon Q Developer in Chat-Anwendungen verwenden, können Sie Chat-Kanäle in konfigurieren. Slack, Microsoft Teamsund Amazon Chime. In Slack and Microsoft Teams Kanäle, Responder können mithilfe einer Reihe von Befehlen direkt vom Chat-Kanal aus mit Vorfällen interagieren. `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 unterDurchführen einer Analyse nach einem Vorfall im Incident Manager.

AWS Systems Manager Incident Manager Änderung der Verfügbarkeit

AWS hat nach reiflicher Überlegung die Entscheidung getroffen, ab dem 7. November 2025 keine neuen Kunden mehr für AWS Systems Manager Incident Manager anzunehmen, und wird Incident Manager künftig keine neuen Funktionen oder Fähigkeiten mehr hinzufügen. AWS wird weiterhin in die Sicherheit und Verfügbarkeit von Incident Manager investieren, und bestehende Incident Manager-Kunden können den Service weiterhin wie gewohnt in Konten nutzen, für die Incident Manager bereits aktiviert ist.

Da Incident Manager keine neuen Funktionen oder Fähigkeiten mehr hinzufügen wird, ist es wichtig, dass Sie Ihre Alternativen für das Incident Management verstehen. Weitere Informationen zu den Alternativen finden Sie unterMigrationshandbücher.

Bei der Migration von Incident Manager zu einer alternativen Lösung empfehlen wir, die Vorfalldaten für weitere Analysen oder Archivierungszwecke zu exportieren. Weitere Informationen finden Sie unter Incident Manager-Daten exportieren.

Sobald Ihre Migration abgeschlossen ist, empfehlen wir außerdem, die verbleibenden Incident Manager-Ressourcen zu bereinigen, um laufende Kosten zu vermeiden. Weitere Informationen finden Sie unter Aufräumen der Incident Manager-Ressourcen.

Für zusätzlichen Support können Sie sich an Ihren Technical Account Manager wenden oder einen Support-Fall im Support Center der erstellen AWS-Managementkonsole.

Migrationshandbücher

Da AWS Systems Manager Incident Manager keine neuen Funktionen oder Fähigkeiten mehr hinzugefügt werden, ist es wichtig, dass Sie Ihre Alternativen für das Incident Management verstehen. In diesem Abschnitt finden Sie Migrationsleitfäden, die Sie beim Übergang von Incident Manager zu alternativen Lösungen unterstützen.

Für die Behebung betrieblicher Probleme in Ihrer AWS Infrastruktur empfehlen wir die Verwendung von AWS Systems Manager OpsCenter. Für automatisierte Paging- und Antwortfunktionen empfehlen wir Lösungen, die von unseren AWS Partner Network-Partnern angeboten werden. AWS Lösungsarchitekten und technische Kundenbetreuer können Sie anhand Ihrer spezifischen Anforderungen zu der am besten geeigneten Option weiterleiten.

Sie können sich auch die folgenden Migrationsleitfäden zur Integration mit Partnerlösungen ansehen:

- Migration zu AWS Systems Manager OpsCenter
- Migration zu Jira Service Management
- Migration zu ServiceNow
- Migration zu PagerDuty

Migration zu AWS Systems Manager OpsCenter

Dieser Leitfaden hilft Ihnen dabei, die wichtigsten Unterschiede zwischen Incident Manager zu verstehen und OpsCenter zu entscheiden, ob er Ihren betrieblichen Anforderungen OpsCenter entspricht, und bietet Möglichkeiten zur Migration OpsCenter von AWS Systems Manager Incident Manager zu.

AWS Systems Manager OpsCenter, eine Funktion von AWS Systems Manager, bietet einen zentralen Ort, an dem Betriebsingenieure und IT-Experten betriebliche Arbeitsaufgaben (OpsItems) im Zusammenhang mit AWS Ressourcen einsehen, untersuchen und lösen können. OpsCenter wurde entwickelt, um die mittlere Zeit bis zur Lösung (MTTR) bei Problemen zu reduzieren, die sich auf Ressourcen auswirken AWS . OpsCenter aggregiert und standardisiert OpsItems alle Dienste und stellt gleichzeitig kontextbezogene Untersuchungsdaten zu den einzelnen OpsItem, verwandten und verwandten Ressourcen bereit. OpsItems OpsCenter ist in Systems Manager Automation integriert, sodass Sie Automation-Runbooks verwenden können, um Probleme zu untersuchen und zu lösen. Sie können automatisch generierte Übersichtsberichte OpsItems nach Status und Quelle anzeigen. Sie können auch die kontenübergreifende Funktion verwendenOpsCenter, um kontenübergreifend zentral zu verwalten. OpsItems

> **Note**
>
> Mit der OpsCenter Nutzung sind Gebühren verbunden. Weitere Informationen finden Sie auf der AWS Systems Manager Preisseite.

Ähnlich wie Incident Manager OpsCenter hat es Integrationen mit Amazon CloudWatch und Amazon EventBridge. Das bedeutet, dass Sie diese Dienste so konfigurieren können, dass sie automatisch ein OpsItem In erstellen OpsCenter , wenn ein CloudWatch Alarm in den `ALARM` Status wechselt oder wenn ein Ereignis aus einem System EventBridge verarbeitet wird AWS-Service , das Ereignisse veröffentlicht. Wenn Sie CloudWatch Alarme und EventBridge Ereignisse so konfigurieren, dass sie

automatisch erstellt werden, OpsItems können Sie Probleme mit AWS Ressourcen von einer einzigen Konsole aus schnell diagnostizieren und beheben.

Die Unterschiede verstehen

AWS Systems Manager Incident Manager bietet Funktionen zur Reaktion auf Vorfälle, darunter automatisierte Reaktionspläne, Einbindung und Eskalation von Einsatzkräften, Rotationsmanagement auf Abruf, Runbook-Automatisierung, Chat-Ops-Integration (Slack, Microsoft Teams, Amazon Chime) und Analyse nach dem Vorfall. Diese Funktionen helfen Unternehmen dabei, kritische, zeitkritische Vorfälle, die gehostete Anwendungen betreffen, zu koordinieren und zu lösen. AWS

Im Gegensatz dazu AWS Systems Manager OpsCenter liegt der Schwerpunkt auf der Verwaltung betrieblicher Arbeitsaufgaben (OpsItems) für day-to-day betriebliche Probleme wie Sicherheitswarnungen, Leistungseinbußen, Ressourcenausfälle, Statusmeldungen und Statusänderungen. OpsCenter lässt sich über Amazon CloudWatch und Amazon EventBridge in AWS Ressourcen integrieren und ermöglicht so eine automatisierte OpsItem Erstellung und Behebung mithilfe von Systems Manager Automation-Runbooks. OpsCenter unterstützt die kontenübergreifende Verwaltung OpsItems innerhalb einer Region, sodass Betriebsteams Probleme über mehrere Konten hinweg einsehen, untersuchen und lösen können. AWS Beinhaltet jedoch OpsCenter keine Funktionen zum Paging oder zur Rotation auf Abruf.

Die Hauptunterschiede zwischen diesen beiden AWS Diensten liegen in ihrer Ausrichtung und ihrem Umfang. Incident Manager wurde für die Reaktion auf kritische, zeitkritische Vorfälle konzipiert und OpsCenter ist auf die Verwaltung umfassenderer betrieblicher Aufgaben und Arbeitsaufgaben ausgerichtet.

In der folgenden Tabelle werden die wichtigsten Funktionen von Incident Manager und OpsCenter verglichen. Verwenden Sie diesen Vergleich, um zu entscheiden, ob es OpsCenter Ihren betrieblichen Anforderungen entspricht.

Merkmal/Fähigkeit	AWS Systems Manager Incident Manager	AWS Systems Manager OpsCenter
Hauptzweck	Reaktion und Koordinat ion kritischer, zeitkritischer Vorfälle	Day-to-day Verwaltung betrieblicher Arbeitselemente
Anwendungsfälle	Vorfälle mit Auswirkungen auf Anwendungen, Sicherhei	Sicherheitswarnung en, Leistungseinbußen,

Merkmal/Fähigkeit	AWS Systems Manager Incident Manager	AWS Systems Manager OpsCenter
	tsverletzungen, Serviceausfälle, kritische Systemausfälle	Ressourcenausfälle, Integritätsmeldungen, Statusänderungen
Automatisiertes Paging	Ja — Integrierte Funktionen für Paging und Responder-Interaktion	Nein — Erfordert die Integration eines Drittanbieters (PagerDuty, ServiceNow, Jira)
Verwaltung der Rotation auf Abruf	Ja — Systemeigene Bereitschaftszeiten und Rotation	Nein — Wird nicht unterstützt
Eskalationsrichtlinien	Ja — Automatisierte Eskalationsketten	Nein — Manuelle Eskalation erforderlich
Chat-Ops-Integration	Ja — Slack, Microsoft Teams, Amazon Chime	Eingeschränkt — Manuelle Integration erforderlich
Runbook-Automatisierung	Ja — Automatisierte Ausführung über Reaktionspläne	Ja — Manuelle Ausführung von Systems Manager Automation-Runbooks
Kontenübergreifende Verwaltung	Ja — Kontoübergreifendes Teilen von Vorfällen	Ja — Kontoübergreifende OpsItem Verwaltung innerhalb einer Region

Optionen für die Migration

Wenn Sie bereits CloudWatch Alarme und EventBridge Regeln in Incident Manager integriert haben, müssen Sie diese aktualisieren, um sie in integrieren zu können OpsCenter. Sie können mit einem der folgenden Ansätze migrieren:

Automatisierte Migration mithilfe von Runbooks

Verwenden Sie Systems Manager Automation-Runbooks, um Ihre CloudWatch Alarme und EventBridge Regeln automatisch von Incident Manager zu zu OpsCenter migrieren. Dieser Ansatz umfasst Backups, konfigurierbare Genehmigungsworkflows und detaillierte Protokollierung.

Sie können wählen, ob Sie vor der Migration eine manuelle Genehmigung verlangen oder den Genehmigungsschritt für automatisierte umfangreiche Migrationen überspringen möchten. step-by-stepAnweisungen finden Sie unter. the section called “Verwendung von Migrations-Runbooks für OpsCenter”

Manuelle Integration

Konfigurieren Sie Ihre CloudWatch Alarme und EventBridge Regeln für die Integration manuell OpsCenter. Anweisungen finden Sie unter Zu CloudWatch erstellende Alarme konfigurieren OpsItems und Zu EventBridge erstellende Alarme konfigurieren OpsItems im Systems Manager Manager-Benutzerhandbuch.

Zugehörige Ressourcen

- AWS Systems Manager OpsCenter Benutzerhandbuch
- the section called “Incident Manager-Daten exportieren”
- the section called “Aufräumen der Incident Manager-Ressourcen”

Verwendung von Migrations-Runbooks für OpsCenter

Dieses Handbuch enthält step-by-step Anweisungen zur Migration Ihrer CloudWatch Amazon-Alarme und EventBridge Amazon-Regeln von AWS Systems Manager Incident Manager zur AWS Systems Manager OpsCenter Verwendung automatisierter Migrations-Runbooks.

Einen Überblick über die OpsCenter Funktionen und Informationen zu den Unterschieden zwischen Incident Manager und OpsCenter finden Sie unter. the section called “Migration zu AWS Systems Manager OpsCenter”

Überblick über die Migration

Der Migrationsprozess verwendet Systems Manager Automation-Runbooks, um Ihre vorhandenen CloudWatch Alarme und EventBridge Regeln in zu integrieren. OpsCenter Der Prozess umfasst die folgenden Schritte:

- Infrastruktur bereitstellen — Stellen Sie den CloudFormation Stack bereit, um die erforderlichen Ressourcen für die Migrations-Runbooks zu erstellen.
- CloudWatch Alarme und EventBridge Regeln migrieren — Führen Sie die Automatisierungs-Runbooks aus, zu denen Sie Ihre Ressourcen migrieren möchten. OpsCenter

- Ressourcen bereinigen — Löschen Sie optional das Replication Set und andere Incident Manager-Ressourcen.

> **Note**
>
> Die Runbooks unterstützen die Migration für ein einzelnes Konto-Region-Paar. Wenn Sie über Ressourcen in mehreren Konten oder Regionen verfügen, müssen Sie die Migration für jede Kombination aus Konto und Region separat ausführen.

Schritt 1: Stellen Sie die Vorlage bereit CloudFormation

Stellen Sie die CloudFormation Vorlage bereit, um die IAM-Rolle, den Amazon S3-Bucket und das Amazon SNS SNS-Thema zu erstellen, die für die Migrations-Runbooks erforderlich sind.

Erforderliche IAM-Berechtigungen

Um diese CloudFormation Vorlage bereitzustellen, benötigen Sie IAM-Berechtigungen für CloudFormation Stack-Operationen (`cloudformation:CreateStack`,`cloudformation:DescribeStacks`), IAM-Rollenmanagement (`iam:CreateRole`,,,`iam:PassRole`) `iam:PutRolePolicyiam:AttachRolePolicy`, Amazon S3 S3-Bucket-Erstellung und -Konfiguration (`s3:CreateBucket`,`s3:PutBucket*`) und Amazon SNS SNS-Themenoperationen (`sns:CreateTopic`,,`sns:Subscribe`). `sns:SetTopicAttributes`

Vollständige Informationen zu CloudFormation Berechtigungen finden Sie in der Referenz zu CloudFormation Berechtigungen im CloudFormation Benutzerhandbuch.

So stellen Sie die CloudFormation Vorlage mithilfe der Konsole bereit

1. Laden Sie die MigrationResourcesAWS-.zip-Datei herunterIncidentManager, die die `AWS-IncidentManager-MigrationResources.yaml` Vorlage enthält, und extrahieren Sie sie.
2. Öffnen Sie die CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.
3. Wählen Sie Stack erstellen aus.
4. Wählen Sie im Abschnitt Specify template (Vorlage angeben) die Option Upload a template file (Vorlagendatei hochladen) aus.
5. Wählen Sie Datei auswählen und wählen Sie dann die `AWS-IncidentManager-MigrationResources.yaml` Datei aus.

6. Wählen Sie Weiter aus.
7. Geben Sie auf der Seite „Stack-Details angeben“ Folgendes ein:
   - Stackname — Geben Sie einen Namen ein (z. B.`im-migration-infrastructure`)
   - ApprovalEmail- Geben Sie die E-Mail-Adresse für den Empfang von Genehmigungsbenachrichtigungen ein (wird nur verwendet, wenn der RequireManualApproval Runbook-Parameter auf true gesetzt ist).
   - IsPrimaryMigrationRegion- Wählen Sie aus, `true` ob dies die erste Region in Ihrem Konto ist, in der Sie den Stack bereitstellen, andernfalls wählen Sie `false`
8. Wählen Sie Weiter aus.
9. Wählen Sie auf der Seite Configure stack options (Stack-Optionen konfigurieren) Next (Weiter) aus.
10. Scrollen Sie auf der Bewertungsseite nach unten und wählen Sie Ich bestätige, dass CloudFormation möglicherweise IAM-Ressourcen mit benutzerdefinierten Namen erstellt werden.
11. Wählen Sie Absenden aus.

CloudFormation zeigt den `CREATE_IN_PROGRESS` Status an. Der Status ändert sich zu dem `CREATE_COMPLETE` Zeitpunkt, an dem der Stapel bereit ist.

> **Note**
>
> Wenn Sie CloudWatch Alarme oder EventBridge Regeln in mehreren Regionen haben, stellen Sie diesen CloudFormation Stack in jeder Region bereit, in der Sie die Migration durchführen möchten.
> Verwenden Sie für AWS unternehmensweite Bereitstellungen mit mehreren Konten zwei: CloudFormation StackSets
>
> - Primär StackSet — Für eine Region IsPrimaryMigrationRegion pro Konto auf „true“ setzen
> - Sekundär StackSet — Für alle anderen Regionen IsPrimaryMigrationRegion auf „Falsch“ gesetzt
>
> Anweisungen finden Sie CloudFormation StackSets im CloudFormation Benutzerhandbuch unter Arbeiten mit.

Um die CloudFormation Vorlage mit dem zu implementieren AWS CLI

Verwenden Sie für die erste Region in Ihrem Konto den folgenden Befehl:

```
aws cloudformation create-stack \
    --stack-name im-migration-infrastructure \
    --template-body file://AWS-IncidentManager-MigrationResources.yaml \
    --parameters ParameterKey=ApprovalEmail,ParameterValue=your-email@example.com \
    ParameterKey=IsPrimaryMigrationRegion,ParameterValue=true \
    --capabilities CAPABILITY_NAMED_IAM \
    --region us-east-1
```

Stellen Sie für weitere Regionen in demselben Konto Folgendes `IsPrimaryMigrationRegion` ein`false`:

```
aws cloudformation create-stack \
    --stack-name im-migration-infrastructure \
    --template-body file://AWS-IncidentManager-MigrationResources.yaml \
    --parameters ParameterKey=ApprovalEmail,ParameterValue=your-email@example.com \
    ParameterKey=IsPrimaryMigrationRegion,ParameterValue=false \
    --capabilities CAPABILITY_NAMED_IAM \
    --region us-west-2
```

Um den Stack-Status zu überprüfen:

```
aws cloudformation describe-stacks \
    --stack-name im-migration-infrastructure \
    --query 'Stacks[0].StackStatus' \
    --output text
```

Warten Sie, bis der Befehl zurückkehrt, `CREATE_COMPLETE` bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 2: CloudWatch Alarme und EventBridge Regeln migrieren

Verwenden Sie die Systems Manager Automation-Runbooks, um Ihre CloudWatch Alarme und EventBridge Regeln von Incident Manager zu zu OpsCenter migrieren.

Runbooks für die Migration

- AWS- MigrateIncidentManagerCloudWatchAlarms
- AWS- MigrateIncidentManagerEventBridgeRules

Weitere Informationen zur Funktionsweise dieser Runbooks, einschließlich detaillierter Schrittbeschreibungen, Eingabeparameter und Ausgaben, finden Sie in der Runbook-Dokumentation.

So funktionieren die Runbooks

Beide Migrations-Runbooks folgen demselben Workflow:

- Erkennung und Batching — Erkennt alle CloudWatch Alarme oder EventBridge Regeln, die mit den Aktionen des Incident Manager-Reaktionsplans konfiguriert sind, und organisiert sie in konfigurierbaren Batches.
- Manuelle Genehmigung (optional) — In der Standardeinstellung ist eine ausdrückliche Genehmigung erforderlich, bevor mit der Migration fortgefahren werden kann. Das Timeout beträgt 24 Stunden. Eine Amazon SNS SNS-Benachrichtigung wird an die bei der CloudFormation Bereitstellung angegebene E-Mail-Adresse gesendet. Alle Konfigurationen werden auf Amazon S3 gesichert, und die vollständige Liste der zu migrierenden Ressourcen wird zur manuellen Überprüfung gespeichert. Dieser Schritt kann übersprungen werden, indem die Einstellung auf „False“ RequireManualApproval gesetzt wird.
- Backup und Migration — Wenn die manuelle Genehmigung auf „true“ gesetzt ist, wird auf die Genehmigung gewartet. Anschließend wird jede Konfiguration auf Amazon S3 gesichert und die Migration durchgeführt. Wenn dieser Wert auf „False“ gesetzt ist, wird direkt mit der Sicherung und Migration fortgefahren.

Eingabeparameter

Beide Runbooks benötigen die folgenden Parameter:

AutomationAssumeRole (Erforderlich)

Der ARN des vom CloudFormation Stack `IM-Migration-Automation-Role` erstellten.

ApproverArn (Erforderlich)

Der ARN der IAM-Rolle oder des Benutzers, der die Migration überprüfen und genehmigen kann.

S3 BucketName (erforderlich)

Der Name des Amazon S3 S3-Buckets, der vom CloudFormation Stack erstellt wurde.

SNSTopicArn (Erforderlich)

Der ARN des Amazon SNS SNS-Themas, das vom CloudFormation Stack erstellt wurde.

MaxNumberOfAlarmsToMigrate oder MaxNumberOfRulesToMigrate (optional)

Die maximale Anzahl von Ressourcen, die in einer einzigen Ausführung migriert werden sollen. Gültige Werte: 1, 5, 10, 50, 100, 500, 5000, 10000, 25000, 50000. Standard: 10000.

BatchSize (Fakultativ)

Die Anzahl der Ressourcen, die in jedem Stapel verarbeitet werden sollen. Gültige Werte: 25, 50, 100, 200, 250, 300, 350, 400, 450, 500. Standard: 100. Das Runbook unterstützt maximal 100 × BatchSize Ressourcen pro Ausführung.

RequireManualApproval (Fakultativ)

Boolescher Wert, um zu steuern, ob vor der Migration eine manuelle Genehmigung erforderlich ist. Wenn diese Option auf true (Standard) gesetzt ist, erhalten Sie eine Amazon SNS-Benachrichtigungs-E-Mail mit dem Amazon S3-Speicherort der Ressourcenliste und einem Link zur Automation-Ausführungskonsole zur Genehmigung, Ablehnung oder Stornierung. Wenn diese Option auf „False“ gesetzt ist, wird das Runbook nach der Erkennung und Sicherung automatisch fortgesetzt. Gültige Werte: true, false. Standard: true

Um mit der Konsole zu migrieren

1. Öffnen Sie die Systems Manager Manager-Konsole unter https://console.aws.amazon.com/systems-manager.
2. Klicken Sie im Navigationsbereich auf Automation.
3. Suchen Sie nach dem Runbook-Namen (oder). `AWS-MigrateIncidentManagerCloudWatchAlarms` `AWS-MigrateIncidentManagerEventBridgeRules`
4. Wählen Sie Automatisierung ausführen.

5. Geben Sie die Parameterwerte aus Ihren CloudFormation Stack-Ausgaben ein.
6. (Optional) Stellen Sie diese Option ein RequireManualApproval, `false` wenn Sie den manuellen Genehmigungsschritt überspringen möchten.
7. Wählen Sie Ausführen.
8. Wenn diese `RequireManualApproval` Option auf „true“ gesetzt ist (Standardeinstellung), erhalten Sie eine E-Mail-Benachrichtigung, wenn die Ausführung auf eine manuelle Überprüfung wartet. Die E-Mail enthält einen Genehmigungslink zur Seite der Automation Execution Console. Überprüfen Sie die Ressourcenliste im Amazon S3 S3-Bucket und genehmigen, verweigern oder stornieren Sie sie dann innerhalb von 24 Stunden entweder über den E-Mail-Link oder die Konsolenseite. Die Migration wird erst nach der Genehmigung fortgesetzt. Wenn der Wert auf false gesetzt ist, wird die Migration nach dem Backup automatisch fortgesetzt.
9. Warten Sie, bis sich der Ausführungsstatus auf Erfolgreich ändert.

