aws

Benutzer-Leitfaden

Amazon DevOps Guru

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

Amazon DevOps Guru: Benutzer-Leitfaden

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

Die Handelsmarken und die 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 Amazon DevOps Guru? 1
Wie funktioniert DevOps Guru? 1
DevOpsGuru-Arbeitsablauf auf hohem Niveau 2
Detaillierter DevOps Guru-Arbeitsablauf 4
Was sind die ersten Schritte? 5
Wie kann ich verhindern, dass Guru-Gebühren anfallen? DevOps 5
Konzepte 6
Anomalie 6
Insight 6
Kennzahlen und betriebliche Ereignisse 7
Gruppen protokollieren und Anomalien protokollieren 7
Empfehlungen 8
Abdeckung 8
Liste der Serviceabdeckungen 10
Ende des Supports für Amazon DevOps Guru 12
-Übersicht 12
Servicestatus bis 30. September 2027 12
Was passiert mit Ihren Ressourcen nach dem 30. September 2027 12
Was bedeutet das für dich 13
Den richtigen Migrationspfad wählen 13
Alternative Lösungen 14
Amazon CloudWatch 14
DevOps Amazon-Vertreter 14
Schritte zur Migration 14
Migrieren Sie die Infrastruktur als Code und CLI-Nutzung 15
Migrieren Sie API-Integrationen 15
Offboarding-Schritte: Exportieren Sie Ihre Daten 15
Löschen Sie Ihre Amazon DevOps Guru-Ressourcen 15
Häufig gestellte Fragen 16
Weitere Ressourcen 16
Übergang von Amazon DevOps Guru zu Amazon CloudWatch und Amazon DevOps Agent 17
Wie DevOps Guru und seine Nachfolger unterscheiden sich 18
So funktioniert der Übergang 18

Wie wir Sie bei der Umstellung unterstützen ... 19
Wer muss handeln und bis wann ... 19
Was ändert sich auf einen Blick ... 20
Erkennung von metrischen Anomalien und Warnmeldungen ... 22
Erkennung von Anomalien protokollieren ... 23
Erkennung von Datenbankanomalien ... 23
Untersuchung und Ursachenanalyse ... 24
Proaktive Einblicke ... 24
Infrastruktur als Code und CLI-Nutzung ... 25
API-Integrationen ... 26
Exportiere deine Daten ... 27
Löschen Sie Ihre DevOps Guru-Ressourcen ... 27
Zeitplan und Support ... 28
Checkliste für den Übergang ... 28
Häufig gestellte Fragen ... 29
Zugehörige Ressourcen ... 29
Einrichtung ... 31
Melde dich an für AWS ... 31
Melde dich für einen an AWS-Konto ... 31
Ermitteln Sie den Versicherungsschutz für DevOps Guru ... 32
Identifizieren Sie Ihr Benachrichtigungsthema ... 33
Ihrem Thema wurden Berechtigungen hinzugefügt ... 33
Schätzung Ihrer Kosten ... 35
Erste Schritte ... 38
Schritt 1: Richten Sie sich ein ... 38
Schritt 2: Aktivieren DevOps Guru ... 38
Überwachen Sie Konten in Ihrer gesamten Organisation ... 38
Überwachen Sie Ihr Girokonto ... 40
Schritt 3: Geben Sie Ihre an DevOps Berichterstattung über Guru-Ressourcen ... 42
Aktivierung von AWS Diensten für die DevOps Guru-Analyse ... 44
Mit Erkenntnissen arbeiten ... 45
Einblicke ansehen ... 45
Einblicke in die DevOps Guru-Konsole verstehen ... 47
Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden ... 50
Die Schweregrade von Insight verstehen ... 51
Datenbanken überwachen ... 52