Um mit dem zu migrieren AWS CLI

Für CloudWatch Alarme:

```
aws ssm start-automation-execution \
    --document-name "AWS-MigrateIncidentManagerCloudWatchAlarms" \
    --parameters '{
        "AutomationAssumeRole": ["arn:aws:iam::123456789012:role/IM-Migration-
Automation-Role"],
        "ApproverArn": ["arn:aws:iam::123456789012:role/Admin"],
        "S3BucketName": ["im-migration-logs-123456789012-us-east-1"],
        "SNSTopicArn": ["arn:aws:sns:us-east-1:123456789012:Automation-IM-Migration-
Approvals"],
        "RequireManualApproval": ["false"]
    }' \
    --region us-east-1
```

Für EventBridge Regeln:

```
aws ssm start-automation-execution \
    --document-name "AWS-MigrateIncidentManagerEventBridgeRules" \
    --parameters '{
```

```
        "AutomationAssumeRole": ["arn:aws:iam::123456789012:role/IM-Migration-
Automation-Role"],
        "ApproverArn": ["arn:aws:iam::123456789012:role/Admin"],
        "S3BucketName": ["im-migration-logs-123456789012-us-east-1"],
        "SNSTopicArn": ["arn:aws:sns:us-east-1:123456789012:Automation-IM-Migration-
Approvals"],
        "RequireManualApproval": ["false"]
    }' \
    --region us-east-1
```

So überprüfen Sie die Ressourcenliste in Amazon S3:

```
# For CloudWatch alarms
aws s3 cp s3://im-migration-logs-123456789012-us-east-1/review/CloudWatch/
review_CW_alarms_to_migrate_123456789012_us-east-1.json ./

# For EventBridge rules
aws s3 cp s3://im-migration-logs-123456789012-us-east-1/review/EventBridge/
review_EB_rules_to_migrate_123456789012_us-east-1.json ./
```

Wenn diese RequireManualApproval Option auf „true“ gesetzt ist, überprüfen Sie die Ressourcenliste und genehmigen Sie die Migration, indem Sie auf den Genehmigungslink in der E-Mail-Benachrichtigung oder auf der Seite der Automation-Ausführungskonsole klicken. Wenn der Wert auf „False“ gesetzt ist, wird die Migration nach dem Backup automatisch fortgesetzt.

Schritt 3: Überprüfen Sie Ihre Migration

Stellen Sie nach Abschluss der Migration sicher, dass Ihre Ressourcen ordnungsgemäß funktionieren:

- Einen Testalarm oder ein Testereignis auslösen — Aktivieren Sie einen Ihrer migrierten CloudWatch Alarme oder EventBridge Regeln, um eine Testbenachrichtigung zu generieren.
- OpsItem Erstellung bestätigen — Stellen Sie sicher, dass automatisch eine erstellt OpsItem wird, OpsCenter wenn der Alarm oder das Ereignis ausgelöst wird.
- Überprüfen Sie die Schweregradzuweisung — Vergewissern Sie sich, dass der Schweregrad aus Ihrer ursprünglichen Incident Manager-Konfiguration in der korrekt beibehalten wurde OpsItem. (Gilt nur für CloudWatch Alarme).

Schritt 4: Bereinigen Sie die Incident Manager-Ressourcen

Nachdem Sie Ihre CloudWatch Alarme und EventBridge Regeln erfolgreich migriert haben, können Sie optional die Incident Manager-Ressourcen bereinigen, um sie vollständig vom Service zu entfernen.

Ausführliche Anweisungen zum Löschen des Replication Sets, der Reaktionspläne, Kontakte, Runbooks und anderer Incident Manager-Ressourcen finden Sie unter. the section called “Aufräumen der Incident Manager-Ressourcen”

CloudFormation Stapel löschen (optional)

Sie können die CloudFormation Stacks löschen, um die für die Migration erstellte IAM-Rolle, das Amazon SNS SNS-Thema und den Amazon S3 S3-Bucket zu entfernen.

> **Important**
>
> Der Amazon S3 S3-Bucket, der Backups aller migrierten Ressourcen enthält, muss vor dem Löschen des Stacks geleert werden. CloudFormation Amazon S3 S3-Buckets, die Objekte enthalten, können nicht gelöscht werden.

Um den Stapel zu löschen CloudFormation

```
aws cloudformation delete-stack --stack-name <your-stack-name>
```

Überwachung und Problembehebung

CloudWatch Protokolle — Migrationsaktivitäten werden in Logs CloudWatch protokolliert:

- CloudWatch Alarme: `/aws/ssm/incidentmanager/cwmigration`
- EventBridge Regeln: `/aws/ssm/incidentmanager/ebmigration`

Amazon S3-Backup-Struktur — Alle Konfigurationen werden vor der Migration auf Amazon S3 gesichert:

```
migration-logs-{AccountId}-{Region}/
```

```
### backups/
#   ### CloudWatch/
#   #   ### {AccountId}/
#   #       ### {Region}/
#   #           ### {AlarmName}_backup.json
#   ### EventBridge/
#       ### {AccountId}/
#           ### {Region}/
#               ### {RuleName}_backup.json
### review/
    ### CloudWatch/
    #   ### review_CW_alarms_to_migrate_{AccountId}_{Region}.json
    ### EventBridge/
        ### review_EB_rules_to_migrate_{AccountId}_{Region}.json
```

Häufig auftretende Probleme:

- Amazon SNS SNS-Benachrichtigung nicht erhalten (wenn RequireManualApproval =true) — Überprüfen Sie das Amazon SNS SNS-Themenabonnement:

  ```
  aws sns list-subscriptions-by-topic --topic-arn <sns-topic-arn>
  ```

- Teilweise Fehler bei der Migration — Suchen Sie in den CloudWatch Protokollen nach detaillierten Fehlermeldungen und versuchen Sie erneut, die Automatisierung mit einer reduzierten Batchgröße durchzuführen.

Rollback-Verfahren:

Wenn Sie die Migration rückgängig machen müssen:

- Backups von Amazon S3 abrufen:

  ```
  aws s3 sync s3://im-migration-logs-123456789012-us-east-1/backups/ ./backups/
  ```

- Ressourcen wiederherstellen:

```
# For CloudWatch alarms
aws cloudwatch put-metric-alarm --cli-input-json file://backups/
CloudWatch/123456789012/us-east-1/MyAlarm_backup.json

# For EventBridge rules
aws events put-targets --rule MyRule --targets file://backups/
EventBridge/123456789012/us-east-1/MyRule_backup.json
```

Häufig gestellte Fragen

F: Was passiert, wenn bei der Automatisierung während der Genehmigung ein Timeout auftritt?

A: Die Automatisierung läuft nach 24 Stunden ab, wenn keine Genehmigung eingeht. Sie können die Automatisierung mit denselben Parametern neu starten.

F: Kann ich Ressourcen zwischen Regionen migrieren?

A: Nein. Jede Region muss mithilfe regionsspezifischer Automatisierungsausführungen separat migriert werden.

F: Wie lange dauert die Migration?

A: Die Migrationszeit hängt von der Anzahl der Ressourcen ab:

- ~100 Alarme/Regeln: 5-10 Minuten
- ~1000 Alarme/Regeln: 30-60 Minuten
- ~10000 Alarme/Regeln: 2-4 Stunden

F: Wird der Schweregrad nach der Migration zu beibehalten? OpsCenter

A: Ja. Der im Incident Manager-Reaktionsplan für die Auswirkungsstufen konfigurierte Schweregrad wird beibehalten und während der CloudWatch Alarmmigration automatisch den entsprechenden OpsCenter Schweregraden zugeordnet. Dies gilt nicht für EventBridge Regeln.

F: Wird mir die Ausführung der Automation-Runbooks in Rechnung gestellt?

A: Nein. Für die Runbooks zur Migrationsautomatisierung fallen keine Ausführungsgebühren an. Für die OpsCenter Nutzung nach der Migration fallen jedoch Gebühren an. Einzelheiten finden Sie in der Preisdokumentation für Systems Manager.

Zugehörige Ressourcen

- the section called “Migration zu AWS Systems Manager OpsCenter”
- AWS Systems Manager OpsCenter Benutzerhandbuch
- Systems Manager Automatisierung
- the section called “Incident Manager-Daten exportieren”
- the section called “Aufräumen der Incident Manager-Ressourcen”

Migration zu Jira Service Management

Jira Service Management (JSM) ist eine IT-Servicemanagement-Lösung (ITSM), die Teams dabei unterstützt, Mitarbeiter- und Kundenanfragen über mehrere Kanäle wie E-Mail, Chat, Help Center und Widgets zu empfangen, zu verfolgen, zu verwalten und zu lösen. Jira Service Management basiert auf der Jira-Plattform und ermöglicht es Teams im gesamten Unternehmen — von der Entwicklung über die IT bis hin zur Personalabteilung —, Anfragen entgegenzunehmen, auf Warnungen und Vorfälle zu reagieren, Änderungen vorzunehmen, Ressourcen nachzuverfolgen, Wissen zu ermitteln und Workflows zu automatisieren. Jira Service Management umfasst Funktionen für das Incident-Management wie Bereitschaftsplanung, Alarmierung, Verwaltung großer Vorfälle, Änderungsmanagement und Funktionen für tadellose Post-Mortem-Funktionen (PIR), die für DevOps Workflows konzipiert sind und bestehende CI/CD Pipelines und Automatisierung nutzen, um den manuellen Aufwand zu reduzieren.

Jira Service Management lässt sich in Amazon CloudWatch und Amazon integrieren EventBridge, sodass Sie automatisch Jira Service Management-Benachrichtigungen erstellen können, wenn CloudWatch Alarme in den `ALARM` Status wechseln oder wenn Ereignisse aus einem EventBridge System verarbeitet werden AWS-Service , das Ereignisse veröffentlicht. Durch die Konfiguration von CloudWatch Alarmen und EventBridge Ereignissen zur automatischen Erstellung von Jira Service Management-Benachrichtigungen können Sie Probleme mit AWS Ressourcen von einer einzigen Plattform aus schnell diagnostizieren und beheben. Jira Service Management fungiert als Dispatcher und benachrichtigt die richtigen Personen auf der Grundlage von Bereitschaftszeitplänen und Eskalationsrichtlinien über mehrere Kanäle (E-Mail, SMS, Telefonanrufe, mobile Push).

Wenn du bereits CloudWatch Alarme und EventBridge Regeln integriert hast, empfehlen wir dir AWS Systems Manager Incident Manager, diese Integrationen zu aktualisieren und stattdessen Jira Service Management zu verwenden. Die offizielle Atlassian-Dokumentation enthält detaillierte Anweisungen zur Integration von Jira Service Management mit CloudWatch und zur Integration von Jira Service Management mit. EventBridge

Neben der automatisierten Erstellung von Warnmeldungen bietet Jira Service Management eine Reihe von Funktionen zur Optimierung des Incident-Managements, wie z. B. die Planung von Bereitschaftsdiensten, Eskalationsrichtlinien und Automatisierungsregeln. Einzelheiten zur Konfiguration dieser Funktionen finden Kunden in der folgenden Atlassian-Dokumentation:

- Entdecke Benachrichtigungen und Bereitschaftsdienste
- Erstellen Sie Bereitschaftszeitpläne
- Eskalationsrichtlinien erstellen
- Richten Sie Teams und Personen ein
- Richten Sie Kontaktmethoden ein
- Benachrichtigungsregeln konfigurieren
- Richten Sie SMS- und Sprachbenachrichtigungen ein
- Richten Sie Automatisierungsregeln ein
- Richten Sie Interessenvertreter für Vorfälle ein und verwalten Sie sie

Wenn du zusätzliche Unterstützung benötigst, kannst du dich an deinen Technical Account Manager oder einen Atlassian-Vertriebsmitarbeiter wenden, um weitere Informationen zu erhalten.

Migration zu ServiceNow

ServiceNow Incident Management ist ein zentrales ITSM-Modul, das darauf ausgelegt ist, den normalen Servicebetrieb nach ungeplanten Unterbrechungen wiederherzustellen und gleichzeitig die Auswirkungen auf das Geschäft zu minimieren. Wie Incident Manager bietet ServiceNow Incident Management ein strukturiertes, automatisiertes System zur Anzeige, Untersuchung und Lösung von IT-Vorfällen mit Funktionen wie automatisierter Priorisierung und integrierten Eskalationsprozessen.

Das Modul ServiceNow Service Operations with Incident Management und Event Management ist in Amazon integriert CloudWatch, sodass Sie automatisch ServiceNow Ereignisse/Benachrichtigungen und Vorfälle erstellen können, wenn CloudWatch Alarme in den `ALARM` Status eintreten. Die Konfiguration von CloudWatch Alarmen zur automatischen Erstellung von ServiceNow Vorfällen mit Webhook to AIOps Event Management ermöglicht es Ihnen, Probleme mit AWS Ressourcen von einer einzigen Plattform aus schnell zu diagnostizieren und zu beheben.

Wenn Sie bereits CloudWatch Alarme integriert haben, empfehlen wir Ihnen AWS Systems Manager Incident Manager, diese Integrationen so zu aktualisieren, dass Sie stattdessen die ServiceNow

Incident Management - und AIOps Event Intelligence-Plattform verwenden. Die offizielle ServiceNow Dokumentation enthält detaillierte Anweisungen zur Integration ServiceNow mit Amazon CloudWatch.

Neben der automatisierten Erstellung von Vorfällen bietet ServiceNow Incident Management eine Reihe von Funktionen zur Verbesserung des Incident-Managements, wie z. B. das Kommunikationsmanagement für Vorfälle, die Planung von Bereitschaftsdiensten, Eskalationsrichtlinien und mehr. Einzelheiten zur Konfiguration dieser Funktionen finden Kunden in der folgenden ServiceNow Dokumentation:

- Dokumentation zum Incident Management
- Verwaltung der Zuverlässigkeit von Diensten
- Kommunikationsmanagement und Ansprechpartner bei Vorfällen
- Zeitpläne für Bereitschaftsdienste
- Eskalationsprozess

Für zusätzliche Unterstützung können Sie sich an Ihren Technical Account Manager oder einen ServiceNow Vertriebsmitarbeiter wenden, um weitere Informationen zu erhalten.

Migration zu PagerDuty

PagerDutyist eine Plattform für das Incident-Management, die Unternehmen dabei unterstützt, Vorfälle zu erkennen, darauf zu reagieren und sie sogar zu verhindern. Wie Incident Manager PagerDuty bietet es einen zentralen Ort, an dem Betriebsteams wichtige Aufgaben im Zusammenhang mit AWS Ressourcen erledigen können, wodurch die Auswirkungen auf die Kunden reduziert werden.

PagerDuty lässt sich in Amazon CloudWatch und Amazon integrieren EventBridge, sodass Sie automatisch PagerDuty Vorfälle erstellen können, wenn CloudWatch Alarme in den `ALARM` Status wechseln oder wenn Ereignisse von einem System EventBridge verarbeitet werden AWS-Service , das Ereignisse veröffentlicht. Durch die Konfiguration von CloudWatch Alarmen und EventBridge Ereignissen zur automatischen Erzeugung von PagerDuty Vorfällen können Sie AWS Ressourcenprobleme von einer einzigen Plattform aus schnell diagnostizieren und beheben.

Wenn Sie bereits CloudWatch Alarme und EventBridge Regeln integriert haben, empfehlen wir Ihnen AWS Systems Manager Incident Manager, diese Integrationen zu aktualisieren, um sie stattdessen zu verwenden PagerDuty . Die offizielle PagerDuty Dokumentation enthält detaillierte Anweisungen zur Integration PagerDuty mit CloudWatch und zur Integration PagerDuty mit EventBridge.

Neben der automatisierten Erstellung von Vorfällen PagerDuty bietet sie eine Reihe von Funktionen zur Verbesserung des Incident-Managements, wie z. B. Bereitschaftsplanung, Eskalationsrichtlinien und mehr als 700 Plattformintegrationen. out-of-box Sie können auch Benachrichtigungsregeln anpassen, Chat-Oberflächen konfigurieren und KI und Automatisierung innerhalb der PagerDuty Plattform nutzen, um die Lösung von Vorfällen zu beschleunigen.

- Nutzer verwalten
- Teams erstellen
- Kontaktmethoden einrichten
- Benachrichtigungsregeln konfigurieren
- Richten Sie eine Rotation auf Abruf ein
- Eskalationsrichtlinien erstellen
- Slack-Integration konfigurieren
- Automatisierungsaktionen einrichten

Für zusätzlichen Support können Sie sich an Ihren Technical Account Manager oder an AWS-IM-help@pagerduty.com wenden, um weitere Informationen zu erhalten.

Incident Manager-Daten exportieren

In diesem Thema wird beschrieben, wie Sie ein Python-Skript verwenden, um Ereignisaufzeichnungen und Analysen nach einem Vorfall aus AWS Systems Manager Incident Manager zu exportieren. Das Skript exportiert Daten für weitere Analyse- oder Archivierungszwecke in strukturierte JSON-Dateien.

Was können Sie exportieren

Das Skript exportiert die folgenden Daten:

- Vollständige Aufzeichnungen über Vorfälle, einschließlich:
  - Zeitleiste der Ereignisse
  - Verwandte Elemente
  - Engagements
  - Automatisierte Ausführungen

  - Ergebnisse zur Sicherheit
  - Tags (Markierungen)
- Dokumente zur Analyse nach einem Vorfall von Systems Manager

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Python 3.7 oder höher installiert
- AWS CLI mit den entsprechenden Anmeldeinformationen konfiguriert
- Die folgenden Python-Pakete sind installiert:

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

Erforderliche IAM-Berechtigungen

Um dieses Skript verwenden zu können, stellen Sie sicher, dass Sie über die folgenden Berechtigungen verfügen:

Berechtigungen für Systems Manager Incidents

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

```
        }
    ]
}
```

Systems Manager Manager-Berechtigungen

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

Struktur exportieren

Das Skript erstellt die folgende Verzeichnisstruktur für exportierte Daten:

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

Das Exportskript wird ausgeführt

Grundlegende Verwendung

Das Incident Manager-Datenexport-Skript wird bereitgestelltlinkhere. Bitte laden Sie das Skript herunter und verwenden Sie die folgenden Anweisungen, um das Skript auszuführen.

Um das Skript mit den Standardeinstellungen auszuführen:

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

Verfügbare Optionen

Sie können den Export mithilfe der folgenden Befehlszeilenoptionen anpassen:

Option	Description	Standard
`--region`	AWS Region	`us-east-1`
`--profile`	AWS Name des Profils	Standardprofil
`--verbose` , `-v`	Aktivieren Sie die detaillierte Protokollierung	FALSE
`--limit`	Maximale Anzahl der zu exportierenden Vorfälle	Kein Limit
`--timeline-events-limit`	Maximale Anzahl von Ereignissen pro Vorfall	100
`--timeline-details-limit`	Maximaler Zeitplan für Ereignisdetails pro Vorfall	100
`--related-items-limit`	Maximale Anzahl verwandter Artikel pro Vorfall	50
`--engagements-limit`	Maximale Anzahl an Interaktionen pro Vorfall	20
`--analysis-docs-limit`	Maximale Anzahl an zu exportierenden Analysedokumenten	50

Beispiele

Export aus einer bestimmten Region mithilfe eines benutzerdefinierten Profils:

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

Export mit ausführlicher Protokollierung und Einschränkungen für Tests:

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

Export mit konservativen Grenzwerten für große Datensätze:

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

Struktur der Ausgabedatei

JSON-Struktur des Ereignisdatensatzes

Jede Vorfallaufzeichnungsdatei enthält die folgende Struktur:

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

```
                "details": {}  // From get-timeline-event
            }
        ],
        "summary_only_events": [],
        "metadata": {
            "total_events_found": 45,
            "events_with_details": 25,
            "limits_applied": {}
        }
    },
    "related_items": {
        "items": [],
        "metadata": {}
    },
    "engagements": {
        "engagements": [],
        "metadata": {}
    },
    "automation_executions": [],
    "findings": [],
    "tags": [],
    "post_incident_analysis": {
        "analysis_reference": {},
        "metadata": {}
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
        "incident_arn": "arn:aws:ssm-incidents::..."
    }
}
```

JSON-Struktur nach der Analyse des Vorfalls

Jede Analysedokumentdatei enthält:

```
{
    "document_metadata": {
        // Document metadata from list-documents
    },
    "document_details": {
        "Name": "037fc5dd-cd86-49bb-9c3d-15720e78798e",
        "Content": "...", // Full JSON content
```

```
        "DocumentType": "ProblemAnalysis",
        "CreatedDate": 1234567890,
        "ReviewStatus": "APPROVED",
        "AttachmentsContent": [],
        // ... other fields from get-document
    },
    "export_metadata": {
        "exported_at": "2025-09-18T...",
        "region": "us-east-*",
        "document_name": "..."
    }
}
```

Aufräumen der Incident Manager-Ressourcen

Wenn Sie die Incident Manager-Ressourcen nicht mehr verwenden AWS Systems Manager Incident Manager, empfehlen wir Ihnen, die verbleibenden Incident Manager-Ressourcen zu bereinigen. Dadurch werden Sie vollständig vom Service ausgeschlossen und laufende Gebühren werden vermieden. Weitere Informationen finden Sie auf der AWS Systems Manager Preisseite.

Löschen des Replikationssatzes

Das Replication Set ist eine wichtige Komponente von Incident Manager, die die Replikation von Vorfalldaten über mehrere AWS Regionen hinweg erleichtert. Wenn Sie Incident Manager nicht mehr benötigen, sollten Sie das Replication Set löschen.

Um das Replikationsset zu löschen:

1. Öffnen Sie die AWS Systems Manager Konsole
2. Wählen Sie im Navigationsbereich Incident Manager
3. Suchen Sie unter „Replikationssätze“ den Replikationssatz, den Sie löschen möchten
4. Klicken Sie auf den Namen des Replikationssatzes, um die Detailseite zu öffnen
5. Klicken Sie auf der Seite mit den Details zum Replikationssatz auf die Schaltfläche „Löschen“
6. Überprüfen Sie im Bestätigungsdialogfeld die Informationen und klicken Sie auf „Replikationssatz löschen“, um mit dem Löschen fortzufahren

> **Note**
>
> Durch das Löschen des Replikationssatzes werden alle im Incident Manager gespeicherten Incident-Daten dauerhaft gelöscht. Stellen Sie sicher, dass Sie keinen Zugriff mehr auf historische Vorfallinformationen benötigen, bevor Sie mit dem Löschen fortfahren.

Löschen von Ressourcen im Zusammenhang mit Incident Manager

Zusätzlich zum Replication Set verfügen Sie möglicherweise über weitere Ressourcen im Zusammenhang mit Incident Manager, wie Reaktionspläne, Kontakte und Runbooks. Wenn Sie diese Ressourcen nicht mehr benötigen, können Sie erwägen, sie vollständig aus Incident Manager zu löschen.

So löschen Sie Ressourcen im Zusammenhang mit Incident Manager:

1. Öffnen Sie die Konsole AWS Systems Manager
2. Wählen Sie im Navigationsbereich Incident Manager
3. Navigieren Sie zum entsprechenden Abschnitt (z. B. „Reaktionspläne“, „Kontakte“, „Runbooks“) und suchen Sie nach den Ressourcen, die Sie löschen möchten
4. Wählen Sie die Ressourcen aus und klicken Sie auf die Schaltfläche „Löschen“, um sie zu entfernen

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
- Erstellen eines Benutzers mit Administratorzugriff
- Erteilen programmgesteuerten Zugriffs
- Erforderliche Rolle für die Einrichtung von Incident Manager

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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen 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. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers 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-Managementkonsoleals 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

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

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center - Benutzerhandbuch.

Erteilen programmgesteuerten Zugriffs

Benutzer benötigen programmatischen Zugriff, wenn sie mit AWS außerhalb des interagieren möchten. AWS-Managementkonsole 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
IAM	(Empfohlen) Verwenden Sie Konsolenanmeldeinformationen als temporäre Anmeldeinformationen, um programmatische Anfragen an AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Anmeldung für AWS lokale Entwicklung im AWS Command Line Interface Benutzerhandbuch.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
		• Weitere Informationen finden Sie unter Anmeldung für AWS lokale Entwicklung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. AWS SDKs
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder AWS APIs zu signieren.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI zur Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs Tools und AWS APIs finden Sie unter IAM Identity Center-Authentifizierung im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	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 das AWS CLI AWS SDKs, oder zu signieren. AWS APIs	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen dazu AWS CLI finden Sie unter Authentifizierung mithilfe von IAM-Benutzeranmeldeinformationen im AWS Command Line Interface Benutzerhandbuch. • Informationen zu AWS SDKs und Tools finden Sie unter Authentifizieren mit langfristigen Anmeldeinformationen im Referenzhandbuch AWS SDKs und im Tools-Referenzhandbuch. • Weitere Informationen finden Sie unter Verwaltung von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch. AWS APIs

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?
- Lebenszyklus von Vorfällen 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 Schnellinstallation 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 unterKonfiguration des Incident Manager-Replikationssatzes.

   - Um einen AWS eigenen Schlüssel zu verwenden, wählen Sie AWS Eigenen Schlüssel verwenden.
   - Um Ihren eigenen AWS KMS Schlüssel zu verwenden, wählen Sie Einen vorhandenen Schlüssel auswählen AWS 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 haben AWS KMS key, wählen Sie Create an AWS KMS key.

5. (Optional) Fügen Sie im Bereich „Tags“ dem Replikationssatz 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 Ressourcen im Incident Manager taggen.

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 Berechtigungsdetails anzeigen.

7. Wählen Sie Erstellen aus.

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

Kontakte (optional bei Get prepared)

Incident Manager kontaktiert Kontakte während eines Vorfalls. Weitere Informationen zu Kontakten finden Sie unterKontakte im Incident Manager erstellen und konfigurieren.

1. Wählen Sie Kontakt erstellen aus.
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 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.

   > **Note**
   >
   > Wir empfehlen, im Engagement-Plan mindestens zwei Kanäle 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 Ressourcen im Incident Manager taggen.

7. Um den Kontaktdatensatz zu erstellen und Aktivierungscodes an die definierten Kontaktkanäle zu senden, wählen Sie Erstellen.
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. Um weitere Kontakte hinzuzufügen, wählen Sie Kontakt erstellen und wiederholen Sie die vorherigen Schritte.

(Optional bei Get prepared) Eskalationspläne

1. Wählen Sie Eskalationsplan erstellen aus.

   Ein Eskalationsplan eskaliert während eines Vorfalls über Ihre Kontakte und stellt so sicher, dass der Incident Manager während eines Vorfalls die richtigen Ansprechpartner einsetzt. Weitere Informationen zu Eskalationsplänen finden Sie unter. Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in 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 für Eskalationskanäle die Kontaktkanäle aus, auf die Sie sich einlassen 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 Ressourcen im Incident Manager taggen.

7. Wählen Sie Eskalationsplan erstellen.

Response-Plan

> **Note**
>
> Möglicherweise müssen Sie zur Startseite von Incident Manager zurückkehren und „Vorbereiten“ wählen, um fortzufahren.

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 Incident-Tags ein oder mehrere Tags zum Reaktionsplan 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 Ressourcen im Incident Manager taggen.
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 Automatisches oder manuelles Erstellen von Vorfällen im Incident Manager.

Verwaltung von Vorfällen über Regionen hinweg AWS-Konten im Incident Manager

Sie können Incident Manager, ein Tool in, so konfigurieren AWS Systems Manager, dass es 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
- Kontoübergreifendes Incident-Management

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 bei Incident Manager in dieser Region ein Ausfall auftritt, wird der Vorfall EventBridge automatisch CloudWatch oder automatisch in einer anderen Region erstellt, in die Ihre Daten repliziert werden.

> **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 RAM verwendet gemeinsam genutzte Ressourcen, um Ressourcen zwischen Konten gemeinsam zu nutzen. In können Sie den Reaktionsplan und die Kontaktressourcen zwischen Konten gemeinsam nutzen AWS 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.

Best Practices

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 Organizations Benutzerhandbuch.
2. (Optional) Verwenden Sie Quick Setup, ein Tool in AWS Systems Manager, 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 Manager Benutzerhandbuch 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 das Konto IDs aller Anwendungskonten an. Mit dieser Rolle können Ihre Anwendungskonten den Status des Runbooks auf der Seite mit den Vorfalldetails ablesen. 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 CloudFormation Stack-Updates benötigt. Diese Informationen werden als Ergebnisse für einen Vorfall gemeldet, wenn die Funktion „Ergebnisse“ aktiviert ist. Weitere Informationen finden Sie unter Identifizierung potenzieller Ursachen für Vorfälle aus anderen Diensten als „Ergebnisse“ im 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

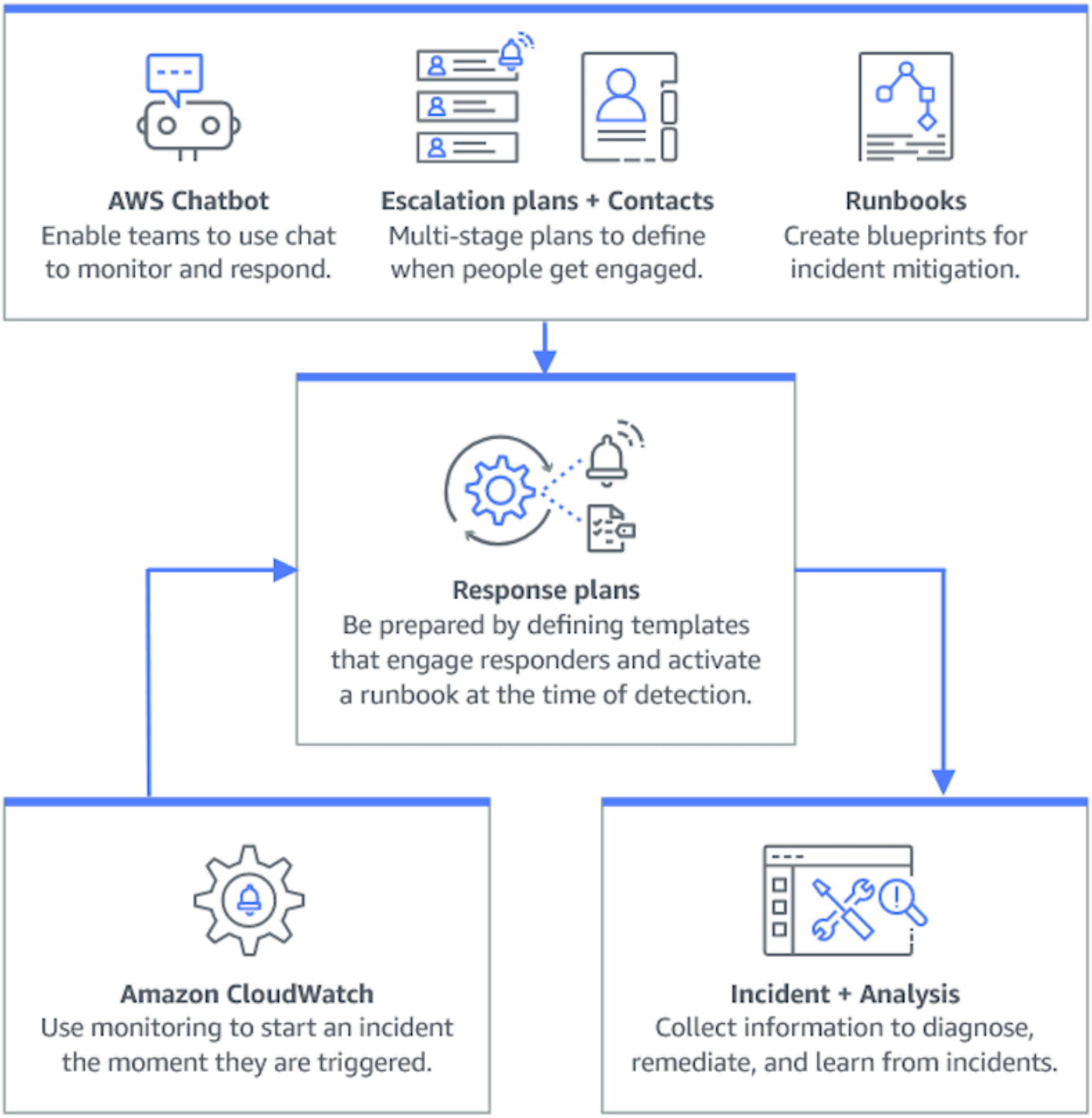
Im Folgenden sind die Einschränkungen der kontenübergreifenden Funktionalität von Incident Manager bekannt:

- 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. Wie die folgende Abbildung zeigt, bereiten Sie sich darauf vor, auf Vorfälle zu reagieren, indem Sie Chat-Kanäle einrichten, Eskalationspläne erstellen, Kontakte angeben und die Automatisierungs-Runbooks für die Reaktion auf Vorfälle festlegen. Verwenden Sie dann einen Reaktionsplan, der festlegt, wie die Überwachung erfolgt und ob die Reaktionen automatisiert werden. Nach Abschluss der Behebung können Sie den Vorfall und die Reaktion auf den Vorfall analysieren, um Ihren Reaktionsplan für future Vorfälle weiter zu verfeinern.



Topics

- Überwachen
- Konfiguration von Replikationssätzen und Ergebnissen in Incident Manager
- Kontakte im Incident Manager erstellen und konfigurieren

- Verwaltung von Responder-Rotationen mit Bereitschaftszeitplänen in Incident Manager
- Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in Incident Manager
- Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren
- Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen
- Erstellung und Konfiguration von Reaktionsplänen in Incident Manager
- Identifizierung potenzieller Ursachen für Vorfälle aus anderen Diensten als „Ergebnisse“ im 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 für die Erledigung einer Aufgabe benötigt wurde oder wurde.
- 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 unterVorfalldetails in der Incident Manager-Konsole anzeigen.

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

Konfiguration von Replikationssätzen und Ergebnissen in Incident Manager

Nachdem Sie den Incident Manager-Assistenten „Get Prepared“ 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

- Konfiguration des Incident Manager-Replikationssatzes
- Tags für einen Replikationssatz verwalten
- Verwaltung der Funktion „Ergebnisse“

Konfiguration des Incident Manager-Replikationssatzes

Das Incident Manager-Replikationsset repliziert Ihre Daten AWS-Regionen auf viele, um Folgendes zu erreichen:

- Erhöhen Sie die regionsübergreifende Redundanz
- Ermöglichen Sie Incident Manager den Zugriff auf Ressourcen in verschiedenen Regionen und reduzieren Sie die Latenz für Ihre Benutzer.
- Verschlüsseln Sie Ihre Daten entweder mit einem Von AWS verwalteter Schlüssel oder Ihrem eigenen, vom Kunden verwalteten Schlüssel.

  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.

Löschen Sie eine Region

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 den Löschschutz auf der Seite Einstellungen deaktivieren. 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.

Um die Ergebnisse kontenübergreifend unterstützen zu können, 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 unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich Roles aus.
3. Geben Sie in das Suchfeld **`IncidentManagerIncidentAccessServiceRole`** ein.
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.

Kontakte im Incident Manager erstellen und konfigurieren

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

Themen

- Kontaktkanäle
- Einsatzpläne
- So erstellen Sie einen Kontakt
- Importieren Sie Kontaktinformationen in Ihr Adressbuch

Kontaktkanäle

Kontaktkanäle sind die verschiedenen Methoden, mit denen Incident Manager Kontakt mit einem Kontakt aufnimmt.

Incident Manager unterstützt die folgenden Kontaktkanäle:

- Email
- 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 Service Benachrichtigungen über Serviceunterbrechungen oder andere Ereignisse an die im angegebenen Workflow enthaltenen Kontaktkanäle sendet. Dazu gehören auch Benachrichtigungen, die im Rahmen eines wechselnden Bereitschaftsdienstes an einen Kontakt gesendet werden. Benachrichtigungen können per E-Mail, SMS-Nachricht oder Sprachanruf gesendet werden, wie in den Kontaktdetails angegeben. Mithilfe dieser Funktionen bestätigen Sie, dass Sie berechtigt sind, die von Ihnen angegebenen Kontaktkanäle zu Incident Manager hinzuzufügen.

Abmeldung

Sie können diese Benachrichtigungen jederzeit stornieren, indem Sie ein Mobilgerät als Kontaktkanal entfernen. Einzelne Empfänger von Benachrichtigungen 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 klicken Sie auf Bearbeiten.
3. Wählen Sie neben dem Kontaktkanal, den Sie entfernen möchten, die Option Entfernen aus.
4. Wählen Sie Aktualisieren.

Deaktivierung des Kontaktkanals

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

Reaktivierung des Kontaktkanals

1. Antworten Sie mit START auf die Nachricht von Incident Manager.
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 klicken Sie auf 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.

Einsatzpläne

Engagementpläne definieren, wann Incident Manager die Kontaktkanäle aktiviert. Sie können die Kontaktkanäle ab Beginn eines Engagements in verschiedenen Phasen mehrfach nutzen. Sie können Engagementpläne in einem Eskalations- oder Reaktionsplan verwenden. Weitere Informationen zu Eskalationsplänen finden Sie unter. Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in 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 im linken Navigationsbereich Kontakte aus.
2. Wählen Sie Kontakt erstellen.

3. Geben Sie den vollständigen Namen des Kontakts und einen eindeutigen und identifizierbaren Alias ein.
4. Definieren Sie einen Kontaktkanal. Wir empfehlen, zwei oder mehr verschiedene Arten von Kontaktkanälen zu verwenden.
   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. die E-Mail-Adresse: 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 Engagement-Plan.

   > **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 Kontakts gewartet werden sollen, bis 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 aus. Incident Manager sendet einen Aktivierungscode an jeden der definierten Kontaktkanäle.
8. (Optional) Um die Kontaktkanäle zu aktivieren, geben Sie den Aktivierungscode ein, den 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 unter. Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in Incident Manager Sie können Kontakte zu einem Reaktionsplan hinzufügen, um direkt Kontakt aufzunehmen. Weitere Informationen zum Erstellen von Reaktionsplänen finden Sie unterErstellung und Konfiguration von Reaktionsplänen in Incident Manager.

Importieren Sie Kontaktinformationen in Ihr Adressbuch

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

Um die Incident Manager-.vcf-Datei herunterzuladen

1. Wählen Sie auf Ihrem Mobilgerät entweder die folgende URL 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.

Verwaltung von Responder-Rotationen mit Bereitschaftszeitplänen in Incident Manager

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

Nachdem Sie einen Bereitschaftsdienst erstellt haben, können Sie ihn als Eskalation in Ihren Eskalationsplan aufnehmen. Wenn ein mit diesem Eskalationsplan verbundener Vorfall eintritt, benachrichtigt Incident Manager den Operator (oder die Mitarbeiter), die gemäß dem Zeitplan auf Abruf sind. Dieser Ansprechpartner kann das Engagement dann bestätigen. In Ihrem Eskalationsplan können Sie einen oder mehrere Bereitschaftszeiten sowie einen oder mehrere einzelne Ansprechpartner für mehrere Eskalationsphasen festlegen. Weitere Informationen finden Sie unter Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in Incident Manager.

> **Tip**
>
> Als bewährte Methode empfehlen wir, Kontakte und Bereitschaftszeiten als Eskalationskanäle in einen Eskalationsplan aufzunehmen. Anschließend sollten Sie einen Eskalationsplan als Engagement in einem Reaktionsplan wählen. Dieser Ansatz bietet die umfassendste Abdeckung für die Reaktion auf Vorfälle in Ihrem Unternehmen.

Jeder Bereitschaftsdienst unterstützt bis zu acht Rotationen. Rotationen können sich überschneiden oder gleichzeitig ablaufen. Dies erhöht die Anzahl der Bediener, die benachrichtigt werden, um zu reagieren, wenn ein Vorfall eintritt. Sie können auch Rotationen erstellen, die nacheinander ablaufen. Dies unterstützt Szenarien wie das Incident-Management nach dem Motto „Follow the Sun“, bei dem es Gruppen auf der ganzen Welt gibt, die denselben Service unterstützen.

Mithilfe der Themen in diesem Abschnitt können Sie Bereitschaftszeitpläne für Ihre Incident-Response-Operationen erstellen und verwalten.

Themen

- Einen Bereitschaftsdienst und eine Rotation in Incident Manager erstellen
- Verwaltung eines bestehenden Bereitschaftszeitplans im Incident Manager

Einen Bereitschaftsdienst und eine Rotation in Incident Manager erstellen

Erstellen Sie einen Bereitschaftsdienst mit einer oder mehreren wechselnden Kontaktpersonen, um auf Vorfälle während der jeweiligen 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 Kontakte im Incident Manager erstellen und konfigurieren.

Berücksichtigung von Änderungen der Sommerzeit

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

Halten Sie sich zum Beispiel an unterschiedliche `America/Los_Angeles` `Europe/Dublin` Sommerzeitpläne. Infolgedessen kann der Zeitunterschied zwischen den beiden Zonen je nach Jahreszeit zwischen 6 und 8 Stunden variieren. Beispielsweise hat ein follow-the-sun Bereitschaftsdienst eine Rotation in der `America/Los_Angeles` Zeitzone und eine Rotation in

`Europe/Dublin` der Zeitzone. In diesem Beispiel kann der Zeitplan aufgrund von Änderungen der Sommerzeit eine Schichtlücke von einer Stunde oder eine Schichtüberschneidung von einer Stunde enthalten.

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

1. Verwenden Sie eine einzige Zeitzone für alle Rotationen in einem Bereitschaftsdienst.
2. Berechnen Sie die Ortszeiten, wenn Sie Einsatzkräfte außerhalb dieser bestimmten Zeitzone zuweisen.

Wenn Sie sich dafür entscheiden, jede Rotation ihrer lokalen Zeitzone zuzuweisen, überprüfen Sie den Zeitplan vor jeder Sommerzeit. Passen Sie dann die Umschaltzeiten nach Bedarf an, um sicherzustellen, dass Sie unbeabsichtigte Lücken oder Überschneidungen in Ihrem Bereitschaftsdienst vermeiden, bevor Änderungen der Sommerzeit wirksam werden.

Um einen Bereitschaftsdienst zu erstellen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Wählen Sie Bereitschaftszeitplan erstellen aus.
4. Geben Sie im Feld Name des Zeitplans einen Namen ein, anhand dessen Sie den Zeitplan leichter identifizieren können, z. B. **`MyApp Primary On-call Schedule`**
5. Geben Sie unter Zeitplan-Alias einen Alias für diesen Zeitplan ein, der im aktuellen Zeitplan eindeutig ist AWS-Region, z. **`my-app-primary-on-call-schedule`** B.
6. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere Tag-Schlüsselnamen- und Wertepaare auf den Bereitschaftsdienst 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 einen Zeitplan beispielsweise taggen, um den Zeitraum zu identifizieren, in dem er ausgeführt wird, welche Arten von Operatoren er enthält oder welchen Eskalationsplan er unterstützt. Weitere Informationen zum Markieren von Incident Manager-Ressourcen finden Sie unter. Ressourcen im Incident Manager taggen
7. Fahren Sie fort, indem Sie dem Bereitschaftsdienst eine oder mehrere Rotationen hinzufügen.

Eine Rotation für einen Bereitschaftsdienst in Incident Manager erstellen

Eine Rotation in einem Bereitschaftsdienst gibt an, wann die Schicht gültig ist. Sie legt auch fest, zwischen welchen Kontakten die Schichten rotieren. 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 unterKontakte im Incident Manager erstellen und konfigurieren.

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

Um eine Rotation für einen Bereitschaftsdienst zu erstellen

1. Geben Sie auf der Seite Bereitschaftsdienst erstellen im Abschnitt Rotation 1 unter Rotationsname einen Namen ein, der die Rotation identifiziert, z. B. **`00:00 - 7:59 Support`** oder. **`Dublin Support Group`**
2. Geben Sie unter Startdatum das Datum ein, an dem diese Rotation aktiv wird, und zwar 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 dient, die Sie für diese Rotation angeben.

   Sie können jede Zeitzone verwenden, die von der Internet Assigned Numbers Authority (IANA) definiert wurde. 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 einer eigenen Zeitzone basieren. Jede Änderung der Sommerzeit in den von Ihnen ausgewählten Zeitzonen kann sich jedoch auf Ihre geplanten Versorgungsfenster auswirken. Weitere Informationen finden Sie weiter oben in diesem Thema unter Berücksichtigung von Änderungen der Sommerzeit (DST).

4. Geben Sie unter Startzeit der Rotation die Zeit, zu der die Schicht dieser Rotation beginnt, im `hh:mm` 24-Stunden-Format ein, 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 für die Rotation wählen, entspricht dies 08:00 Uhr in Dublin, Irland, und 13:30 Uhr in Mumbai, Indien.

5. Geben Sie für die Endzeit der Rotation die Zeit ein, zu der die Schicht dieser Rotation endet, im `hh:mm` 24-Stunden-Format, z. B. `23:59`

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

6. (Optional) Um die Dauer der Rotation auf 24 Stunden festzulegen, wählen Sie 24-Stunden-Abdeckung 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 rund um die Uhr verfügbar ist und der Schichtwechsel um 11 Uhr erfolgt, 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 Bereitschaftstarif beispielsweise die Abdeckung am Wochenende ausschließt, wählen Sie alle Tage außer Sonntag und Samstag aus.

8. Fahren Sie fort, indem Sie Kontakte zur Rotation hinzufügen.

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

Für jede Rotation in Ihrem Bereitschaftsdienst können Sie einen oder mehrere Kontakte hinzufügen, insgesamt bis zu 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 unterKontakte im Incident Manager erstellen und konfigurieren.

So fügen Sie Kontakte zu einer Rotation in einem Bereitschaftsdienst hinzu

1. Wählen Sie auf der Seite Bereitschaftsdienst 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, entspricht der Reihenfolge, in der sie im Rotationsplan zuerst aufgeführt werden. Sie können die Reihenfolge ändern, nachdem Sie Kontakte hinzugefügt haben.
3. Wählen Sie Bestätigen aus.
4. Um die Position eines Kontakts in der Reihenfolge 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 der Rotation angeben.

Geben Sie die Schichtwiederholung und die Länge der Schichten an und fügen Sie einer Rotation im Incident Manager Tags hinzu

Die Schichtwiederholung gibt an, wie oft die Kontakte in einer Rotation hin- und herwechseln, wenn sie auf Abruf sind. Die Dauer der Wiederholungen kann in einer Anzahl von Tagen, Wochen oder Monaten angegeben werden.

Um Schichtwiederholung und -länge festzulegen und einer Rotation Tags hinzuzufügen

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

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

Wenn Sie beispielsweise auswählen `Daily` und eingeben**1**, dass die Bereitschaftsschicht jedes Kontakts einen Tag dauert. Wenn Sie wählen `Weekly` und eingeben**3**, dauert die Bereitschaftsschicht jedes Kontakts drei Wochen.

2. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere Paare von Tag-Schlüsselnamen und -werten 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 eine Rotation beispielsweise taggen, um den Standort der ihr zugewiesenen Kontakte, die Art der Abdeckung, die sie bieten soll, oder den Eskalationsplan, den sie unterstützt, zu identifizieren. Weitere Informationen zur Kennzeichnung von Incident Manager-Ressourcen finden Sie unter. Ressourcen im Incident Manager taggen
3. (Empfohlen) Verwenden Sie die Kalendervorschau, um sicherzustellen, dass Ihr Bereitschaftsdienst nicht unbeabsichtigt unterbrochen wird.
4. Wählen Sie Erstellen aus.

Sie können den Bereitschaftsdienst jetzt als Eskalationskanal zu einem Eskalationsplan hinzufügen. Weitere Informationen finden Sie unter Erstellen Sie einen Eskalationsplan.