Relationale Datenbanken ... 52
Überwachung von Datenbankoperationen in Amazon RDS ... 52
Überwachung von Datenbankvorgängen in Amazon Redshift ... 55
Arbeiten mit Anomalien in Guru für RDS DevOps ... 56
Nichtrelationale Datenbanken ... 76
Überwachung von Datenbankoperationen in Amazon DynamoDB ... 77
Überwachung von Datenbankoperationen in Amazon ElastiCache ... 78
Integration mit CodeGuru Profiler ... 79
Definition von Anwendungen mithilfe von AWS Ressourcen ... 80
Verwenden Sie Tags, um Ressourcen in Ihren Anwendungen zu identifizieren ... 81
Was ist ein Tag? ... 82
Definition einer Anwendung mithilfe eines Tags ... 83
Verwenden von Stichwörtern mit DevOps Guru ... 83
Hinzufügen von Tags zu Ressourcen ... 84
Verwenden Sie Stacks, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren ... 85
Auswahl der zu analysierenden Stapel ... 86
Arbeiten mit EventBridge ... 88
Veranstaltungen für DevOps Guru ... 88
DevOps Guru New Insight: Offene Veranstaltung ... 88
Benutzerdefiniertes Beispielereignismuster für einen neuen Einblick mit hohem Schweregrad ... 90
Einstellungen werden aktualisiert ... 91
Aktualisierung Ihres Verwaltungskontos ... 91
Aktualisierung Ihres AWS Analysebereichs ... 92
Aktualisierung deiner Benachrichtigungen ... 92
Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole ... 93
Hinzufügen von Amazon SNS SNS-Benachrichtigungsthemen ... 93
Amazon SNS SNS-Benachrichtigungsthemen entfernen ... 94
Aktualisierung der Amazon SNS SNS-Benachrichtigungskonfigurationen ... 94
Ihrem Thema wurden Berechtigungen hinzugefügt ... 95
Filtere deine Benachrichtigungen ... 96
Filtern von Benachrichtigungen mit einer Amazon SNS SNS-Abonnementfilterrichtlinie ... 96
Beispiel für eine gefilterte Amazon SNS SNS-Benachrichtigung ... 97
Aktualisierung der Systems Manager Manager-Integration ... 99
Aktualisierung der Erkennung von Protokollanomalien ... 100

Die Verschlüsselung wird aktualisiert 100
Benachrichtigungen anzeigen 102
Neue Erkenntnisse 102
Geschlossener Einblick 103
Neuer Verband 105
Neue Empfehlung 106
Schweregrad wurde erhöht 107
Fehler bei der Ressourcenvalidierung 108
Analysierte Ressourcen anzeigen 110
Aktualisierung Ihres AWS Analysebereichs 110
Die Ansicht „Analysierte Ressourcen“ wird für Benutzer entfernt 112
Bewährte Methoden 114
Sicherheit 115
Datenschutz 116
Datenverschlüsselung 117
Wie DevOps Guru verwendet Zuschüsse in AWS KMS 118
Überwachung Ihrer Verschlüsselungsschlüssel in DevOps Guru 119
Erstellen eines kundenseitig verwalteten Schlüssels 119
Datenschutz für Datenverkehr 121
Identitäts- und Zugriffsverwaltung 121
Zielgruppe 122
Authentifizierung mit Identitäten 122
Verwalten des Zugriffs mit Richtlinien 124
Richtlinienaktualisierungen 126
Wie Amazon DevOps Guru arbeitet mit IAM 131
Identity-based Politik 137
Verwenden von servicegebundenen Rollen 148
DevOps Referenz zu Guru-Berechtigungen 154
Berechtigungen für Amazon SNS-Themen 159
Berechtigungen für verschlüsselte Amazon SNS-Themen 163
Fehlerbehebung 163
Überwachung DevOps Guru 168
Überwachung mit CloudWatch 168
Protokollierung DevOps Guru-API-Aufrufe mit AWS CloudTrail 171
VPC-Endpunkte (AWS PrivateLink) 174
Überlegungen für DevOps Guru VPC-Endpunkte 175

Erstellen eines Schnittstellen-VPC-Endpunkts für DevOps Guru 175
Erstellen einer VPC-Endpunktrichtlinie für DevOps Guru 175
Sicherheit der Infrastruktur 176
Ausfallsicherheit 177
Kontingente und -Einschränkungen 178
Benachrichtigungen 178
CloudFormation Stapel 178
DevOpsGrenzwerte für die Überwachung von Guru-Ressourcen 178
DevOpsGuru-Kontingente für die Erstellung, Bereitstellung und Verwaltung einer API 179
Dokumentverlauf 180
AWS Glossar 189

Hinweis zum Ende des Supports: Amazon DevOps Guru wird am 29. Oktober 2026 keine neuen Kunden mehr annehmen. Aktuelle Kunden sind davon nicht betroffen und können Amazon weiterhin nutzen DevOps Guru bis 30. September 2027. Nach dem 30. September 2027 können Sie nicht mehr auf Amazon zugreifen DevOps Guru. Weitere Informationen finden Sie unter Ende des Supports für Amazon DevOps Guru.

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 Amazon DevOps Guru?

Willkommen im Amazon DevOps Guru-Benutzerhandbuch.

DevOpsGuru ist ein vollständig verwalteter Betriebsservice, der es Entwicklern und Betreibern leicht macht, die Leistung und Verfügbarkeit ihrer Anwendungen zu verbessern. DevOpsMit Guru können Sie die administrativen Aufgaben im Zusammenhang mit der Identifizierung von Betriebsproblemen auslagern, sodass Sie Empfehlungen zur Verbesserung Ihrer Anwendung schnell umsetzen können. DevOpsGuru erstellt reaktive Erkenntnisse, die du jetzt nutzen kannst, um deine Anwendung zu verbessern. Es liefert auch proaktive Einblicke, die Ihnen helfen, Betriebsprobleme zu vermeiden, die sich in Zukunft auf Ihre Anwendung auswirken könnten.

DevOpsGuru verwendet maschinelles Lernen, um Ihre Betriebsdaten sowie Anwendungskennzahlen und Ereignisse zu analysieren, um Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Sie werden benachrichtigt, wenn DevOps Guru ein Betriebsproblem oder ein Betriebsrisiko feststellt. Für jedes Problem gibt DevOps Guru intelligente Empfehlungen zur Behebung aktueller und prognostizierter zukünftiger Betriebsprobleme.

Um zu beginnen, siehe Wie fange ich mit DevOps Guru an?

Wie funktioniert DevOps Guru?

Der DevOps Guru-Workflow beginnt, wenn Sie den Umfang und die Benachrichtigungen konfigurieren. Nachdem du DevOps Guru eingerichtet hast, beginnt es mit der Analyse deiner Betriebsdaten. Wenn es anomales Verhalten erkennt, erstellt es einen Einblick, der Empfehlungen und Listen von Metriken, Protokollgruppen und Ereignissen enthält, die mit dem Problem zusammenhängen. DevOpsGuru benachrichtigt dich für jeden Einblick. Wenn du diese Option aktiviert hast AWS Systems Manager OpsCenter, OpsItem wird eine erstellt, sodass du den Systems Manager verwenden kannst OpsCenter , um deine Erkenntnisse zu verfolgen und zu verwalten. Jeder Einblick enthält Empfehlungen, Metriken, Protokollgruppen und Ereignisse im Zusammenhang mit anomalem Verhalten. Verwenden Sie Informationen in einem Einblick, die Ihnen helfen, das anomale Verhalten zu verstehen und zu beheben.

DevOpsGuru-Arbeitsablauf auf hoher EbeneWeitere Informationen zu den drei übergeordneten Workflow-Schritten finden Sie unter. Unter erfahren Detaillierter DevOps Guru-Arbeitsablauf Sie mehr über den detaillierteren DevOps Guru-Workflow, einschließlich seiner Interaktion mit anderen AWS Diensten.