Verwaltung eines bestehenden Bereitschaftszeitplans im Incident Manager

Mithilfe der Inhalte in diesem Abschnitt können Sie mit bereits erstellten Bereitschaftszeitplänen arbeiten.

Themen

- Details zum Bereitschaftsdienst anzeigen
- Einen Bereitschaftsplan bearbeiten
- Einen Bereitschaftszeitplan kopieren
- Einen Override für eine Rotation im Bereitschaftsdienst erstellen
- Löschen eines Bereitschaftszeitplans

Details zum Bereitschaftsdienst anzeigen

Eine at-a-glance Zusammenfassung eines Bereitschaftszeitplans finden Sie auf der Seite Details zum Bereitschaftsdienst 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 einem bestimmten Zeitpunkt in Rufbereitschaft sind.

Um Details zum Bereitschaftsdienst einzusehen

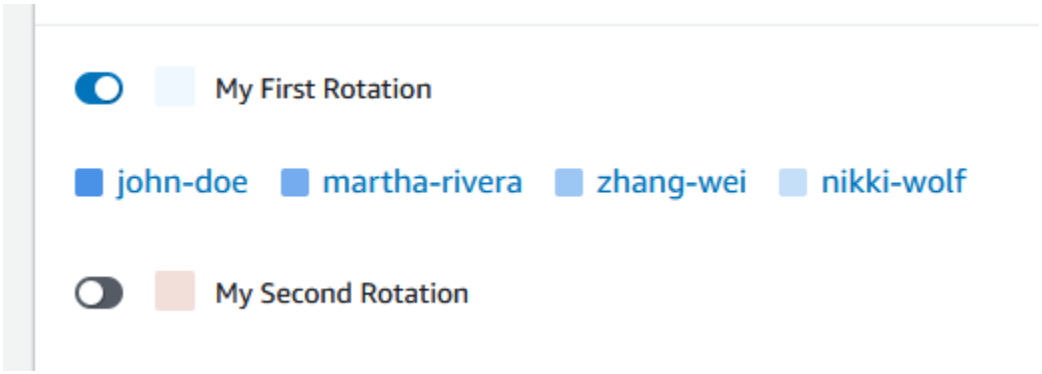
1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Führen Sie in der Zeile, in der der Zeitplan für den Bereitschaftsdienst angezeigt werden soll, einen der folgenden Schritte aus:

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

     –oder–

     Wählen Sie das Optionsfeld für die Zeile aus und wählen Sie dann Ansicht aus.
   - 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 zu erstellen,.
   - Um die Anzeige einer bestimmten Rotation im Kalender ein- oder auszuschalten, klicken Sie auf den Schalter neben dem Namen der Rotation.



Einen Bereitschaftsplan bearbeiten

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

- Der Alias für den Zeitplan

- Namen der Rotationen
- 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 Bereitschaftszeitplan kopieren.

Um einen Bereitschaftsdienst zu bearbeiten

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie das Optionsfeld in der Zeile für den Bereitschaftsdienst, den Sie bearbeiten möchten, und wählen Sie dann Bearbeiten aus.
   - Wählen Sie den Zeitplan-Alias für den Bereitschaftszeitplan, um die Seite mit den Details zum Bereitschaftsdienst anzeigen zu öffnen, und klicken Sie dann auf Bearbeiten.
4. Nehmen Sie alle erforderlichen Änderungen am Bereitschaftszeitplan und seinen Rotationen vor. Sie können die Konfigurationsoptionen für die Rotation ändern, z. B. die Start- und Endzeiten, Kontakte und Wiederholungen. Sie können dem Zeitplan nach Bedarf Rotationen hinzufügen oder daraus entfernen. In der Kalendervorschau werden Ihre Änderungen angezeigt, während Sie sie vornehmen.

   Informationen zum Arbeiten mit den Optionen auf der Seite finden Sie unterEinen Bereitschaftsdienst und eine Rotation in Incident Manager erstellen.
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 Ihnen, Ihre Schichtüberschreibungen nach der Aktualisierung des Zeitplans genau zu überprüfen.

Einen Bereitschaftszeitplan kopieren

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

Um einen Bereitschaftsdienst zu kopieren

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Wählen Sie das Optionsfeld in der Zeile aus, in der der Bereitschaftszeitplan kopiert werden soll.
4. Wählen Sie die Option 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.

   Informationen zum Arbeiten mit den Optionen auf der Seite finden Sie unterEinen Bereitschaftsdienst und eine Rotation in Incident Manager erstellen.
6. Wählen Sie Create & Copy (Erstellen und Kopieren).

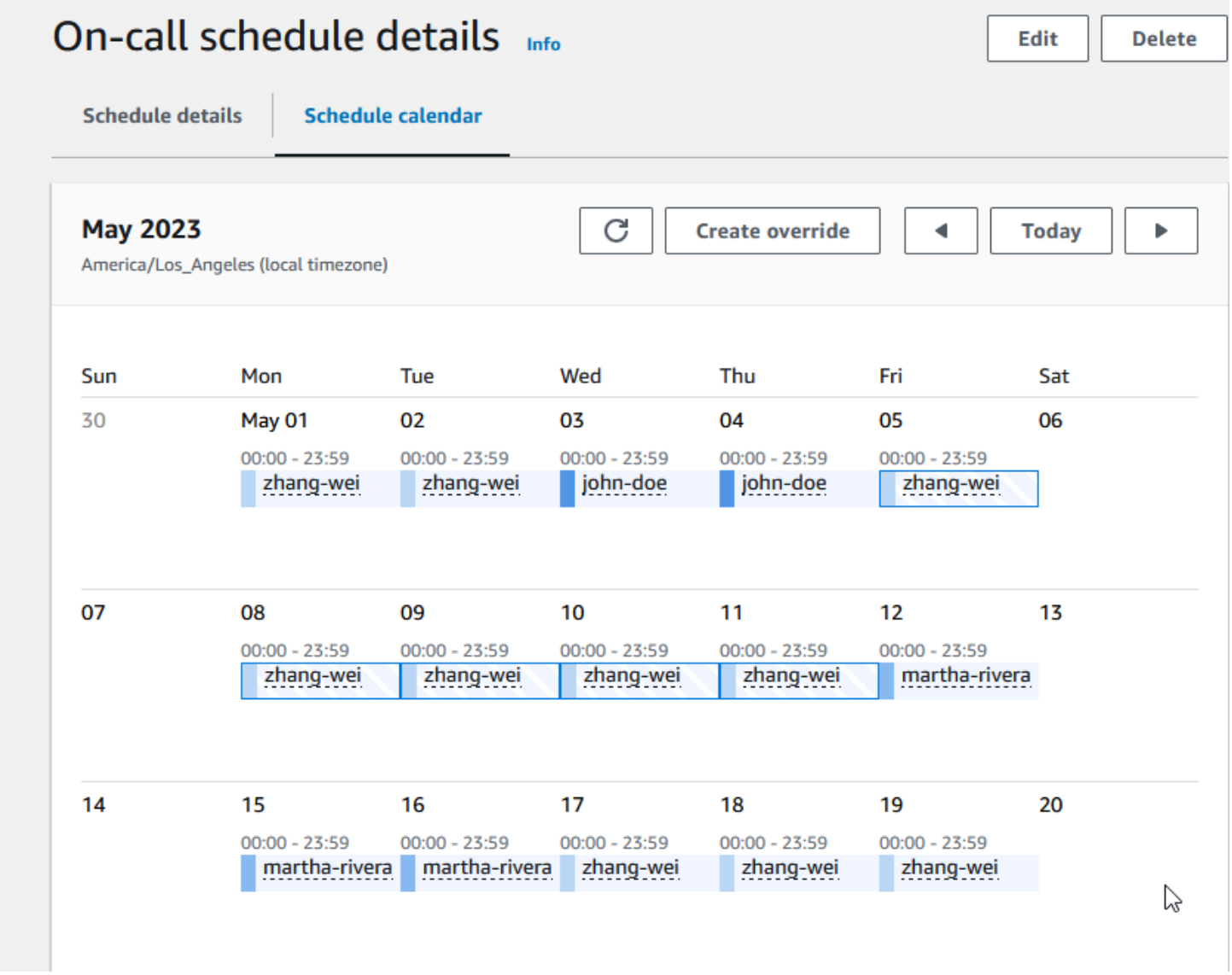
Einen Override für eine Rotation im Bereitschaftsdienst erstellen

Wenn Sie einmalig Änderungen an einem bestehenden Rotationsplan vornehmen müssen, können Sie einen Override erstellen. Mit einer Überschreibung 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 einer Override nur Kontakte zuweisen, die bereits der Rotation zugewiesen sind.

In der Kalendervorschau werden überschriebene Schichten mit einem gestreiften Hintergrund statt mit einem einfarbigen Hintergrund angezeigt. Die folgende Abbildung zeigt, dass der Kontakt mit dem

Namen Zhang Wei im Bereitschaftsdienst ist. Die Überschreibung umfasst Teile der Schichten für John Doe und Martha Rivera, die am 5. Mai beginnen und am 11. Mai enden.



Um eine Überschreibung für einen Bereitschaftsdienst zu erstellen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Führen Sie in der Zeile, in der der Zeitplan für den Bereitschaftsdienst angezeigt werden soll, einen der folgenden Schritte aus:
   - Wählen Sie den Zeitplan-Alias und anschließend den Tab Terminkalender.
   - Wählen Sie „Kalender anzeigen“

4. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie „Überschreibung erstellen“.
   - Wählen Sie in der Kalendervorschau den Namen eines Kontakts aus und wählen Sie dann „Schicht überschreiben“.
5. Gehen Sie im Dialogfeld „Schichtüberschreibung erstellen“ wie folgt vor:

   > **Note**
   >
   > Eine Überschreibung muss mindestens 30 Minuten dauern. Sie können eine Überschreibung nur für Schichten angeben, die nicht länger als sechs Monate in der future liegen.

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

Nachdem Sie eine Überschreibung erstellt haben, können Sie sie anhand ihres gestreiften Hintergrunds identifizieren. Wenn Sie den Kontaktnamen für eine überschriebene Schicht wählen, wird sie in einem Informationsfeld als überschriebene Schicht gekennzeichnet. Sie können „Überschreibung löschen“ wählen, um ihn zu entfernen und den ursprünglichen Bereitschaftsdienst wiederherzustellen.

Löschen eines Bereitschaftszeitplans

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

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

Um einen Bereitschaftsdienst zu löschen

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie in der linken Navigationsleiste die Option Bereitschaftszeiten aus.
3. Wählen Sie das Optionsfeld in der Zeile aus, in der der Bereitschaftsdienst gelöscht werden soll.
4. Wählen Sie Löschen aus.
5. Im Bereich Bereitschaftsdienst löschen? Geben Sie **`confirm`** in das Textfeld ein.
6. Wählen Sie Löschen aus.

Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in Incident Manager

AWS Systems Manager Incident Manager bietet Eskalationspfade über Ihre definierten Ansprechpartner oder Bereitschaftszeitpläne, die zusammen als Eskalationskanäle bezeichnet werden. Sie können mehrere Eskalationskanäle gleichzeitig in einen Vorfall einbeziehen. Wenn die angegebenen Kontakte im Eskalationskanal nicht antworten, eskaliert Incident Manager an die nächste Kontaktgruppe. Sie können auch festlegen, ob ein Plan nicht mehr eskaliert, sobald ein Benutzer das Engagement bestätigt hat. Sie können einem Reaktionsplan Eskalationspläne hinzufügen, sodass die Eskalation automatisch zu Beginn eines Vorfalls beginnt. Sie können einem aktiven Vorfall auch Eskalationspläne hinzufügen.

Topics

- Stufen
- Erstellen Sie einen Eskalationsplan

Stufen

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

- Dauer — Die Zeitspanne, für 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 einziger Ansprechpartner oder ein Bereitschaftsdienst, der sich aus mehreren Kontakten zusammensetzt, deren Zuständigkeiten nach einem festgelegten Zeitplan wechseln. Der Eskalationsplan bezieht jeden Kanal anhand seines definierten Engagementplans ein. Sie können jeden Eskalationskanal so einrichten, dass die weitere Umsetzung des Eskalationsplans gestoppt wird, bevor er zur nächsten Phase übergeht. Jede Phase kann mehrere Eskalationskanäle haben.

  Informationen zum Einrichten einzelner Kontakte finden Sie unterKontakte im Incident Manager erstellen und konfigurieren. Informationen zum Erstellen von Bereitschaftszeitplänen finden Sie unterVerwaltung von Responder-Rotationen mit Bereitschaftszeitplänen in Incident Manager.

Erstellen Sie einen Eskalationsplan

1. Öffnen Sie die Incident Manager-Konsole und wählen Sie in der linken Navigationsleiste Eskalationspläne aus.
2. Wählen Sie Eskalationsplan erstellen aus.
3. Geben Sie unter Name einen eindeutigen Namen für den Eskalationsplan ein, z. B. **`My Escalation Plan`**
4. Geben Sie für Alias einen Alias ein, um den Plan leichter identifizieren zu können, z. B. **`my-escalation-plan`**
5. Geben Sie für Phasendauer die Anzahl der Minuten ein, die Incident Manager warten soll, bis er zur nächsten Phase übergeht.
6. Wählen Sie unter Eskalationskanal einen oder mehrere Ansprechpartner oder Bereitschaftszeiten aus, mit denen Sie in dieser Phase Kontakt aufnehmen möchten.
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 Phase hinzuzufügen, wählen Sie Phase hinzufügen.

10. Wiederholen Sie die Schritte 5 bis 9, bis Sie alle gewünschten Eskalationskanäle und Stufen für diesen Eskalationsplan hinzugefügt haben.
11. (Optional) Wenden Sie im Bereich „Tags“ ein oder mehrere Tag-Schlüsselnamen- und Wertepaare 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 einen Eskalationsplan beispielsweise taggen, um zu ermitteln, für welche Art von Vorfällen er verwendet werden soll, welche Arten von Eskalationskanälen er enthält oder welchen Eskalationsplan er unterstützt. Weitere Informationen zur Kennzeichnung von Incident Manager-Ressourcen finden Sie unter. Ressourcen im Incident Manager taggen
12. Wählen Sie Eskalationsplan erstellen aus.

Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren

Incident Manager, ein Tool in AWS Systems Manager, bietet Einsatzkräften die Möglichkeit, während eines Vorfalls direkt über Chat-Kanäle zu kommunizieren. Ein Chat-Kanal ist ein Chatroom, den Sie in Amazon Q Developer in Chat-Anwendungen einrichten. 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. Der Incident Manager leitet außerdem alle Updates und Benachrichtigungen über den Vorfall direkt an den Chat-Kanal weiter. Es sendet diese Benachrichtigungen mithilfe eines oder mehrerer Amazon Simple Notification Service (Amazon SNS) -Themen, die Sie in Ihrer Chatroom-Konfiguration angeben.

Amazon Q Developer in Chat-Anwendungen und Incident Manager unterstützen Chat-Kanäle in den folgenden Anwendungen:

- Slack
- Microsoft Teams
- Amazon Chime

Der Prozess zur Einrichtung eines Chat-Kanals für Ihre Vorfälle 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: Einen Chat-Kanal in Amazon Q Developer in Chat-Anwendungen erstellen
- Aufgabe 3: Fügen Sie den Chat-Kanal zu einem Reaktionsplan in Incident Manager hinzu
- 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 Verlagen an Abonnenten (auch bekannt als Produzenten und Verbraucher) 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. Es hat sich bewährt, in jedem AWS-Region , den Sie zu Ihrem Replikationssatz hinzugefügt haben, ein SNS-Thema zu erstellen.

> **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 Thema Creating an Amazon SNS im Amazon Simple Notification Service Developer Guide.

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

2. Wählen Sie das von Ihnen erstellte Thema aus und notieren oder kopieren 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 Statement-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 den *placeholder values* Text 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 des Themas AWS-Konto , in dem Sie gerade arbeiten, z. `111122223333` B.
5. Wählen Sie Änderungen speichern aus.
6. Wiederholen Sie den Vorgang in jeder Region, die in Ihrem Replikationssatz enthalten ist.

Aufgabe 2: Einen Chat-Kanal in Amazon Q Developer in Chat-Anwendungen erstellen

Sie können einen Chat-Kanal in SlackMicrosoft 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 Ihres Amazon Q-Entwicklers in den Chat-Kanälen von Chat-Anwendungen überprüfen. Mithilfe von Bewertungen können Sie sicherstellen, dass nur die entsprechenden Antwortenden und andere Beteiligte Zugriff auf Ihre Chat-Kanäle haben.

In Slack Kanälen und Microsoft Teams Kanälen, die in Amazon Q Developer in Chat-Anwendungen erstellt wurden, können Incident Responder eine Reihe von Incident Manager-CLI-Befehlen direkt aus der Slack Microsoft Teams OR-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 den Chat-Kanälen auch weitere Benutzer hinzufügen, z. B. Interessenvertreter und Vorfallbeobachter.

Allgemeine Informationen zu Amazon Q Developer in Chat-Anwendungen finden Sie unter Was ist Amazon Q Developer in Chat-Anwendungen im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

Wählen Sie aus den folgenden Anwendungen, in denen Sie Ihren Kanal erstellen möchten:

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 Ihre Incident-Responder den Vorfall direkt vom Slack Chat-Kanal aus aktualisieren und mit ihm interagieren. Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

Um einen Chat-Kanal zu erstellen in Slack

- Folgen Sie den Schritten unter Tutorial: Erste Schritte mit“ Slack im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen und nehmen Sie Folgendes in Ihre Konfiguration auf.
  - 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-Richtlinien für 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 Benachrichtigungen über Vorfälle an den Chat-Kanal zu senden.
  - Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen aus 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 vom Microsoft Teams Chat-Kanal aus aktualisieren und mit ihm interagieren. Weitere Informationen finden Sie unter Interaktion über den Chat-Kanal.

Um einen Chat-Kanal zu erstellen in Microsoft Teams

- Folgen Sie den Schritten unter Tutorial: Erste Schritte mit“ Microsoft Teams im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen und nehmen Sie Folgendes in Ihre Konfiguration auf:
  - 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-Richtlinien für 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 Benachrichtigungen über Vorfälle an den Chat-Kanal zu senden.
- Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen aus 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 Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen und nehmen Sie Folgendes in Ihre Konfiguration auf:
  - 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 Benachrichtigungen über Vorfälle an den Chat-Kanal zu senden.
    - Wählen Sie für jede weitere Region in Ihrem Replikationssatz die Option Weitere Region hinzufügen aus und fügen Sie die zusätzlichen Regionen und SNS-Themen hinzu.

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

Aufgabe 3: Fügen Sie den Chat-Kanal zu einem Reaktionsplan in Incident Manager hinzu

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

Wenn Sie den Schritten unter folgenErstellung eines Reaktionsplans, wählen Sie für den Abschnitt 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 ermöglicht Incident Manager den EinsatzkräftenMicrosoft Teams, mithilfe der folgenden `ssm-incidents` Befehle direkt vom Chat-Kanal aus mit Vorfällen zu interagieren:

- Vorfall 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. *`cli-options`*Ersetzen Sie es 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
```

Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen

Sie können Runbooks von AWS Systems Manager Automation, einem Tool in, verwenden AWS Systems Manager, um allgemeine Anwendungs- und Infrastrukturaufgaben in Ihrer Umgebung zu automatisieren. AWS Cloud

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 Wiederherstellung Ihrer Ressourcen zu automatisieren. AWS

In Incident Manager steuert ein Runbook die Reaktion auf Vorfälle und deren Behebung, 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 auftritt.

> **Important**
>
> Incidents, die durch ein regionsübergreifendes Failover verursacht wurden, rufen keine Runbooks auf, die in den Reaktionsplänen angegeben sind.

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

- Informationen zum Hinzufügen eines Runbooks zu einem Reaktionsplan finden Sie unter. Erstellung und Konfiguration von Reaktionsplänen in Incident Manager

- Weitere Informationen zu Runbooks finden Sie im AWS Systems Manager Benutzerhandbuch unter AWS Systems Manager Automatisierung und in der Runbook-Referenz zur AWS Systems Manager Automatisierung.
- Informationen zu den Kosten für die Verwendung von Runbooks finden Sie unter Systems Manager Manager-Preise.
- Informationen zum automatischen Aufrufen von Runbooks, wenn ein Vorfall durch einen CloudWatch Amazon-Alarm oder ein EventBridge Amazon-Ereignis ausgelöst wird, finden Sie unter Tutorial: Systems Manager Automation-Runbooks mit Incident Manager verwenden.

Themen

- Zum Starten und Ausführen von Runbook-Workflows sind IAM-Berechtigungen erforderlich
- Arbeiten mit Runbook-Parametern
- Definieren Sie ein Runbook
- Runbook-Vorlage für Incident Manager

Zum Starten und Ausführen von Runbook-Workflows sind IAM-Berechtigungen erforderlich

Incident Manager benötigt im Rahmen Ihrer Incident-Response Berechtigungen zum Ausführen von Runbooks. 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 Incident Manager die erforderlichen Berechtigungen, um auf den Workflow für das Runbook zuzugreifen und ihn zu starten.

Die Automatisierung `AssumeRole` stellt die Berechtigungen bereit, die für die Ausführung der einzelnen Befehle erforderlich sind, die im Runbook angegeben sind.

> **Note**
>
> Wenn nein angegeben `AssumeRole` ist, versucht Systems Manager Automation, die Runbook-Dienstrolle für einzelne Befehle zu verwenden. Wenn Sie keine angeben`AssumeRole`, müssen Sie der Runbook-Servicerolle die erforderlichen Berechtigungen hinzufügen. Andernfalls kann das Runbook diese Befehle nicht ausführen.

Aus Sicherheitsgründen empfehlen wir jedoch, eine separate `AssumeRole` Methode zu verwenden. Mit einer separaten `AssumeRole` Option können Sie die erforderlichen Berechtigungen einschränken, die Sie jeder Rolle hinzufügen müssen.

Weitere Informationen zur Automatisierung `AssumeRole` finden Sie unter Konfiguration des Zugriffs auf eine Servicerolle (Rolle übernehmen) für Automatisierungen 'im AWS Systems Manager Benutzerhandbuch.

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

Berechtigungen für Runbook-Servicerollen

Berechtigungen für Runbook-Dienstrollen werden über eine Richtlinie bereitgestellt, die der folgenden ähnelt.

Die erste Anweisung ermöglicht es Incident Manager, den Systems Manager `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 Ausführen von Automatisierungen in mehreren AWS-Regionen Konten.AWS Systems Manager

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:111122223333:document/{{DocumentName}}",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
```

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

Berechtigungen für die Automatisierung AssumeRole

Wenn Sie einen Reaktionsplan erstellen oder aktualisieren, können Sie aus mehreren AWS verwalteten Richtlinien wählen, die Sie an AssumeRole die von Incident Manager erstellten Richtlinien anhängen können. Diese Richtlinien bieten 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 wählen können, wenn Sie sie in der Incident Manager-Konsole erstellen. `AssumeRole`

Name der von AWS verwalteten Richtlinie	Beschreibung der Richtlinie
`AmazonSSMAutomationRole`	Erteilt dem Systems Manager Automation-Dienst Berechtigungen zur Ausführung von Aktivitäten, die in Runbooks definiert sind. Weisen Sie diese Richtlinie Administratoren und vertrauenswürdigen Hauptbenutzern zu.
`AWSIncidentManagerResolverAccess`	Erteilt Benutzern die Berechtigung, Vorfälle zu starten, anzuzeigen und zu aktualisieren. Sie können sie auch verwenden, um Ereignisse in der Kundenzeitleiste und verwandte Elemente im Incident-Dashboard 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`. Weitere Informationen finden Sie in der AWS Systems Manager Automation-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 Incident erstellt, erfasst das System die ARNs Ressourcen, die an dem Vorfall beteiligt waren. Diese Ressourcen ARNs werden dann diesem Parameter im Runbook zugewiesen.

Über zugehörige Ressourcen

Incident Manager kann Runbook-Parameterwerte mit den AWS Ressourcen füllen, die ARNs in CloudWatch Alarmen, EventBridge Ereignissen und manuell erstellten Incidents angegeben sind. In

diesem Abschnitt werden die verschiedenen Ressourcentypen beschrieben, für die Incident Manager Daten erfassen kann, ARNs wenn dieser Parameter aufgefüllt wird.

CloudWatch Alarme

Wenn aufgrund einer CloudWatch Alarmaktion ein Vorfall ausgelöst wird, extrahiert Incident Manager automatisch die folgenden Ressourcentypen aus den zugehörigen Metriken. Anschließend werden die ausgewählten Parameter mit den folgenden beteiligten Ressourcen aufgefüllt:

AWS Dienst	Ressourcentyp
Amazon DynamoDB	Globale sekundäre Indizes Streams Tabellen
Amazon EC2	Bilder Instances
AWS Lambda	Aliase für Funktionen 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 Incident Manager die ausgewählten Parameter mit der `Resources` Eigenschaft des Ereignisses. Weitere Informationen finden Sie unter EventBridgeAmazon-Veranstaltungen im EventBridge Amazon-Benutzerhandbuch.

Manuell erstellte Vorfälle

Wenn Sie mithilfe der StartIncidentAPI-Aktion einen Incident erstellen, füllt Incident Manager die ausgewählten Parameter anhand der Informationen aus dem API-Aufruf aus. Insbesondere werden Parameter mithilfe von Elementen des Typs aufgefülltINVOLVED_RESOURCE, die `relatedItems` im Parameter übergeben wurden.

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

Definieren Sie ein Runbook

Beim Erstellen eines Runbooks können Sie die hier angegebenen Schritte befolgen, oder Sie können der ausführlicheren Anleitung folgen, die im Abschnitt Arbeiten mit Runbooks im Systems Manager Manager-Benutzerhandbuch bereitgestellt wird. Wenn Sie ein Runbook mit mehreren Konten AWS-Regionen und Regionen erstellen, finden Sie weitere Informationen unter Ausführen von Automatisierungen in mehreren Konten im Systems Manager Manager-Benutzerhandbuch.

Definieren Sie ein Runbook

1. Öffnen Sie die Systems Manager Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option 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 annehmen soll. Dadurch kann das Runbook Befehle automatisch ausführen. Weitere Informationen finden Sie unter Konfiguration eines Zugriffs auf eine Servicerolle für Automatisierungsworkflows.
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 Vorfall, 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 Tags hinzu.
10. Geben Sie die Schritte ein, die das Runbook ausführen soll, 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, geben Sie das Runbook in Ihrem Verwaltungskonto für alle Anwendungskonten frei, die das Runbook während eines Vorfalls verwenden.

Teilen Sie ein Runbook

1. Öffnen Sie die Systems Manager Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option Dokumente aus.
3. Wählen Sie in der Dokumentenliste das Dokument aus, das Sie teilen möchten, und klicken Sie dann auf 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 Bearbeiten aus.
5. Um den Befehl öffentlich freizugeben, wählen Sie Public und dann die Option Save. Um den Befehl privat zu teilen, wählen Sie Privat aus, geben Sie die AWS-Konto ID ein, wählen Sie „Berechtigung hinzufügen“ und dann „Speichern“.

Runbook-Vorlage für Incident Manager

Incident Manager bietet die folgende Runbook-Vorlage, mit der Ihr Team mit der Erstellung von Runbooks in Systems Manager Automation beginnen kann. Sie können diese Vorlage unverändert

verwenden oder sie so bearbeiten, dass sie spezifische Details zu Ihrer Anwendung und Ihren Ressourcen enthält.

Suchen Sie die Incident Manager-Runbook-Vorlage

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

> **Tip**
>
> Geben Sie Text **`AWSIncidents-`** als Freitext ein, anstatt die Filteroption für das Präfix des Dokumentnamens zu verwenden.

Verwenden Sie eine Vorlage

1. Öffnen Sie die Systems Manager Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich die Option 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 Dokumente aus.
6. Wählen Sie Create automation (Automation erstellen).
7. Geben Sie einen eindeutigen und identifizierbaren Namen ein.
8. Wählen Sie die Registerkarte Editor.
9. Wählen Sie Bearbeiten aus.
10. Fügen Sie die kopierten Details in den Dokumenteditor 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 bereitstellt. Diese Schritte sind allgemein genug, um sie in den meisten Anwendungen zu verwenden, aber detailliert genug, damit die Einsatzkräfte mit der Lösung von Vorfällen beginnen können.

Erstellung und Konfiguration von 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.

Best Practices

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.

So erstellen Sie einen Reaktionsplan

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 Anzeigename einen Namen ein, der für Menschen besser lesbar ist, damit Sie den Reaktionsplan leichter identifizieren 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.

Wenn Sie Amazon Q Developer in Chat-Anwendungen verwenden, können Sie einen Kanal fürSlack, für oder für Amazon Chime erstellenMicrosoft Teams, den Sie in Ihren Reaktionsplänen verwenden können. Informationen zum Erstellen eines Chat-Kanals in Amazon Q Developer in Chat-Anwendungen finden Sie im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

> **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 unterChat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren.

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

1. Wählen Sie unter Chat-Kanal einen Chat-Kanal von Amazon Q Developer in Chat-Anwendungen aus, über den die Mitarbeiter während eines Vorfalls kommunizieren können.

   > **Tip**
   >
   > Um einen neuen Chat-Kanal in Amazon Q Developer in Chat-Anwendungen zu erstellen, 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. Fahren Sie fort, indem Sie die Ansprechpartner, Bereitschaftszeiten und Eskalationspläne auswählen, die während eines Vorfalls kontaktiert 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.

   > **Note**
   >
   > Derzeit wird die Möglichkeit, einen Kontakt, der von einem anderen Konto aus geteilt wurde, zu einem Reaktionsplan hinzuzufügen, nicht unterstützt.

2. Wählen Sie einen Eskalationsplan als Engagement in einem Reaktionsplan.

Weitere Informationen zu Kontakten und Eskalationsplänen finden Sie unter Kontakte im Incident Manager erstellen und konfigurieren und. Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in 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 Minderung von Vorfällen an

Sie können Runbooks von AWS Systems Manager Automation, einem Tool in, verwenden AWS 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. Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen

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 Existierendes 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 Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen.

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-Instances 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`*. 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 AWS verwaltete 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-Servicerolle 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. Verwaltung von Vorfällen über Regionen hinweg AWS-Konten 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 anzugeben AWS-Konto , wo der Runbook-Workflow ausgeführt werden soll.

   - Konto des Eigentümers des Reaktionsplans — Startet den Runbook-Workflow in dem AWS-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 Zugangsdaten in einem geheimen Ordner AWS Secrets Manager.
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 name/value Tag-Schlüsselpaare 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. Ressourcen im Incident Manager taggen
2. Wählen Sie Reaktionsplan erstellen aus.

Identifizierung potenzieller Ursachen für Vorfälle aus anderen Diensten als „Ergebnisse“ im 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. Jedes Ergebnis 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.

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: AWSIncident ManagerIncidentAccessServiceRolePolicy.

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 können AWS 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 CloudFormation Vorlage bereitgestellt wird, die von bereitgestellt wird AWS, wodurch die Rolle erstellt wird`IncidentManagerIncidentAccessServiceRole`.

Informationen zum Herunterladen und Bereitstellen dieser Vorlage in einem Anwendungskonto finden Sie in Schritt 4 unterVerwaltung von Vorfällen über Regionen hinweg AWS-Konten im Incident Manager.

Automatisches oder manuelles Erstellen von Vorfällen im Incident Manager

Incident Manager, ein Tool in AWS Systems Manager, hilft Ihnen dabei, Vorfälle zu verwalten und schnell darauf zu reagieren. Sie können Amazon CloudWatch und Amazon so konfigurieren EventBridge , dass automatisch Vorfälle auf der Grundlage von CloudWatch Alarmen und EventBridge Ereignissen erstellt werden. Sie können Vorfälle auch manuell auf der Seite mit der Vorfallliste oder mithilfe der StartIncidentAPI-Aktion aus dem SDK AWS CLI oder dem AWS SDK erstellen. Incident Manager dedupliziert Vorfälle, die aufgrund desselben CloudWatch Alarms oder EventBridge Ereignisses erstellt wurden, für denselben Vorfall.

Bei Vorfällen, die automatisch durch CloudWatch Alarme oder EventBridge Ereignisse ausgelöst werden, versucht Incident Manager, einen Vorfall in derselben Reihenfolge AWS-Region wie die Ereignisregel oder der Alarm zu erstellen. Falls Incident Manager in den in Ihrem Replikationssatz angegebenen Regionen nicht verfügbar ist AWS-Region, CloudWatch oder erstellen Sie den Incident EventBridge automatisch in einer der verfügbaren Regionen. Weitere Informationen finden Sie unter Verwaltung von Vorfällen über Regionen hinweg AWS-Konten im Incident Manager.

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

Wenn das System einen Vorfall erstellt, erstellt es auch ein übergeordnetes operatives Arbeitselement (OpsItem) in OpsCenter, eine Komponente von Systems Manager, und verknüpft es als verwandtes Element mit dem Vorfall. Sie können dies verwenden OpsItem , um verwandte Arbeiten und future Vorfallanalysen nachzuverfolgen. Anrufe, bei denen OpsCenter Kosten anfallen. 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 Vorfälle in anderen Fällen erzeugen, AWS-Regionen wenn Sie in Ihrem Replikationssatz mindestens zwei Regionen angegeben haben. Hinweise zur Konfiguration eines Replikationssatzes finden Sie unterErste Schritte mit Incident Manager.
- Durch ein regionsübergreifendes Failover verursachte Vorfälle rufen keine Runbooks auf, die in den Reaktionsplänen angegeben sind.

Automatisches Erstellen von Vorfällen mit Alarmen CloudWatch

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

- Der Incident Manager wurde konfiguriert und der Replikationssatz wurde erstellt. In diesem Schritt wird die mit dem Incident Manager-Dienst verknüpfte Rolle in Ihrem Konto erstellt und die erforderlichen Berechtigungen bereitgestellt.
- Ein konfigurierter Incident Manager-Reaktionsplan. Informationen zur Konfiguration von Incident Manager-Reaktionsplänen finden Sie Erstellung und Konfiguration von Reaktionsplänen in Incident Manager im Abschnitt Incident-Vorbereitung dieses Handbuchs.
- Konfigurierte CloudWatch Metriken zur Überwachung Ihrer Anwendung. Bewährte Methoden zur Überwachung finden Sie Überwachen im Abschnitt 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 Systems Manager Manager-Aktion hinzufügen aus.
3. Wählen Sie Vorfall erstellen und wählen Sie den Reaktionsplan für diesen Vorfall aus.
4. Führen Sie die verbleibenden Schritte in der Anleitung zum 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 anhand des ausgewählten Reaktionsplans einen Vorfall.

Erstellen von Vorfällen mithilfe von SaaS-Partnerereignissen

Sie können so konfigurieren EventBridge , dass Ereignisse von Software-as-a-Service (SaaS) -Partneranwendungen und -diensten empfangen werden, was die Integration von Drittanbietern ermöglicht. Nachdem Sie EventBridge die Konfiguration für den Empfang von Ereignissen von Drittanbietern konfiguriert haben, können Sie Regeln erstellen, die auf Partnerereignisse abgestimmt sind, um Vorfälle zu erzeugen. 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. Kehren Sie zur EventBridge Konsole zurück 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 Ereignissen eines SaaS-Partners ausgelöst wird

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
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 Event Bus den Event Bus aus, der diesem Partner entspricht.
6. Bei Regeltyp wählen Sie 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. Wählen Sie als Quelle für das Ereignis die Option EventBridgePartner
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 Bearbeiten, nehmen Sie Ihre Änderungen vor und wählen Sie dann Speichern.
13. Wählen Sie Weiter aus.
14. Wählen Sie unter Ziel auswählen die Option Incident Manager-Reaktionsplan und anschließend einen Reaktionsplan aus.

> **Note**
>
> Wenn Sie einen Reaktionsplan auswählen, werden alle Reaktionspläne, die Sie besitzen und die mit Ihrem Konto geteilt wurden, in der Dropdownliste Reaktionsplan angezeigt.

15. EventBridge kann die IAM-Rolle erstellen, die für die Ausführung Ihrer Regel erforderlich ist:
    - Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Eine neue Rolle für diese spezifische Ressource erstellen aus.
    - Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden).
16. Wählen Sie Weiter aus.
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 Weiter aus.
19. Überprüfen Sie Ihre Regel und wählen Sie dann Regel erstellen.

Vorfälle mithilfe von AWS Serviceereignissen erstellen

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

Erstellen Sie eine Regel, die bei Ereignissen eines AWS Dienstes ausgelöst wird

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Regeln aus.
3. Wählen Sie Regel erstellen aus.
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 Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
7. Wählen Sie Weiter aus.
8. Wählen Sie als Quelle der Veranstaltung AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.
9. Wählen Sie für Ereignismuster die Option Ereignismusterformular.
10. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
11. Wählen Sie als Dienstname den Dienst aus, der nach einem Vorfall sucht.

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 Bearbeiten aus, nehmen Sie Ihre Änderungen vor und wählen Sie dann Speichern.
13. Wählen Sie Weiter aus.
14. Wählen Sie unter Ziel auswählen die Option Incident Manager-Reaktionsplan und anschließend einen Reaktionsplan aus.

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

    - Um automatisch eine IAM-Rolle zu erstellen, wählen Sie Eine neue Rolle für diese spezifische Ressource erstellen aus.
    - Wenn Sie eine zuvor erstellte IAM-Rolle verwenden möchten, wählen Sie Use existing role (Vorhandene Rolle verwenden).
16. Wählen Sie Weiter aus.
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 Weiter aus.
19. Überprüfen Sie Ihre Regel und wählen Sie dann Regel erstellen.

Manuelles Erstellen von Vorfällen

Einsatzkräfte können einen Vorfall mithilfe der Incident Manager-Konsole mithilfe eines vordefinierten Reaktionsplans manuell verfolgen. Gehen Sie wie folgt vor, um einen Vorfall zu erstellen.

1. Öffnen Sie die Incident Manager-Konsole.
2. Wählen Sie Vorfall starten.
3. Wählen Sie für 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 den Wert „Auswirkung des Vorfalls“ ein.

Erforderliche IAM-Berechtigungen für das manuelle Starten von Incidents

Um Incidents manuell zu starten, benötigen Benutzer Berechtigungen, um auf die Incident Manager-Konsole zuzugreifen, Reaktionspläne einzusehen und Incidents zu starten. Wenn ein Benutzer einen Incident auslöst, verwendet Incident Manager Forward Access Sessions (FAS), um den `StartEngagement` Anruf als Teil von `StartIncident` zu tätigen.

Die folgende IAM-Richtlinie bietet die erforderlichen Berechtigungen zum manuellen Starten von Incidents, zum Anzeigen der Reaktionspläne, mit denen Incidents erstellt werden können, und zum Anzeigen und Bearbeiten von Incidents, nachdem sie erstellt wurden.

JSON

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

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

Diese Richtlinie umfasst die folgenden Berechtigungen:

- ssm-incidents: StartIncident — Ermöglicht Benutzern das manuelle Starten eines Incidents mithilfe der Konsole oder API. Dadurch wird aus einem Reaktionsplan ein neuer Vorfalldatensatz erstellt.
- ssm-incidents: GetResponsePlan - Ermöglicht Benutzern das Abrufen von Informationen zu einem bestimmten Reaktionsplan.
- ssm-incidents: ListResponsePlans — Ermöglicht Benutzern, alle Reaktionspläne in ihrem Konto aufzulisten.
- ssm-incidents: TagResource — Ermöglicht das Hinzufügen von Tags zu Incident Manager-Ressourcen, einschließlich Vorfällen und Reaktionsplänen.
- ssm-incidents: GetIncidentRecord — Ermöglicht Benutzern das Abrufen detaillierter Informationen zu einem bestimmten Vorfall.
- ssm-incidents: ListIncidentRecords - Ermöglicht Benutzern, alle Vorfälle in ihrem Konto aufzulisten.
- ssm-incidents: UpdateIncidentRecord — Ermöglicht Benutzern, die Details eines bestehenden Vorfalls zu aktualisieren.

- ssm-contacts: StartEngagement (mit Bedingung) — Ermöglicht Incident Manager, Interaktionen mit Kontakten zu beginnen. Die Bedingung stellt sicher, dass dies nur über den Incident Manager aufgerufen werden kann.
- ssm: CreateOpsItem (mit Bedingung) — Ermöglicht dem Incident Manager, einen OpsItem in OpsCenter zu erstellen. Die Bedingung stellt sicher, dass dies nur über den Incident Manager aufgerufen werden kann.

Der Schlüssel aws: CalledViaFirst condition stellt sicher, dass bestimmte Berechtigungen (wie`StartEngagement`) nur verwendet werden können, wenn die Anfrage über den Incident Manager-Service eingeht. Bei diesem Ansatz werden FAS anstelle von dienstbezogenen Rollen verwendet, wodurch potenzielle kontenübergreifende Anrufe, die Sicherheitsrisiken darstellen könnten, verhindert werden.

Vorfalldetails in der Incident Manager-Konsole anzeigen

AWS Systems 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.

Topics

- Die Liste der Vorfälle in der Konsole anzeigen
- Vorfalldetails in der Konsole anzeigen

Die Liste der Vorfälle in der Konsole anzeigen

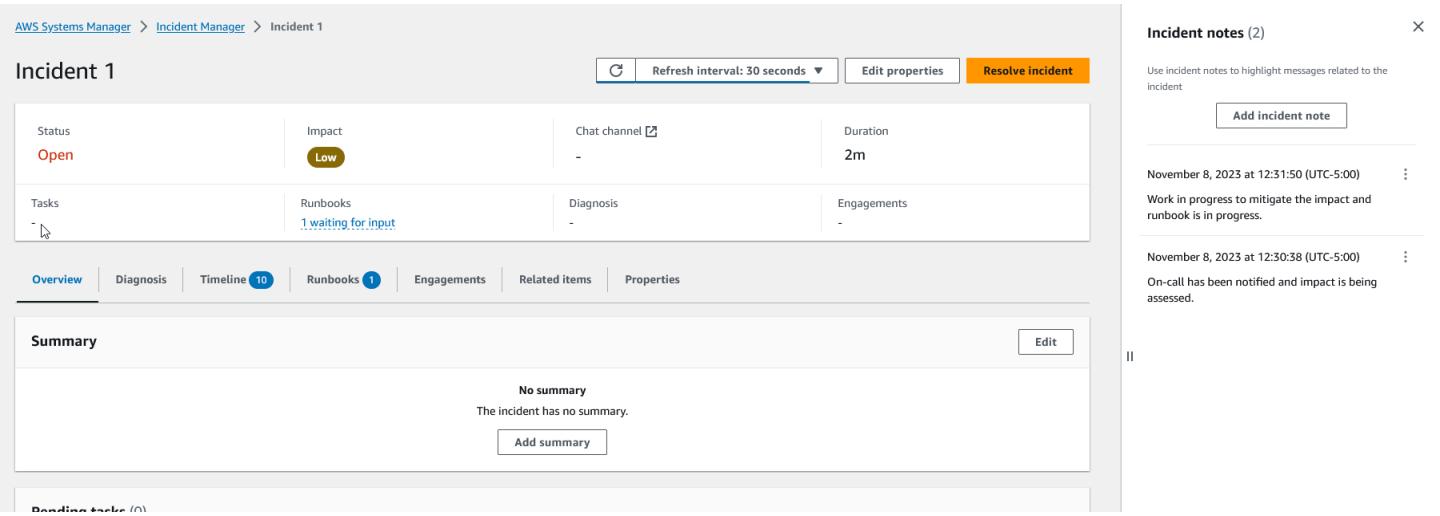
Die Seite mit der Liste der Vorfälle besteht aus drei Abschnitten: Offene Incidents, Behobene Incidents und Analysen. Auf dieser Seite können Sie neue Vorfälle manuell verfolgen und Analysen erstellen. Weitere Informationen zur manuellen Nachverfolgung eines Vorfalls finden Sie Manuelles Erstellen von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

Vorfalldetails in der Konsole anzeigen

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.

Wie in der folgenden Abbildung dargestellt, umfasst die Seite mit den Incident-Details mehrere Abschnitte: Top-Banner, Incident-Notizen und sieben Tabs mit zusätzlichen Informationen und Ressourcen. Standardmäßig werden die Abschnitte „Top-Banner“ und „Hinweise zum Vorfall“ auf allen Seiten mit den 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 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. Durchführen 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 Erstellung eines Eskalationsplans für die Einbindung von Einsatzkräften in Incident Manager Abschnitten Kontakte im Incident Manager erstellen und konfigurieren 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 Erstellung und Konfiguration von Reaktionsplänen in Incident Manager Abschnitt dieses Handbuchs.

In der Tabelle finden Sie Informationen zu den einzelnen Kontakten. 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 ARNs um Links zu externen Ressourcen oder um 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 unterRessourcen im Incident Manager taggen.

Durchführen einer Analyse nach einem Vorfall im Incident Manager

Die Analyse nach dem Vorfall führt Sie durch die Identifizierung von Verbesserungen bei der Reaktion auf Vorfälle, einschließlich der Zeit bis zur Erkennung und Behebung von Vorfällen. Eine Analyse kann Ihnen auch dabei helfen, die Grundursache der Vorfälle zu verstehen. Incident Manager erstellt Handlungsempfehlungen, um Ihre Reaktion auf Vorfälle zu verbessern.

Vorteile einer Analyse nach dem Vorfall

- Verbessern Sie die Reaktion auf Ereignisse
- Verstehen Sie die Ursache des Problems
- Beheben Sie die Grundursachen mit umsetzbaren Aktionspunkten
- Analysieren Sie die Auswirkungen von Vorfällen
- Erfassen Sie Erkenntnisse und teilen Sie sie innerhalb einer Organisation

Wofür sollte eine Analyse nicht verwendet werden

Eine Analyse ist untadelig und nennt Personen nicht beim Namen.

„Unabhängig davon, was wir herausfinden, verstehen wir und glauben fest daran, dass jeder die beste Arbeit geleistet hat, wenn man bedenkt, was er zu dem Zeitpunkt wusste, welche Fähigkeiten und Fähigkeiten er hatte, die verfügbaren Ressourcen und die aktuelle Situation.“ - Norm Kerth, Projektrückblicke: Ein Handbuch zur Überprüfung durch Teams

Einzelheiten der 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 mit einigen wichtigen Unterschieden wie historischen Kennzahlen, editierbarem 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, Dauer

und wichtige Maßnahmen, um zu verhindern, dass sich der Vorfall wiederholt. Der Überblick ist auf hohem Niveau. Weitere Einzelheiten 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 Metrikdiagramme hinzufügen, in denen eine oder mehrere Metriken im selben Diagramm 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 den wichtigsten Zeitpunkten des Vorfalls hinzuzufügen.