Themen

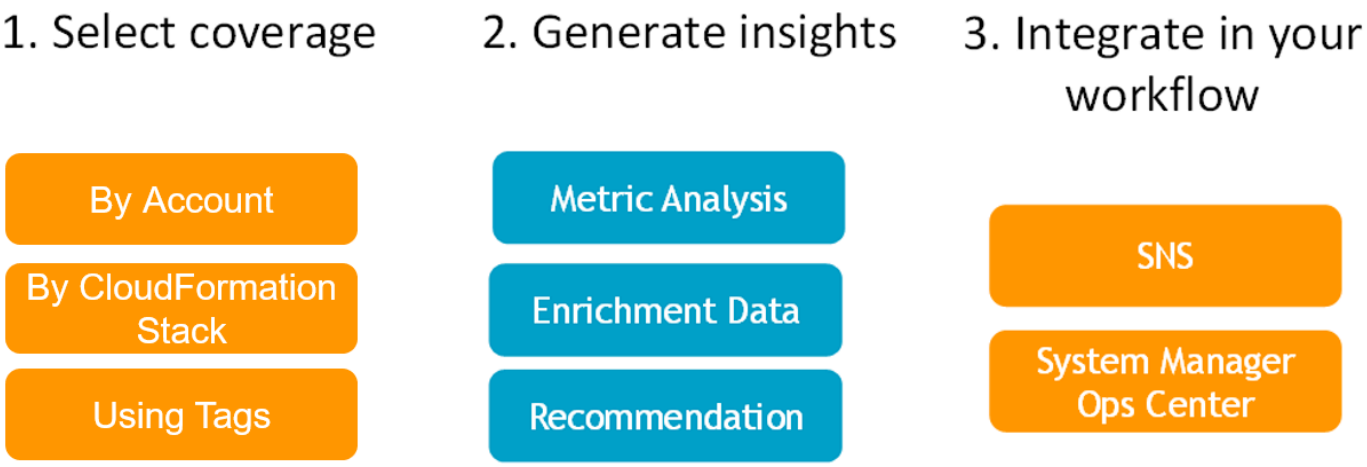
- DevOpsGuru-Arbeitsablauf auf hoher Ebene
- Detaillierter DevOps Guru-Arbeitsablauf

DevOpsGuru-Arbeitsablauf auf hoher Ebene

Der Amazon DevOps Guru-Workflow kann in drei übergeordnete Schritte unterteilt werden.

1. Geben Sie die DevOps Guru-Abdeckung an, indem Sie angeben, welche AWS Ressourcen in Ihrem AWS Konto analysiert werden sollen.
2. DevOpsGuru beginnt mit der Analyse von CloudWatch Amazon-Metriken und anderen Betriebsdaten AWS CloudTrail, um Probleme zu identifizieren, die Sie beheben können, um Ihren Betrieb zu verbessern.
3. DevOpsGuru stellt sicher, dass Sie über Erkenntnisse und wichtige Informationen informiert sind, indem er Ihnen für jedes wichtige DevOps Guru-Ereignis eine Benachrichtigung sendet.

Du kannst DevOps Guru auch so konfigurieren, dass ein Login OpsItem erstellt wird AWS Systems Manager OpsCenter , mit dem du deine Erkenntnisse nachverfolgen kannst. Das folgende Diagramm zeigt diesen allgemeinen Arbeitsablauf.