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

- Änderung der Bereitstellung
- Konfigurationsänderung
- Startzeit des Vorfalls
- Uhrzeit des Alarms
- Zeitpunkt der Verlobung
- Startzeit der Schadensbegrenzung
- Uhrzeit der 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 im CloudWatch Benutzerhandbuch unter Accountübergreifende CloudWatch Cross-Region-Konsole.

Zeitplan

Beschreiben Sie die wichtigsten Zeitpunkte auf der Zeitleiste, während Sie sich eingehender mit dem Vorfall befassen. Die Zeitleiste der Vorfälle wird auf dieser Registerkarte automatisch ausgefüllt.

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 der Fragen die Registerkarten Metriken und Zeitleiste, um die Genauigkeit zu erhöhen. Die Fragen konzentrieren sich auf die folgenden Hauptaspekte der Reaktion auf Vorfälle:

- Erkennung — Könnten Sie die Zeit bis zur Erkennung verkürzen? Gibt es Aktualisierungen von Metriken und Alarmen, durch die der Vorfall früher erkannt würde?
- Diagnose — Können Sie die Zeit bis zur Diagnose verkürzen? Gibt es Aktualisierungen Ihrer Reaktions- oder Eskalationspläne, mit denen die richtigen Notfallteams früher eingeschaltet werden könnten?
- Schadensbegrenzung — Können Sie die Zeit bis zur Schadensbegrenzung verkürzen? Gibt es Runbook-Schritte, die Sie hinzufügen oder verbessern könnten?
- Prävention — Können Sie verhindern, dass sich future Vorfälle ereignen? Um die Hauptursachen eines Vorfalls zu ermitteln, verwendet Amazon bei der Problemuntersuchung den 5-Whys-Ansatz.

Aktionen

Incident Manager erstellt Handlungsempfehlungen, die Sie beim Ausfüllen 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 abgelehnte Aktionspunkte überprüfen, indem Sie Abgelehnte Aktionspunkte wählen. Bei Aktionspunkten handelt es sich um einen Typ OpsItem , der mit der Analyse und dem Vorfall in verknüpft ist OpsCenter.

Checkliste

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

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

Vorlagen für Analysen

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.

AWS Standardvorlage

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

Erstellen Sie eine 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 für die Erstellung von Analysevorlagen in Ihrem Verwaltungskonto. Anschließend können Sie Ihre Analysevorlagen in jeder Region duplizieren, in der Sie Incident Manager aktiviert haben.

Erstellen Sie eine 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 API Reference.
2. Der Inhalt der Antwort enthält die JSON-Bausteine für die Analyse. Verwenden Sie die Fragebausteine, um zusätzliche Fragen in die Analyse einzufügen. Wir empfehlen, dass Sie dem `Incident questions` Abschnitt Fragen oder Abschnitte hinzufügen.
3. Um die neue Vorlage zu erstellen, verwenden Sie den `CreateDocument` Vorgang mit dem aktualisierten JSON aus dem vorherigen Schritt. Sie müssen Folgendes angeben, wo *`Analysis_Template_Name`* ist der Name Ihrer Vorlage,

   - `DocumentFormat: "JSON"`

- `DocumentType: "ProblemAnalysisTemplate"`
- `Name: "Analysis_Template_Name"`

Erstellen Sie eine Analyse

1. Um eine Analyse zu erstellen, wählen Sie auf der Seite mit den Vorfalldetails eines abgeschlossenen Vorfalls die Option Analyse erstellen aus.
2. Wählen Sie die Analysevorlage aus, aus der diese Analyse erstellt werden soll, und geben Sie einen aussagekräftigen 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 jeweils eine Analyse ausdrucken. Das Batch-Drucken mehrerer 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 in der oberen rechten Ecke der Analysedetailseite die Option Drucken aus.
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 Ihr Druckformat. Sie können einen lokalen Drucker oder einen Netzwerkdrucker wählen oder die Analyse als PDF speichern. Nehmen Sie bei Bedarf Änderungen an den übrigen 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 von dort aus zugänglich sind.

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.

Topics

- Tutorial: Systems Manager Automation-Runbooks mit Incident Manager verwenden
- Tutorial: Verwaltung von Sicherheitsvorfällen in Incident Manager

Tutorial: Systems Manager Automation-Runbooks mit Incident Manager verwenden

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
- Erstellung und Konfiguration von 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
- Aufgabe 2: Eine IAM-Rolle erstellen
- Aufgabe 3: Verbinden Sie das Runbook mit Ihrem Reaktionsplan
- Aufgabe 4: Ihrem Reaktionsplan einen CloudWatch Alarm zuordnen
- Aufgabe 5: Überprüfung der Ergebnisse

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 unter Einrichten von Automation im AWS Systems Manager -Benutzerhandbuch.

> **Important**
>
> Lesen Sie sich die folgenden wichtigen Informationen zum Erstellen des Runbooks für dieses Tutorial durch:
>
> - 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 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 unter https://console.aws.amazon.com/iam/ die IAM-Konsole.

2. Wählen Sie im Navigationsbereich Rollen und dann 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 aus.
8. Kopieren Sie die folgende Berechtigungsrichtlinie und fügen Sie sie in den JSON-Editor ein. Ersetzen Sie *`account_ID`* mit Ihrer AWS-Konto -ID.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:111122223333:document/
IncidentResponseRunbook",
                "arn:aws:ssm:*::document/AWS-RestartEC2Instance",
                "arn:aws:ssm:*:111122223333:automation-execution/*"
            ],
            "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: Tags aus.
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 IncidentRecordArnParameter 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.

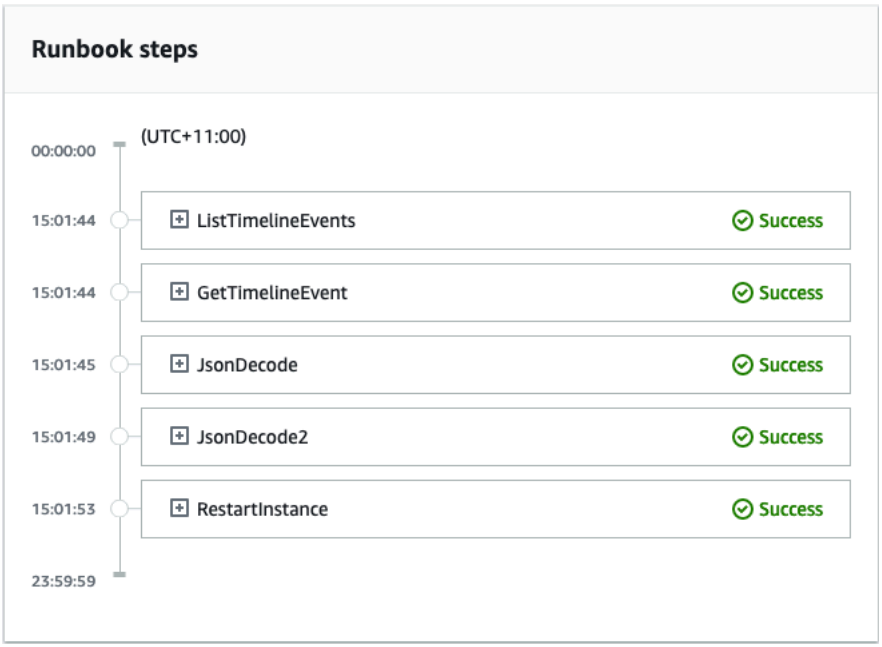
3. Wählen Sie einen Alarm für eine Amazon EC2 EC2-Instance aus, die Sie mit Ihrem Reaktionsplan verbinden möchten.
4. Wählen Sie Actions und anschließend Bearbeiten. Stellen Sie sicher, dass die Metrik eine Dimension namens `InstanceId` hat.
5. Wählen Sie Weiter aus.
6. Wählen Sie für den Assistenten 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 set-alarm-statein der AWS CLI Befehlsreferenz.

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, wie die Schritte, die das Runbook, das Sie in diesem Tutorial erstellt haben, ausgeführt hat, in der Konsole angezeigt werden. 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.

Tutorial: Verwaltung von Sicherheitsvorfällen in Incident Manager

Sie können Amazon und Incident Manager zusammen verwenden AWS Security Hub CSPM EventBridge, um Sicherheitsvorfälle in Ihren AWS gehosteten Anwendungen zu identifizieren und zu verwalten. Dieses Tutorial führt Sie durch die Konfiguration einer EventBridge Regel, die einen Vorfall auf der Grundlage der automatisch gesendeten Ergebnisse von Security Hub CSPM erstellt.

Note

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

Voraussetzungen

- Richten Sie Security Hub CSPM ein. Weitere Informationen finden Sie unter Einrichten AWS Security Hub CSPM.
- Erstellen oder aktualisieren Sie Ergebnisse in Security Hub CSPM. Weitere Informationen finden Sie unter Ergebnisse in. AWS Security Hub CSPM
- 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 CSPM 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 Regeln 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 Regeltyp wählen Sie 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 CSPM.
12. Wählen Sie als Ereignistyp Security Hub CSPM Findings — Imported aus.
13. Standardmäßig EventBridge konfiguriert das Ereignismuster ohne Filterwerte. Für jedes Attribut ist die *attribute name* Option Beliebig 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 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 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.

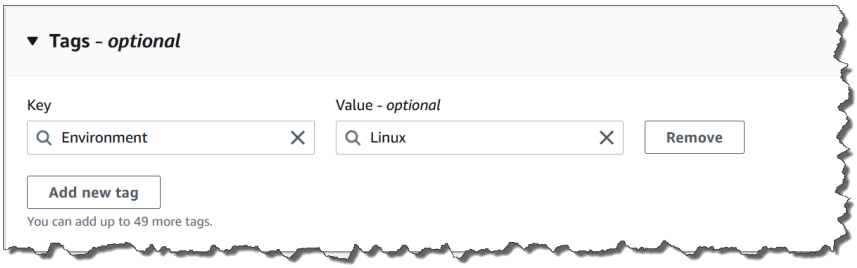
Ressourcen im Incident Manager taggen

Tags sind optionale Metadaten, die Sie Ihren Incident Manager-Ressourcen in den in Ihrem Replikationssatz AWS-Regionen angegebenen Werten zuweisen können. Sie können Reaktionsplänen, Incident-Datensätzen und Kontakten Tags zuweisen. Sie können auch Tags zu Bereitschaftszeitplänen und Rotationen hinzufügen. Sie können auch dem Replikationssatz selbst Tags hinzufügen. Mithilfe von Tags können Sie den Zugriff auf diese Ressourcen auf unterschiedliche Weise kategorisieren und steuern. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Wir empfehlen Ihnen, für jeden Incident Manager-Ressourcentyp eine Reihe von Tag-Schlüsseln zu entwickeln, die Ihren Anforderungen entsprechen. Die Verwendung eines konsistenten Satzes von Tag-Schlüsseln erleichtert Ihnen die Verwaltung dieser Ressourcen und den Zugriff auf sie. Sie können Ressourcen anhand von Stichwörtern suchen und filtern. Weitere Informationen zur Steuerung des Zugriffs auf Ressourcen mithilfe von Tags finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags im IAM-Benutzerhandbuch.

Bei der Erstellung eines Reaktionsplans können Sie im Abschnitt Incident-Standard 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 ausschließlich als Zeichenfolge interpretiert.

Mithilfe der Incident Manager-Konsole können Sie Tags hinzufügen oder entfernen. Der folgende Screenshot zeigt den Tags-Bereich einer Konsolenseite mit Feldern zum Hinzufügen von Tag-Schlüsseln und -Werten sowie Schaltflächen zum Hinzufügen und Entfernen von Tags.



Verwenden Sie die folgenden API-Aktionen, um programmgesteuert mit Tags zu arbeiten:

- TagResource

- UntagResource
- ListTagsForResource

> **Important**
>
> Tags, die auf Reaktionspläne, Vorfallaufzeichnungen, Kontakte, Bereitschaftszeitpläne 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 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.

Topics

- Datenschutz im Incident Manager
- Identity and Access Management für AWS Systems Manager Incident Manager
- Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen in Incident Manager
- Überprüfung der Einhaltung der Vorschriften für AWS Systems Manager Incident Manager
- Resilienz in AWS Systems Manager Incident Manager
- Sicherheit der Infrastruktur in AWS Systems Manager Incident Manager
- Arbeiten mit VPC-Endpunkten AWS Systems Manager Incident Manager und Schnittstellen ()AWS PrivateLink
- 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).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 AWS-Services über die Konsole, API oder arbeiten. AWS CLI AWS SDKs 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 AWS KMS key (KMS-Schlüssel) verwenden, um Ihren Replikationssatz und die Incident Manager-Daten zu verschlüsseln, sich aber später dazu entschließen, den Replikationssatz zu löschen, stellen Sie sicher, dass Sie den Replikationssatz löschen, bevor Sie den KMS-Schlüssel 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 AWS KMS key für den Incident Manager in Ihrem Konto verwendeten Incident Manager zu finden.
- Ermöglicht es Incident Manager, den KMS-Schlüssel zur Erstellung von Zuschüssen und zur Beschreibung des Schlüssels zu verwenden, jedoch nur, wenn er im Namen von Prinzipalen im Konto handelt, die über die Berechtigung zur Verwendung von Incident Manager verfügen. 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.us-east-2.amazonaws.com",
            "ssm-contacts.us-east-2.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

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Wie AWS Systems Manager Incident Manager funktioniert mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS Systems Manager Incident Manager
- Beispiele für ressourcenbasierte Richtlinien AWS Systems Manager Incident Manager
- Dienstübergreifende Vermeidung verwirrter stellvertretender Mitarbeiter in Incident Manager
- Verwenden von serviceverknüpften Rollen für Incident Manager

- AWS verwaltete Richtlinien für AWS Systems Manager Incident Manager
- Problembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Problembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie AWS Systems Manager Incident Manager funktioniert mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe 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 sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der

Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM 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 definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

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

IAM-Feature	Unterstützung durch Incident Manager
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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. 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. Weitere Informationen finden Sie unter Kontoübergreifender 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. Verwaltung von Vorfällen über Regionen hinweg AWS-Konten im Incident Manager

Beispiele für ressourcenbasierte Richtlinien in Incident Manager

Beispiele für ressourcenbasierte Richtlinien von Incident Manager finden Sie unter. Beispiele für ressourcenbasierte Richtlinien 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 Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs 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. Beispiel:

- `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 heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Incident Manager-Ressourcentypen und ihrer Eigenschaften 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 Richtlinien von Incident Manager 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 Vorfälle. Wenn ein Benutzer Zugriff auf einen Kontakt oder einen Eskalationsplan hat, kann er den Kontakt oder die Kontakte im Eskalationsplan einbeziehen.

Schlüssel zur Richtlinienbedingung für Incident Manager

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Nein

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

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Zugriffskontrolllisten (ACLs) im Incident Manager

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten 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, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, um Operationen zu ermöglichen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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 Definieren von Berechtigungen mit ABAC-Autorisierung 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

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Serviceübergreifende Prinzipalberechtigungen für Incident Manager

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen 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 Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen. Wenn Sie einen Chat-Kanal für Amazon Q Developer in Chat-Anwendungen 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 unterChat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren. Weitere Informationen zu den IAM-Richtlinien in Amazon Q Developer in Chat-Anwendungen finden Sie unter Verwaltung von Berechtigungen für die Ausführung von Befehlen mit Amazon Q Developer in Chat-Anwendungen im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

Servicebezogene 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. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

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

Einzelheiten zu den von Incident Manager definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und

Bedingungsschlüssel für AWS Systems Manager Incident Manager in der Service Authorization Reference.

Themen

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

Best Practices 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. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads 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 Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen 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. 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 mit 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices 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.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan"
      },
      {
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/
exampleplan/*"
      }
   ]
```

```
}
```

Beispiele für ressourcenbasierte Richtlinien 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 Erstellung und Konfiguration von Reaktionsplänen in Incident Manager und. Kontakte im Incident Manager erstellen und konfigurieren

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, bei dem es sich um einen AWS Organizations bestimmten Bedingungsschlüssel handelt. Weitere Informationen zu diesen Bedingungsschlüsseln finden Sie unter Bedingungen in einer Richtlinie angeben.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationAccess",
            "Effect": "Allow",
            "Principal": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-abc123def45"
                }
            },
            "Action": [
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:StartIncident",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:UpdateRelatedItems",
                "ssm-incidents:ListRelatedItems"
            ],
            "Resource": [
                "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
                "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
            ]
        }
    ]
}
```

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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
            },
```

```
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact",
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

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 angegebene dienstbezogene Rolle. AWSServiceRoleforIncidentManager Diese Rolle ermöglicht es Incident Manager, Incident Manager-Incident-Aufzeichnungen und zugehörige Ressourcen in Ihrem Namen zu verwalten.

Die AWSService RoleforIncidentManager 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: für `cloudwatch:PutMetricData` CloudWatch Metriken innerhalb der `AWS/Usage` Namespaces `AWS/IncidentManager` und

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-Managementkonsole, 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 AWSService RoleforIncidentManager serviceverknüpfte 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 AWSService RoleforIncidentManager

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 AWSService RoleforIncidentManager 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 dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, 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 vom Kunden verwaltete 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: AWSIncident ManagerIncidentAccessServiceRolePolicy

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. 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.

Weitere Einzelheiten zu dieser Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter AWSIncidentManagerIncidentAccessServiceRolePolicy im AWS Referenzhandbuch für verwaltete Richtlinien.

AWS verwaltete Richtlinie: **`AWSIncidentManagerServiceRolePolicy`**

Sie können `AWSIncidentManagerServiceRolePolicy` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, 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 der 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 und Nutzungsmetriken veröffentlichen kann.

Weitere Einzelheiten zu dieser Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter AWSIncidentManagerServiceRolePolicy im AWS Referenzhandbuch für 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 Servicerolle Amazon Q Developer in Chat-Anwendungen oder direkt Ihrer vom Kunden verwalteten Rolle zuordnen, die mit einem beliebigen Chat-Kanal verknüpft ist, der für die Zusammenarbeit bei Vorfällen verwendet wird. Weitere Informationen zu den IAM-Richtlinien in Amazon Q Developer in Chat-Anwendungen finden Sie unter Verwaltung von Berechtigungen für die Ausführung von Befehlen mit Amazon Q Developer in Chat-Anwendungen im Administratorhandbuch für Amazon Q Developer in Chat-Anwendungen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `ssm-incidents`— Ermöglicht Principals, 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 Artikel aufzulisten, verwandte Artikel zu erstellen und verwandte Artikel zu aktualisieren.
- `ssm-contacts`— Ermöglicht Principals, während der Erstellung von Incidents Interaktionen mit Kontakten aufzunehmen.

Weitere Einzelheiten zu dieser Richtlinie, einschließlich der neuesten Version des JSON-Richtliniendokuments, finden Sie unter AWSIncidentManagerResolverAccess im AWS Referenzhandbuch für verwaltete Richtlinien.

Incident Manager aktualisiert verwaltete Richtlinien AWS

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.

Änderungen	Beschreibung	Date
`AWSIncidentManagerResolverAccess` — Aktualisierung der Richtlinie	Incident Manager hat die Erlaubnis hinzugefügt, Interaktionen mit Kontakten zu beginnen.	20. November 2025
`AWSIncidentManagerServiceRolePolicy` — Aktualisierung der Richtlinie	Incident Manager hat eine neue Berechtigung hinzugefügt, die es Incident Manager ermöglicht, Metriken innerhalb des `AWS/Usage` Namespace in Ihrem Konto zu veröffentlichen.	27. Januar 2025
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
`AWSIncidentManagerIncidentAccessServiceRolePolicy` – Neue Richtlinie	Incident Manager hat eine neue Richtlinie hinzugefügt, die Incident Manager berechtigt, im Rahmen der Verwaltung eines Vorfalls	17. November 2023

Änderungen	Beschreibung	Date
	andere AWS-Services Personen anzurufen.	
AWSIncidentManagerServiceRolePolicy — Aktualisierung der Richtlinie	Incident Manager hat eine neue Berechtigung hinzugefügt, die es Incident Manager ermöglicht, Metriken in Ihrem Konto zu veröffentlichen.	16. Dezember 2022
AWSIncidentManagerResolverAccess – Neue Richtlinie	Incident Manager hat eine neue Richtlinie hinzugefügt, mit der Sie Incidents starten, Reaktionspläne auflisten, Incidents auflisten, Incidents aktualisieren, Timeline-Ereignisse auflisten, benutzerdefinierte Timeline-Ereignisse erstellen, benutzerdefinierte Timeline-Ereignisse aktualisieren, benutzerdefinierte Timeline-Ereignisse löschen, verwandte Elemente auflisten, verwandte Elemente erstellen und verwandte Elemente aktualisieren können.	26. April 2021

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

Ich bin nicht berechtigt, 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 durchzuführen: 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, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, 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 unter. Wie 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 unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Arbeiten mit gemeinsamen Kontakten und Reaktionsplänen in Incident Manager

Durch die gemeinsame Nutzung von Kontakten können Sie als Kontaktinhaber Kontaktinformationen, Eskalationspläne und Interaktionen mit anderen Personen AWS-Konten oder innerhalb einer AWS Organisation teilen.

Durch die gemeinsame Nutzung von Reaktionsplänen können Sie als Verantwortlicher für einen Reaktionsplan einen Reaktionsplan und die damit verbundenen Vorfälle mit anderen AWS-Konten oder innerhalb einer AWS Organisation teilen.

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
- Zugehörige Services
- Einen Kontakt- oder Reaktionsplan teilen
- Beenden Sie das Teilen eines geteilten Kontakt- oder Antwortplans
- Identifizieren eines gemeinsam genutzten Kontakt- oder Antwortplans
- Geteilte Kontakt- und Antwortplanberechtigungen
- Fakturierung und Messung
- Instance-Limits

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 beliebigen Personen AWS-Konto oder über diese teilen 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.

> **Note**
>
> Derzeit wird die Möglichkeit, einen Kontakt, der von einem anderen Konto aus geteilt wurde, zu einem Antwortplan hinzuzufügen, nicht unterstützt.

Um einen Kontakt oder einen Antwortplan, der Ihnen gehört, mithilfe der AWS RAM Konsole zu teilen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um einen Kontakt- oder Antwortplan, den Sie besitzen, zu teilen, verwenden Sie die 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, Engagements oder Incidents 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 die AWS CLI

Verwenden Sie die ListContactsBefehle ListResponsePlansoder. Der Befehl gibt die Kontakte und Antwortpläne 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 entsprechende 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.

Um zu erfahren, 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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

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, um Ihre Anforderungen an Datenstabilität und Datensicherung zu erfüllen. 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 unterKonfiguration des Incident Manager-Replikationssatzes.

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.

Arbeiten mit VPC-Endpunkten AWS Systems Manager Incident Manager und Schnittstellen ()AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer VPC und AWS Systems Manager Incident Manager durch die Erstellung eines Schnittstellen-VPC-Endpunkts herstellen. 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 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 Schnittstellen-VPC-Endpunkte (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 unter Verwendung unterstützter Dienstnamen für Incident Manager in Ihrem AWS-Region. Die folgenden Beispiele zeigen die Schnittstellen-Endpunktformate für IPv4 und Dual-Stack-Endpunkte.

IPv4 Endpunktformate

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

Dual-Stack IPv4 - (und IPv6) Endpunktformate

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

Eine Liste der unterstützten Endgeräte für alle Regionen finden Sie unter AWS Systems Manager Incident Manager-Endpunkte und Kontingente im AWS Allgemeinen Referenzhandbuch.

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an Incident Manager stellen, indem Sie dessen standardmäßige regionale DNS-Namen im folgenden Format verwenden. Die folgenden Beispiele zeigen das Standardformat für regionale DNS-Namen.

- `ssm-incidents.region.amazonaws.com`
- `ssm-contacts.region.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

Für Konfiguration und IT-Kontrollen sind Sie, unser Kunde, gemeinsam verantwortlich. AWS 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.

Topics

- Bewährte Methoden zur präventiven Sicherheit für Incident Manager
- Bewährte Methoden zur Detektivsicherheit für Incident Manager

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.

SlackKanäle, die in Amazon Q Developer in Chat-Anwendungen erstellt wurden, erben die Berechtigungen der IAM-Rolle, die zur Konfiguration von Amazon Q Developer in Chat-Anwendungen verwendet wird. Auf diese Weise können Responder in einem Slack Kanal, für den Amazon Q Developer in Chat-Anwendungen aktiviert ist, jede Aktion aufrufen, auf der die Zulassungsliste aufgeführt ist, z. B. den Incident Manager APIs und das Abrufen von Metrikdiagrammen.

Halten Sie die Tools auf dem neuesten Stand AWS

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 der Funktionalität aufbauen, die das AWS SDK for .NET. 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 -Ressourcengruppen -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 gesammelten Informationen können Sie die Anfrage AWS CloudTrail, die an Incident Manager gestellt wurde, 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 Protokollieren von AWS Systems Manager Incident Manager API-Aufrufen mit AWS CloudTrail.

Überwachen Sie AWS die Sicherheitshinweise

Überprüfen Sie regelmäßig die Trusted Advisor für Sie veröffentlichten Sicherheitshinweise. AWS-Konto Sie können dies programmgesteuert tun mit. describe-trusted-advisor-checks

Überwachen Sie außerdem aktiv die primäre E-Mail-Adresse, die für jeden von Ihnen registriert ist. AWS-Konten 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 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

Überwachung im Incident Manager

AWS Systems Manager Incident Manager lässt sich in die folgenden Dienste integrieren, die Überwachungs- und Protokollierungsfunktionen bieten:

CloudWatch Metriken

Verwenden Sie CloudWatch Metriken, um Statistiken über Datenpunkte für Ihre AWS Systems Manager Incident Manager-Operationen als geordneten Satz von Zeitreihendaten abzurufen, die als Metriken bezeichnet werden. Mit diesen Metriken können Sie überprüfen, ob Ihr System die erwartete Leistung zeigt. Weitere Informationen finden Sie unter Überwachung von Metriken in Incident Manager mit Amazon CloudWatch.

CloudTrail logs

Wird verwendet AWS CloudTrail , um detaillierte Informationen über die Anrufe zu erfassen AWS APIs. Sie können diese Aufrufe als Protokolldateien in Amazon Simple Storage Service speichern. Anhand dieser CloudTrail Protokolle können Sie beispielsweise ermitteln, welcher Anruf getätigt wurde, von welcher Quell-IP-Adresse der Anruf kam, wer den Anruf getätigt hat und wann der Anruf getätigt wurde. Die CloudTrail Protokolle enthalten Informationen über die Aufrufe von API-Aktionen für Incident Manager. Weitere Informationen finden Sie unterProtokollieren von AWS Systems Manager Incident Manager API-Aufrufen mit AWS CloudTrail.

Trusted Advisor

AWS Trusted Advisor kann Ihnen helfen, Ihre AWS Ressourcen zu überwachen, um Leistung, Zuverlässigkeit, Sicherheit und Wirtschaftlichkeit zu verbessern. Vier Trusted Advisor Checks stehen allen Benutzern zur Verfügung; mehr als 50 Checks stehen Benutzern mit einem Business- oder Enterprise-Supportplan zur Verfügung. Trusted Advisor Überprüft bei Incident Manager, ob die Konfiguration eines Replikationssatzes mehr als einen verwendet, AWS-Region um regionales Failover und regionale Reaktionen zu unterstützen. Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support -Benutzerhandbuch.

Überwachung von Metriken in Incident Manager mit Amazon CloudWatch

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.

Metrik	Description
`NumberOfCreateIncidents`	Anzahl der erstellten Vorfälle. 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.

Metrik	Description
	Gültige Dimensionen:] (Leere Dimension), [`ResponsePlan `], [`Impact`], [`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,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	Description
`By Response Plan`	Zeigen Sie aggregierte Kennzahlen nach Reaktionsplan an.
`By Impact Level`	Zeigen Sie aggregierte Kennzahlen nach Schweregrad an.

Dimension	Description
`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.
`Response Plan Name and Impact Level`	Zeigen Sie aggregierte Kennzahlen für jede Kombination aus Reaktionsplan und Schweregrad an.

Protokollieren von AWS Systems Manager Incident Manager API-Aufrufen mit AWS CloudTrail

AWS Systems Manager Incident Manager ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe für Incident Manager als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Incident Manager-Konsole und Code-Aufrufe an die Incident Manager-API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Incident Manager gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anforderung mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Event-Verlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS-Managementkonsole sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den

Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung.

Ereignisse zur Verwaltung von Incident Manager in CloudTrail

Managementereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. In der Standardeinstellung werden Verwaltungsereignisse CloudTrail protokolliert.

AWS Systems Manager Incident Manager protokolliert alle Operationen auf der Incident Manager-Steuerungsebene als Managementereignisse. Eine Liste der Vorgänge auf der AWS Systems Manager Incident Manager Kontrollebene, die Incident Manager protokolliert CloudTrail, finden Sie in der AWS Systems Manager Incident Manager API-Referenz.

Beispiele für Incident Manager-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

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": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```

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": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
```

```
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```


Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalte.

Produkt- und Serviceintegrationen mit Incident Manager

Incident Manager, ein Tool in AWS Systems Manager, lässt sich in die folgenden Produkte, Services und Tools integrieren.

Integration mit AWS-Services

Incident Manager lässt sich in die AWS-Services in der folgenden Tabelle beschriebenen Tools integrieren.

AWS CDK	Das AWS CDK ist ein Entwicklungsframew ork, mit dem Sie mithilfe von Code Ihre Cloud-Infrastruktur definieren und CloudFormation für die Bereitstellung verwenden können. Das AWS CDK unterstützt mehrere Programmi ersprachen TypeScript, darunter, JavaScript PythonJava, und C#/.Net. Informationen zur Verwendung von AWS CDK mit Incident Manager finden Sie in den folgenden Abschnitten der AWS CDK API-Referenz: • @aws-cdk/aws-ssmincidentsModul • @aws-cdk/aws-ssmcontactsModul
Amazon Q Developer in Chat-Anwendungen	Amazon Q Developer in Chat-Anwendungen ermöglicht es DevOps und Softwareentwicklun gsteams, Chatrooms von Messaging-Programmen zu verwenden, um betriebliche Ereignisse in ihren zu überwachen und darauf zu reagieren AWS Cloud. Wenn Sie Amazon Q Developer in Chat-Anwe ndungen mit Incident Manager verwenden, können Sie Chat-Kanäle erstellen, über die Einsatzkräfte Vorfälle überwachen und darauf

	reagieren können. Amazon Q Developer in Chat-Anwendungen unterstützt Slack Chatrooms, Microsoft Teams Kanäle und Amazon Chime Chime-Chatrooms als Chat-Kanäle. Im Rahmen 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 Verlagen an Abonnenten ermöglicht. Wenn Sie in Incident-Response-Plänen einen von Ihnen erstellten Chat-Kanal mit dem Plan verknüpfen, 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 Incident-Responder zu senden. Weitere Informationen finden Sie unter Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren.

CloudFormation	CloudFormation ist ein Dienst, mit dem Sie eine Vorlage mit allen Ressourcen erstellen können, die Sie für Ihre Anwendung benötigen, und die Ressourcen anschließend 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 CloudFormation mit Incident Manager finden Sie in den folgenden Themen im AWS CloudFormation Benutzerhandbuch: • Referenz zum Ressourcentyp von Incident Manager • Referenz zum Ressourcentyp für Kontakte Referenz zum Ressourcentyp

Amazon CloudWatch	CloudWatchüberwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können CloudWatch damit Metriken sammeln und 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 zu erstellen. CloudWatch arbeitet mit Systems Manager und Incident Manager zusammen, um anhand einer Reaktionsplanvorlage einen Vorfall zu erstellen, wenn ein Alarm in den Alarmzustand übergeht. Weitere Informationen finden Sie unter Automatisches Erstellen von Vorfällen mit Alarmen CloudWatch.
Amazon Chime	Amazon Chime ist ein Online-Arbeitsplatz, der Besprechungen, Chats und Geschäfts gespräche kombiniert. Mit Amazon Chime können Sie sich innerhalb und außerhalb Ihrer Organisation treffen, chatten und geschäftliche Anrufe tätigen. Sie können einen Amazon Chime-Raum in Ihren Incident Manager-Betrieb integrieren, indem Sie in Amazon Q Developer in Chat-Anwendungen einen Chat-Kanal für Amazon Chime erstellen und diesen Kanal dann zu einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren.

Amazon EventBridge	EventBridgeist ein serverloser Service, der Ereignisse verwendet, um Anwendung skomponenten miteinander zu verbinden , sodass Sie leichter skalierbare, ereignisg esteuerte Anwendungen erstellen können. Sie können EventBridge Regeln konfiguri eren, um nach Ereignismustern in Ihren AWS Ressourcen Ausschau zu halten und in Incident Manager einen Vorfall zu erstellen, wenn ein Ereignis einem von Ihnen definierten Muster entspricht. Mit Ihren Regeln können Sie in Dutzenden von Anwendungen AWS-Servi ces und Diensten von Drittanbietern nach Ereignismustern suchen. Weitere Informationen finden Sie unter Automatisches Erstellen von Vorfällen mit EventBridge Ereignissen.
AWS Secrets Manager	Secrets Manager hilft Ihnen dabei, Datenbank anmeldedaten, Anwendungsanmelded aten, OAuth Token, API-Schlüssel und andere Geheimnisse während ihrer gesamten Lebensdauer zu verwalten, abzurufen und zu rotieren. Wenn Sie Incident Manager in den PagerDuty Service integrieren, erstellen Sie in Secrets Manager ein Geheimnis, das Ihre PagerDuty Anmeldeinformationen enthält. Weitere Informationen finden Sie unter Speichern von PagerDuty Zugangsdaten in einem geheimen Ordner AWS Secrets Manager.

AWS Systems Manager	Systems Manager ist ein Operations Hub, mit dem Sie Ihre Anwendungsinfrastruktur anzeigen und steuern können, sowie eine sichere end-to-end Verwaltungslösung für Cloud-Umgebungen. Die folgenden Systems Manager Manager-Tools lassen sich direkt in Incident Manager integrieren: • Automatisierung — Ein Automatisierungs-Runbook definiert die Aktionen, die Systems Manager auf Ihren AWS Ressourcen ausführt. In Incident Manager definiert ein Runbook eine Reihe automatisierter und manueller Schritte, mit denen Sie Ihre Vorfälle lösen können. Informationen zum Erstellen von Automation-Runbooks für die Verwendung mit Incident Manager finden Sie unter. Integration von Systems Manager Automation-Runbooks in Incident Manager zur Behebung von Vorfällen • OpsCenter— OpsCenter bietet einen zentralen Ort, an dem Betriebsingenieure und IT-Experten betriebliche Arbeitsaufgaben verwalten können, die sich auf AWS Ressourcen beziehen. OpsItems Sie können OpsItems direkt aus einer Analyse nach einem Vorfall Daten erstellen, um damit zusammenhängende Arbeiten weiterzuverfolgen. Weitere Informationen finden Sie unter Durchführen einer Analyse nach einem Vorfall im Incident Manager.

AWS Trusted Advisor	Trusted Advisorist ein Tool, das AWS Kunden mit einem Basic- oder Developer-Supportp lan zur Verfügung steht. Trusted Advisor untersucht Ihre AWS Umgebung und gibt dann Empfehlungen, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Trusted Advisor Überprüft bei Incident Manager, ob die Konfiguration eines Replikati onssatzes mehr als einen verwendet, AWS-Region um regionales Failover und regionale Reaktionen zu unterstützen.

Integration in andere Produkte und Services

Sie können Incident Manager mit den in der folgenden Tabelle beschriebenen Drittanbieterdiensten integrieren oder zusammen verwenden.

Jira Cloud	Mithilfe von können Sie Incident Manager in Jira Cloud (Atlassian), eine cloudbasierte Workflow-Plattform eines Drittanbieters, integrieren. AWS Service Management Connector Wenn Sie nach der Konfiguration der Integrati on mit Jira Cloud einen neuen Incident in Incident Manager erstellen, erstellt die Integrati on den Incident auch in Jira Cloud. Wenn Sie einen Incident in Incident Manager aktualisi eren, werden diese Aktualisierungen auf den entsprechenden Incident in Jira Cloud angewendet. Wenn Sie einen Vorfall entweder in Incident Manager oder Jira Cloud lösen, löst die Integration den Vorfall in beiden Diensten

	auf der Grundlage der von Ihnen konfigurierten Einstellungen. Weitere Informationen findest du unter Integrieren AWS Systems Manager Incident Manager (Jira Cloud) im AWS Service Management Connector Administratorhandbuch.
Jira Service Management	Mithilfe von können Sie Incident Manager in Jira Service Management integrieren, eine cloudbasierte Workflow-Plattform eines Drittanbieters. AWS Service Management Connector Wenn Sie nach der Konfiguration der Integration mit Jira Service Management einen neuen Incident in Incident Manager erstellen, erstellt die Integration den Incident auch in Jira Service Management. Wenn Sie einen Incident Manager aktualisieren, werden diese Aktualisierungen auf den entsprechenden Incident in Jira Service Management angewendet. Wenn Sie einen Vorfall entweder in Incident Manager oder Jira Service Management lösen, löst die Integration den Vorfall in beiden Diensten auf der Grundlage der von Ihnen konfigurierten Einstellungen. Weitere Informationen finden Sie unter Konfiguration von Jira Service Management im Administratorhandbuch.AWS Service Management Connector

Microsoft Teams	Microsoft Teamsbietet kollaborative Cloud-Tools für Team-Messaging, Audio- und Videokonferenzen und Filesharing. Sie können einen Microsoft Teams Kanal in Ihren Incident Manager-Betrieb integrieren, indem Sie einen Chat-Kanal für Microsoft Team in Amazon Q Developer in Chat-Anwendungen erstellen und diesen Kanal dann zu einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren.

PagerDuty	PagerDutyist ein Tool zur Reaktion auf Vorfälle, das Paging-Workflows und Eskalationsrichtli nien unterstützt. Wenn Sie Incident Manager mit integrieren PagerDuty, können Sie Ihrem PagerDuty Reaktionsplan einen Service hinzufügen. Danach wird bei jeder Erstellung eines Vorfalls im PagerDuty Incident Manager ein entsprech ender Vorfall erstellt. Der Incident PagerDuty verwendet den Paging-Workflow und die Eskalationsrichtlinien, die Sie dort zusätzlich zu denen in Incident Manager definiert haben. PagerDutyfügt Timeline-Ereignisse aus Incident Manager als Notizen zu Ihrem Vorfall hinzu. Um Incident Manager mit zu integrieren PagerDuty, müssen Sie zunächst ein Secret in erstellen AWS Secrets Manager , das Ihre PagerDuty Anmeldeinformationen enthält. Informationen zum Hinzufügen eines PagerDuty REST-API-Schlüssels und anderer erforderl icher Details zu einem Secret in AWS Secrets Manager finden Sie unterSpeichern von PagerDuty Zugangsdaten in einem geheimen Ordner AWS Secrets Manager. Informationen zum Hinzufügen eines PagerDuty Dienstes aus Ihrem PagerDuty Konto zu einem Reaktionsplan in Incident Manager finden Sie unter den Schritten zur Integration eines PagerDuty Dienstes in den Reaktionsplan im ThemaErstellung eines Reaktionsplans.

ServiceNow	Mithilfe von können Sie Incident Manager in eine cloudbasierte Workflow-Plattform eines Drittanbieters integrieren. AWS Service Management ConnectorServiceNow Wenn Sie nach der Konfiguration der Integrati on mit ServiceNow einen neuen Incident in Incident Manager erstellen, erstellt die Integration ServiceNow auch den Incident in. Wenn Sie einen Incident in Incident Manager aktualisieren, werden diese Aktualisierungen in den entsprechenden Incident übernommen ServiceNow. Wenn Sie einen Vorfall entweder im Incident Manager oder lösen ServiceNo w, löst die Integration den Vorfall in beiden Diensten auf der Grundlage der von Ihnen konfigurierten Einstellungen. Weitere Informationen finden Sie unter Integrier en AWS Systems Manager Incident Manager ServiceNow im AWS Service Management Connector Administratorhandbuch.
Slack	Slackbietet cloudbasierte Kollaborationstool s für Team-Messaging, Audio- und Videokonf erenzen und Filesharing. Sie können einen Slack Kanal in Ihren Incident Manager-Betrieb integrieren, indem Sie einen Chat-Kanal für Slack in Amazon Q Developer in Chat-Anwendungen erstellen und diesen Kanal dann zu einem Reaktionsplan hinzufügen. Weitere Informationen finden Sie unter Chat-Kanäle für Einsatzkräfte in Incident Manager erstellen und integrieren.

Terraform	HashiCorp Terraform ist ein Open-Source-Softwaretool für Infrastructure as Code (IaC), das einen Befehlszeilenschnittstellen (CLI)-Workflow zur Verwaltung verschiedener Cloud-Services bereitstellt. Für Incident Manager können Sie Terraform verwenden, um Folgendes zu verwalten oder bereitzustellen: SSM Incident Manager: Kontakte und Ressourcen • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Datenquellen von SSM Contacts • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Ressourcen für SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan SSM Incident Manager-Datenquellen • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Speichern von PagerDuty Zugangsdaten in einem geheimen Ordner AWS Secrets Manager

Nachdem Sie die Integration mit PagerDuty für einen Reaktionsplan aktiviert haben, arbeitet Incident Manager auf folgende PagerDuty Weise mit:

- Incident Manager erstellt einen entsprechenden Incident PagerDuty , wenn Sie einen neuen Incident in Incident Manager erstellen.
- Der Paging-Workflow und die Eskalationsrichtlinien, in denen Sie erstellt haben, PagerDuty werden in der PagerDuty Umgebung verwendet. Incident Manager importiert Ihre PagerDuty Konfiguration jedoch nicht.
- Incident Manager veröffentlicht Ereignisse auf der Zeitleiste als Notizen zum Vorfall in PagerDuty bis zu 2.000 Notizen.
- Sie können festlegen, dass PagerDuty Vorfälle automatisch behoben werden, wenn Sie den entsprechenden Vorfall in Incident Manager lösen.

Um Incident Manager mit zu integrieren PagerDuty, müssen Sie zunächst ein Secret in erstellen AWS Secrets Manager , das Ihre PagerDuty Anmeldeinformationen enthält. Diese ermöglichen es Incident Manager, mit Ihrem PagerDuty Service zu kommunizieren. Anschließend können Sie einen PagerDuty Service in Reaktionspläne aufnehmen, die Sie in Incident Manager erstellen.

Dieses Geheimnis, das Sie in Secrets Manager erstellen, muss im richtigen JSON-Format Folgendes enthalten:

- Ein API-Schlüssel von Ihrem PagerDuty Konto. Sie können entweder einen REST-API-Schlüssel für allgemeinen Zugriff oder einen REST-API-Schlüssel für Benutzertoken verwenden.
- Eine gültige Benutzer-E-Mail-Adresse aus Ihrer PagerDuty Subdomain.
- Die PagerDuty Serviceregion, in der Sie Ihre Subdomain bereitgestellt haben.

> **Note**
>
> Alle Dienste in einer PagerDuty Subdomain werden in derselben Serviceregion bereitgestellt.

Voraussetzungen

Bevor Sie das Geheimnis in Secrets Manager erstellen, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen.

KMS-Schlüssel

Sie müssen das von Ihnen erstellte Geheimnis mit einem vom Kunden verwalteten Schlüssel verschlüsseln, den Sie in AWS Key Management Service (AWS KMS) erstellt haben. Sie geben diesen Schlüssel an, wenn Sie das Geheimnis erstellen, in dem Ihre PagerDuty Anmeldeinformationen gespeichert werden.

> **Important**
>
> Secrets Manager bietet die Möglichkeit, das Geheimnis 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.
- Verwendung des Schlüssels: Wählen Sie Verschlüsseln und Entschlüsseln.
- Regionalität: Wenn Sie Ihren Reaktionsplan auf mehrere replizieren möchten, stellen Sie sicher AWS-Regionen, dass Sie den Schlüssel für mehrere Regionen auswählen.

Schlüsselrichtlinie

Der Benutzer, der den Reaktionsplan konfiguriert, muss über die entsprechenden Berechtigungen für die `kms:GenerateDataKey` ressourcenbasierte `kms:Decrypt` Richtlinie des Schlüssels verfügen. Der `ssm-incidents.amazonaws.com` Dienstprinzipal muss über Berechtigungen für `kms:GenerateDataKey` und `kms:Decrypt` für die ressourcenbasierte Richtlinie des Schlüssels verfügen.

Die folgende Richtlinie veranschaulicht diese Berechtigungen. Ersetzen Sie jeden *`user input placeholder`* durch Ihre Informationen.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Informationen zum Erstellen eines neuen, vom Kunden verwalteten Schlüssels finden Sie im AWS Key Management Service Entwicklerhandbuch unter Erstellen von KMS-Schlüsseln mit symmetrischer Verschlüsselung. Weitere Informationen zu AWS KMS Schlüsseln finden Sie unter AWS KMS Konzepte.

Wenn ein vorhandener, vom Kunden verwalteter Schlüssel alle vorherigen Anforderungen erfüllt, können Sie seine Richtlinie bearbeiten, um diese Berechtigungen hinzuzufügen. Informationen zur Aktualisierung der Richtlinie in einem vom Kunden verwalteten Schlüssel finden Sie unter Ändern einer Schlüsselrichtlinie im AWS Key Management Service Entwicklerhandbuch.

> **Tip**
>
> Sie können einen Bedingungsschlüssel angeben, um den Zugriff noch weiter einzuschränken. Die folgende Richtlinie erlaubt beispielsweise den Zugriff über Secrets Manager nur 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`Erlaubnis

Die IAM-Identität (Benutzer, Rolle oder Gruppe), die den Reaktionsplan erstellt, muss über die IAM-Berechtigung verfügen. `secretsmanager:GetSecretValue`

Um die PagerDuty Zugangsdaten geheim zu speichern AWS Secrets Manager

1. Folgen Sie den Schritten bis Schritt 3a unter Create an AWS Secrets Manager Secret (Ein Geheimnis erstellen) im AWS Secrets Manager Benutzerhandbuch.
2. Gehen Sie für Schritt 3b für Schlüssel/Wert-Paare wie folgt vor:
   - Wählen Sie die Registerkarte Klartext.
   - Ersetzen Sie den Standardinhalt der Box durch die folgende JSON-Struktur:

```
{
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
}
```

- Ersetzen Sie in dem JSON-Beispiel, das Sie eingefügt haben, *placeholder values* wie folgt:

  - *pagerduty-token*: Der Wert eines REST-API-Schlüssels für allgemeinen Zugriff oder eines REST-API-Schlüssels für Benutzertoken aus Ihrem PagerDuty Konto.

    Weitere Informationen finden Sie in der PagerDuty Knowledge Base unter API-Zugriffsschlüssel.
  - *pagerduty-region*: Die Serviceregion des PagerDuty Rechenzentrums, das Ihre PagerDuty Subdomain hostet.

    Weitere Informationen finden Sie in der PagerDuty Knowledge Base unter Serviceregionen.
  - *pagerduty-email*: Die gültige E-Mail-Adresse für einen Benutzer, der zu Ihrer PagerDuty Subdomain gehört.

    Weitere Informationen finden Sie in der PagerDuty Knowledge Base unter Benutzer verwalten.

  Das folgende Beispiel zeigt einen vollständigen JSON-Secret, der die erforderlichen PagerDuty Anmeldeinformationen enthält:

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. Wählen Sie in Schritt 3c für den Verschlüsselungsschlüssel einen von Ihnen erstellten, 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 Richtlinienfeldes 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 Replicate secret wie folgt vor, wenn Sie Ihren Reaktionsplan auf mehrere repliziert haben: AWS-Region
   - Erweitern Sie Secret replizieren.
   - Wählen Sie für die Region aus AWS-Region, in die Sie Ihren Reaktionsplan repliziert haben.
   - Wählen Sie als Verschlüsselungsschlüssel einen vom Kunden verwalteten Schlüssel aus, den Sie in dieser Region erstellt oder in diese Region repliziert haben und der die im Abschnitt Voraussetzungen aufgeführten Anforderungen erfüllt.
   - Wählen Sie für jede weitere AWS-Region Region die Option Region hinzufügen und wählen Sie den Namen der Region und den vom Kunden verwalteten Schlüssel aus.
6. Führen Sie die verbleibenden Schritte unter Create an AWS Secrets Manager Secret im AWS Secrets Manager Benutzerhandbuch durch.

Informationen zum Hinzufügen eines PagerDuty Dienstes zu einem Incident Manager-Incident-Workflow finden Sie im Thema unter Integrieren eines PagerDuty Dienstes in den ReaktionsplanErstellung eines Reaktionsplans.

Ähnliche Informationen

So automatisieren Sie die Reaktion auf Vorfälle mit PagerDuty und AWS Systems Manager Incident Manager (AWS Cloud Operations and Migrations Blog)

Geheime Verschlüsselung finden Sie AWS Secrets Manager im Benutzerhandbuch AWS Secrets Manager

Problembehebung bei AWS Systems Manager Incident Manager

Wenn Sie bei der Verwendung von AWS Systems Manager Incident Manager auf Probleme stoßen, können Sie die folgenden Informationen verwenden, um diese gemäß unseren Best Practices zu lösen. Wenn die Probleme, auf die Sie stoßen, nicht in den Anwendungsbereich der folgenden Informationen fallen oder wenn sie nach dem Versuch, sie zu lösen, weiterhin bestehen, wenden AWS SupportSie sich an.

Topics

- Fehlermeldung: ValidationException – We were unable to validate the AWS Secrets Manager secret
- Fehlerbehebung bei anderen Problemen

Fehlermeldung: `ValidationException – We were unable to validate the AWS Secrets Manager secret`

Problem 1: Die AWS Identity and Access Management (IAM-) Identität (Benutzer, Rolle oder Gruppe), die den Reaktionsplan erstellt, verfügt nicht über die `secretsmanager:GetSecretValue` IAM-Berechtigung. IAM-Identitäten müssen über diese Berechtigung verfügen, um Secrets Manager zu validieren.

- Lösung: Fügen Sie die fehlende `secretsmanager:GetSecretValue` Berechtigung zur IAM-Richtlinie für die IAM-Identität hinzu, die den Reaktionsplan erstellt. Weitere Informationen finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) oder Hinzufügen von IAM-Richtlinien (AWS CLI) im IAM-Benutzerhandbuch.

Problem 2: Dem Secret ist keine ressourcenbasierte Richtlinie zugeordnet, die es der IAM-Identität ermöglicht, die `GetSecretValue`Aktion auszuführen, oder die ressourcenbasierte Richtlinie verweigert den Zugriff auf die Identität.

- Lösung: Erstellen Sie eine `Allow` Anweisung oder fügen Sie der ressourcenbasierten Richtlinie des Geheimnisses eine Erklärung hinzu, die der IAM-Identität Zugriff gewährt. `secrets:GetSecretValue` Oder, wenn Sie eine `Deny` Anweisung verwenden, die die IAM-

Identität enthält, aktualisieren Sie die Richtlinie, sodass die Identität die Aktion ausführen kann. Weitere Informationen finden Sie im AWS Secrets Manager Benutzerhandbuch unter Anhängen einer Berechtigungsrichtlinie an ein AWS Secrets Manager Geheimnis.

Problem 3: Den Geheimnissen ist keine ressourcenbasierte Richtlinie zugeordnet, die den Zugriff auf den Incident Manager-Service Principal ermöglicht. `ssm-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 Geheimnisses AWS KMS key ausgewählte Schlüssel ist kein vom Kunden verwalteter Schlüssel, oder der ausgewählte vom Kunden verwaltete Schlüssel stellt keine IAM-Berechtigungen für den Incident Manager-Service `kms:Decrypt` `kms:GenerateDataKey*` Principal bereit. Alternativ verfügt die IAM-Identität, die den Reaktionsplan erstellt, möglicherweise nicht über die IAM-Berechtigung. `GetSecretValue`

- Lösung: Stellen Sie sicher, dass Sie die im Thema unter Voraussetzungen beschriebenen Anforderungen erfüllen. Speichern von PagerDuty Zugangsdaten in einem geheimen Ordner AWS Secrets Manager

Problem 5: Die ID des Geheimnisses, das den REST-API-Schlüssel für den allgemeinen Zugriff oder den REST-API-Schlüssel für Benutzertoken enthält, ist ungültig.

- Lösung: Stellen Sie sicher, dass Sie die ID des Secrets Manager Manager-Geheimnisses korrekt und ohne Leerzeichen eingegeben haben. Sie müssen in derselben Datei arbeiten AWS-Region , die das Geheimnis speichert, das Sie verwenden möchten. Sie können ein gelöschtes Geheimnis nicht verwenden.

Problem 6: In seltenen Fällen kann ein Problem mit dem Secrets Manager Manager-Dienst auftreten, oder Incident Manager kann Probleme haben, mit ihm zu kommunizieren.

- Lösung: Warten Sie ein paar Minuten und versuchen Sie es dann erneut. Suchen Sie unter AWS Health Dashboardnach Problemen, die sich auf einen der Dienste auswirken könnten.

Fehlerbehebung bei anderen Problemen

Wenn das Problem durch die vorherigen Schritte nicht behoben wurde, finden Sie zusätzliche Hilfe in den folgenden Ressourcen:

- Informationen zu IAM-Problemen, die für Incident Manager spezifisch sind, wenn Sie auf die Incident Manager-Konsole zugreifen, finden Sie unterProblembehebung bei AWS Systems Manager Incident Manager Identität und Zugriff.
- Informationen zu allgemeinen Authentifizierungs- und Autorisierungsproblemen beim Zugriff auf AWS-Managementkonsole finden Sie unter Problembehandlung bei IAM im IAM-Benutzerhandbuch

Dokumentenverlauf für Incident Manager

Änderung	Beschreibung	Datum
AWS Systems Manager Incident Manager veröffentlichte Migrationsdokumente	Incident Manager hat Migrationsdokumente veröffentlicht, um Kunden dabei zu helfen, einige der Optionen zu verstehen, von denen aus sie migrieren können AWS Systems Manager Incident Manager. Weitere Informationen finden Sie unter Änderung der AWS Systems Manager Incident Manager Verfügbarkeit.	21. November 2025
Aktualisierung der verwalteten Richtlinie `AWSIncidentManagerResolverAccess`	Incident Manager hat die verwaltete Richtlinie aktualisiert und `AWSIncidentManagerResolverAccess` nun SSM-Kontakte hinzugefügt: die StartEngagement Erlaubnis, während eines Vorfalls Interaktionen mit Kontakten zu starten. Weitere Informationen finden Sie unter Aktualisierungen verwalteter Richtlinien durch Incident Manager. AWS	20. November 2025
AWS Systems Manager Incident Manager steht neuen Kunden nicht mehr offen.	AWS Systems Manager Incident Manager steht neuen Kunden nicht mehr offen. Bestandskunden können den Service weiterhin wie gewohnt	7. November 2025

	nutzen. Weitere Informationen finden Sie unter Änderung der AWS Systems Manager Incident Manager Verfügbarkeit.	
AWS Systems Manager Incident Manager wird ab dem 7. November 2025 nicht mehr für Neukunden geöffnet sein.	AWS Systems Manager Incident Manager wird ab dem 7. November 2025 nicht mehr für Neukunden geöffnet sein. Wenn Sie Incident Manager nutzen möchten, melden Sie sich vor diesem Datum an. Bestandskunden können den Service weiterhin wie gewohnt nutzen. Weitere Informationen finden Sie unter Änderung der AWS Systems Manager Incident Manager Verfügbarkeit.	7. Oktober 2025

Änderung der Berechtigungsanforderungen für die manuelle Erstellung von Incidents	Die IAM-Berechtigungen, die ein Benutzer für die manuelle Erstellung eines Incidents benötigt, haben sich geändert und es wird keine dienstbezogene Rolle mehr verwendet. Stattdessen verwendet Incident Manager jetzt Forward Access Sessions (FAS) für Anrufe `ssm-contacts:StartEngagement` als Teil von. `ssm-incidents:StartIncident` Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen für das manuelle Starten von Incidents.	10. Juni 2025
Aktualisierung der verwalteten Richtlinie `AWSServiceRoleforIncidentManagerPolicy`	Incident Manager hat eine neue Berechtigung hinzugefügt`AWSServiceRoleforIncidentManagerPolicy`, die es Incident Manager ermöglicht, Metriken innerhalb des `AWS/Usage` Namespace in Ihrem Konto zu veröffentlichen. Weitere Informationen finden Sie unter Incident Manager-Updates für AWS verwaltete Richtlinien.	28. Januar 2025

Aktualisierung der verwalteten Richtlinie `AWSIncidentManagerIncidentAccessServiceRolePolicy`	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. Weitere Informationen finden Sie unter Updates AWS verwalteter Richtlinien durch Incident Manager.	20. Februar 2024
Zusätzliche HashiCorp Terraform-Unterstützung: Rotationen auf Abruf	Terraform hat seine Unterstützung für Incident Manager erweitert. Mit Terraform können Sie jetzt Bereitschaftsressourcen für Incident Manager bereitstellen oder verwalten. Informationen zu dieser und anderen Integrationen von Drittanbietern mit Incident Manager finden Sie unter Integration mit anderen Produkten und Diensten.	2. Februar 2024

Neue Funktion: Erkenntnisse aus anderen AWS-Services	Die Ergebnisse bieten Ihnen Informationen zu Änderungen im Zusammenhang mit AWS CloudFormation Stacks und AWS CodeDeploy Bereitste llungen, die ungefähr zur gleichen Zeit stattfanden, als ein Incident in Incident Manager erstellt wurde. In der Incident Manager-Konsole können Sie zusammenf assende Informationen zu diesen Änderungen einsehen und in vielen Fällen auf Links zu den CodeDeploy Konsolen CloudFormation oder zugreifen, um vollständ ige Informationen zu der Änderung zu erhalten. Die Ergebnisse reduzieren den Zeitaufwand für die Bewertung potenzieller Ursachen von Vorfällen. Sie verringern auch die Wahrscheinlichkeit , dass Einsatzkräfte auf das falsche Konto oder die falsche Konsole zugreifen, um die Ursache eines Vorfalls zu untersuchen. Mit dieser Funktion wird auch eine neue verwaltete Richtlinie eingeführ t`AWSIncidentManager IncidentAccessServ iceRolePolicy` , die es Incident Manager ermöglich t, Ressourcen in anderen	15. November 2023

	Bereichen zu lesen, AWS-Services um Ergebnisse im Zusammenhang mit Vorfällen zu identifizieren. Weitere Informationen finden Sie unter den folgenden Themen: • Mit Ergebnissen arbeiten • AWS verwaltete Richtlinie: AWSIncidentManagerIncidentAccessServiceRolePolicy	
Aktualisierte Listen der Integrationen mit Incident Manager	Das Thema Produkt- und Serviceintegrationen mit Incident Manager wurde erweitert und listet und beschreibt nun alle Tools AWS-Services und Tools von Drittanbietern, die Sie mit Incident Manager in Ihre Abläufe zur Erkennung und Reaktion auf Vorfälle integrieren können.	9. Juni 2023

Integration mit AWS Trusted Advisor	Trusted Advisor prüft jetzt, ob die Konfiguration eines Replikationssatzes mehr als einen verwendet, AWS-Regio n um regionales Failover und regionale Reaktionen zu unterstützen. Für Vorfälle, die durch CloudWatch Alarme oder EventBridge Ereigniss e verursacht werden, erstellt Incident Manager einen Vorfall auf dieselbe Weise 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, wird Trusted Advisor gemeldet, wenn ein Replikationssatz nur für eine Region konfiguriert ist. Informationen zur Arbeit mit Trusted Advisor finden Sie AWS Trusted Advisorim AWS Support Benutzerhandbuch.	28. April 2023

Microsoft TeamsAls Chat-Kanal in Reaktionsplänen verwenden	Durch die Integration mit Microsoft Teams und Amazon Q Developer in Chat-Anwendungen können Sie jetzt Microsoft Teams den Chat-Kanal in Ihren Antwortplänen verwenden. Dies gilt zusätzlich zur Slack Unterstützung von Amazon Chime Chime-Chat-Kanälen. Während eines Vorfalls sendet Incident Manager Statusbenachrichtigungen direkt an einen Chat-Kanal, um alle Einsatzkräfte auf dem Laufenden zu halten. Die Einsatzkräfte können in der Microsoft Teams Anwendung auch miteinander und über AWS CLI Befehle im Zusammenhang mit Vorfällen 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

Neue Funktion: Bereitschaftszeitpläne	Ein Bereitschaftsdienst im Incident Manager legt fest, wer benachrichtigt wird, wenn ein Vorfall eintritt, der ein Eingreifen des Bedieners erfordert. Ein Bereitschaftsdienst besteht aus einer oder mehreren Rotationen, die Sie für den Zeitplan erstellen. Jede Rotation kann bis zu 30 Kontakte umfassen. Nachdem Sie einen Bereitschaftsdienst erstellt haben, können Sie ihn als Eskalation in Ihren Eskalationsplan aufnehmen. Wenn ein mit diesem Eskalationsplan verbundener Vorfall eintritt, benachrichtigt Incident Manager den Operator (oder die Mitarbeiter), die gemäß dem Zeitplan auf Abruf sind. Weitere Informationen finden Sie unter Arbeiten mit Bereitschaftszeitplänen in Incident Manager.	28. März 2023

Drucken Sie eine formatierte Vorfallanalyse aus oder speichern Sie sie als PDF	Die Seite mit der Vorfallanalyse enthält jetzt die Schaltfläche Drucken, mit der Sie eine Version der Analyse erstellen können, die für den Druck formatiert ist. Mithilfe der für Ihr Gerät konfigurierten Druckerziele können Sie die Vorfallanalyse als PDF speichern oder an einen lokalen Drucker oder Netzwerkdrucker senden. Weitere Informationen finden Sie unter Drucken einer formatierten Vorfallanalyse.	17. Januar 2023

PagerDuty Integration: Incident Manager kopiert jetzt Ereignisse in der Zeitleiste von Vorfällen in PagerDuty Vorfälle	Wenn Sie die Integration mit PagerDuty in einem Reaktionsplan aktivieren, fügt Incident Manager die anhand dieses Plans erstellten Zeitleistenereignisse dem entsprechenden Incident-Datensatz in hinzu PagerDuty. PagerDuty fügt Timeline-Ereignisse als Notizen zum Vorfall hinzu, bis zu einem Maximum von 2.000 Notizen. Weitere Informationen zu diesen Änderungen finden Sie in den folgenden Themen: • Speichern PagerDuty Sie die Zugangsdaten AWS Secrets Manager geheim • Integrieren Sie einen PagerDuty Service in den Reaktionsplan	15. Dezember 2022
Integration von Incident Manager mit CloudWatch Kennzahlen.	Sie können jetzt vorfallbezogene Metriken in veröffentlichen lassen. CloudWatch Weitere Informationen finden Sie unter Metriken. CloudWatch Dies beinhaltet AWSIncidentManagerServiceRolePolicy eine zusätzliche Genehmigung, die es unserem Service ermöglicht, Metriken in Ihrem Namen zu veröffentlichen.	15. Dezember 2022

Die Hinweise zum Vorfall wurden veröffentlicht und der Bildschirm mit den Vorfalldetails aktualisiert.	Mithilfe von Incident Notes können Sie mit anderen Benutzern, die an einem Vorfall arbeiten, zusammenarbeiten und mit ihnen kommunizieren. Darüber hinaus können Sie den Status von Runbooks und Engagements auf dem Bildschirm mit den Incident-Details einsehen. Weitere Informationen finden Sie unter Incident-Details.	16. November 2022
Die Incident-Notizen wurden veröffentlicht und der Bildschirm mit den Incident-Details aktualisiert	Mithilfe von Incident Notes können Sie mit anderen Benutzern, die an einem Vorfall arbeiten, zusammenarbeiten und mit ihnen kommunizieren. Darüber hinaus können Sie den Status von Runbooks und Engagements auf dem Bildschirm mit den Incident-Details einsehen. Weitere Informationen finden Sie unter Incident-Details.	16. November 2022

Integrieren Sie PagerDuty Eskalationspläne und Paging-Workflows in die Reaktionspläne von Incident Manager	Sie können jetzt Incident Manager in einen Reaktionsplan integrieren PagerDuty und einen PagerDuty Service zu einem Reaktionsplan hinzufügen. Nachdem Sie die Integration konfiguriert haben, kann Incident Manager PagerDuty für jeden neuen Incident, der in Incident Manager erstellt wird, einen entsprechenden Incident erstellen. 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 PagerDuty Sie die Zugangsdaten geheim AWS Secrets Manager • Integrieren Sie einen PagerDuty Service in den Reaktionsplan im Thema Erstellung eines Reaktionsplans • Fehlersuche	16. November 2022

Tagging-Unterstützung für Replikationssätze	Sie können Ihrem Replikationssatz jetzt Tags zuweisen. AWS Systems Manager Incident Manager Dies erweitert die bestehende Unterstützung für das Zuweisen von Stichwörtern zu Reaktionsplänen, Ereignisdatensätzen und Kontakten in den in Ihrem Replikationssatz AWS-Regionen angegebenen Daten. Weitere Informationen finden Sie unter den folgenden Themen: • Assistent zur Vorbereitung • Taggen von Incident Manager-Ressourcen	02. November 2022

Integration von Incident Manager mit Atlassian Jira Service Management	Du kannst Incident Manager mit Jira Service Management integrieren, indem du den Service Management Connector für Jira AWS Service Management verwendest. Nachdem Sie die Integration konfiguriert haben, erstellen neue Incidents, die in Incident Manager erstellt wurden, einen entsprechenden Incident in Jira. Wenn Sie einen Incident in Incident Manager aktualisieren, werden die Updates dem entsprechenden Incident in Jira hinzugefügt. Wenn Sie einen Vorfall entweder in Incident Manager oder in Jira lösen, wird der entsprechende Vorfall ebenfalls behoben, basierend auf den konfigurierten Einstellungen. Weitere Informationen finden Sie unter Konfiguration von Jira Service Management im AWS Service Management Connector-Administratorhandbuch.	6. Oktober 2022

Verbesserte Tagging-Unterstützung	Incident Manager unterstützt die Zuweisung von Tags zu Reaktionsplänen, Incident-Datensätzen und Kontakten in den in Ihrem Replikationssatz AWS-Regionen angegebenen Daten. Incident Manager unterstützt auch die automatische Zuweisung von Tags zu Vorfällen, die anhand von Reaktionsplänen erstellt wurden. Weitere Informationen finden Sie unter Tagging Incident Manager-Ressourcen.	28. Juni 2022

Integration von Incident Manager mit ServiceNow	Sie können Incident Manager mit integrieren, ServiceNo windem Sie den AWS Service Management Connector für verwenden ServiceNow. Nachdem Sie die Integration konfiguriert haben, erstellen neue Incidents, die in Incident Manager erstellt wurden, einen entsprechenden Incident in ServiceNow. Wenn Sie einen Incident in Incident Manager aktualisi eren, werden die Updates dem entsprechenden Vorfall in hinzugefügt ServiceNo w. Wenn Sie einen Vorfall entweder im Incident Manager oder lösen ServiceNow, wird der entsprechende Vorfall auf der Grundlage der konfigurierten Einstellungen ebenfalls behoben. Weitere Informationen finden Sie unter Integrieren von AWS Systems Manager Incident Manager in ServiceNow.	9. Juni 2022

Kontaktinformationen importieren	Wenn ein Vorfall erstellt wird, kann Incident Manager die Einsatzkräfte mithilfe von Sprach- oder SMS-Benachrichtigungen benachrichtigen. Um sicherzustellen, dass die Einsatzkräfte sehen, dass der Anruf oder die SMS-Benachrichtigung von Incident Manager stammt, empfehlen wir allen Einsatzkräften, die Incident Manager-Datei im Virtual Card-Format (.vcf) in das Adressbuch auf ihren Mobilgeräten herunterzuladen. Weitere Informationen finden Sie unter Kontaktdaten in Ihr Adressbuch importieren.	18. Mai 2022

Zahlreiche Funktionsverbesserungen zur besseren Erstellung und Behebung von Vorfällen	Incident Manager hat die folgenden Funktionsverbesserungen eingeführt, um die Erstellung und Behebung von Vorfällen zu verbessern: • Automatisch Vorfälle in anderen erstellen AWS-Regionen: Falls Incident Manager nicht 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 Regionalübergreifendes Incident Management. • Automatisches Auffüllen von Runbook-Parametern mit Incident-Metadaten : Sie können Incident Manager jetzt so konfigurieren, dass Informationen über AWS Ressourcen aus Vorfällen gesammelt werden. Incident Manager kann dann Runbook-Parameter mit den gesammelten Informationen füllen. Weitere Informationen finden Sie unter Tutorial:	17. Mai 2022

	Verwenden von Systems Manager Automation-Runbooks mit Incident Manager. • Automatisches Sammeln von AWS Ressource ninformationen: Wenn das System einen Vorfall erstellt, sammelt Incident Manager jetzt automatis ch Informationen über die am Vorfall beteiligten AWS Ressourcen. Incident Manager fügt diese Informati onen dann der Registerk arte „Verwandte Elemente“ hinzu.	
Unterstützung mehrerer Runbooks	Incident Manager unterstützt jetzt das Ausführen mehrerer Runbooks während eines Vorfalls für die Seite mit den Incident-Details.	14. Januar 2022
Incident Manager wurde neu gestartet AWS-Regionen	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 den Regionen und Allgemeine AWS-Referenz Kontingenten von Incident Manager finden Sie im Referenzhandbuch.	8. November 2021

Bestätigung des Einsatzes auf der Konsole	Sie können Anfragen jetzt direkt von der Incident Manager-Konsole aus bestätigen.	05. August 2021
Registerkarte „Eigenschaften“	Incident Manager hat auf der Seite mit den Incident-Details einen Eigenschaften-Tab eingeführt, der mehr Informationen zu den Incidents, dem übergeordneten OpsItem Ereignis und der zugehörigen Analyse nach dem Vorfall bietet.	3. August 2021
Start von Incident Manager	Incident Manager ist eine Incident-Management-Konsole, die Benutzern hilft, Vorfälle, die sich auf ihre AWS gehosteten Anwendungen auswirken, zu minimieren und diese zu beheben.	10. Mai 2021