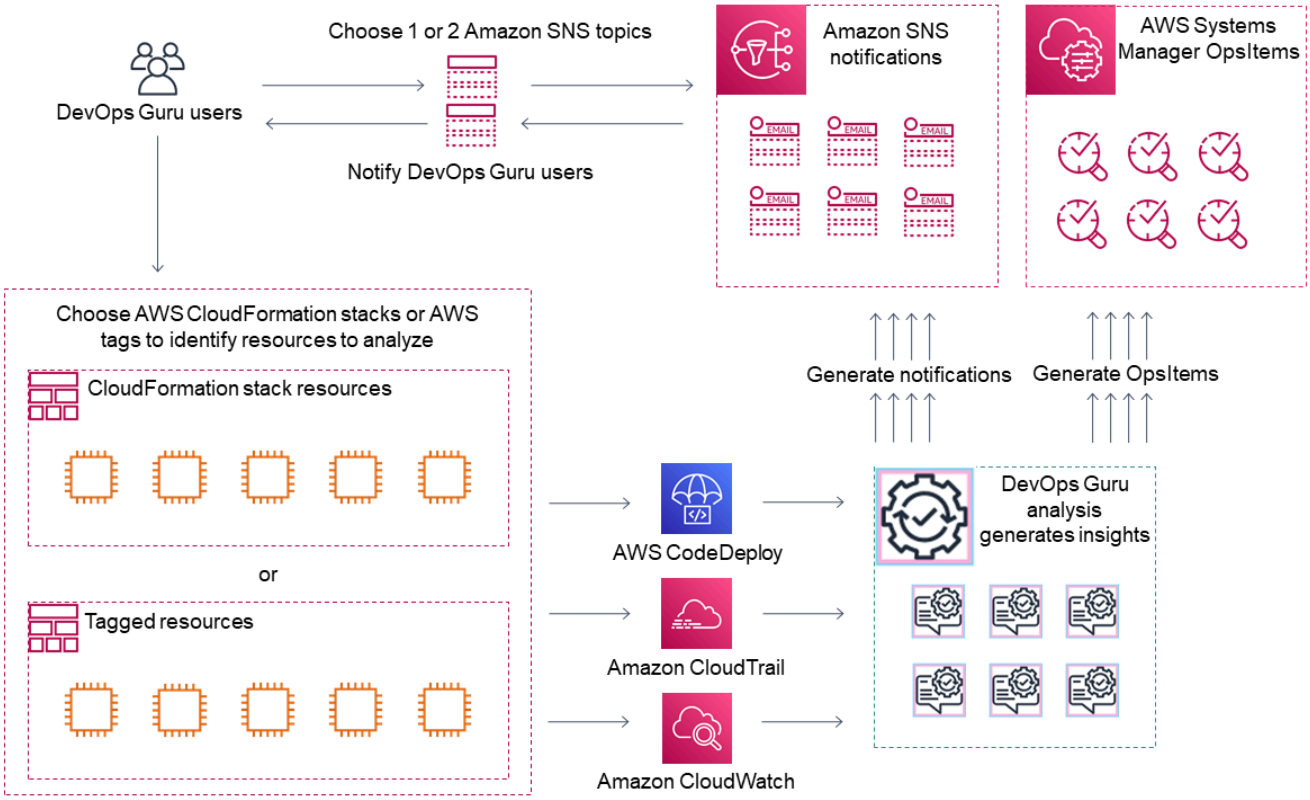
1. Im ersten Schritt wählen Sie Ihren Versicherungsschutz aus, indem Sie angeben, welche AWS Ressourcen in Ihrem AWS Konto analysiert werden. DevOpsGuru kann alle Ressourcen in einem AWS Konto abdecken oder analysieren, oder du kannst AWS CloudFormation Stapel oder AWS Tags verwenden, um eine Teilmenge der zu analysierenden Ressourcen in deinem Konto anzugeben. Stellen Sie sicher, dass die von Ihnen angegebenen Ressourcen

Ihre geschäftskritischen Anwendungen, Workloads und Microservices ausmachen. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

2. Im zweiten Schritt analysiert DevOps Guru die Ressourcen, um Erkenntnisse zu gewinnen. Dies ist ein fortlaufender Prozess. Sie können die Erkenntnisse sowie die darin enthaltenen Empfehlungen und zugehörigen Informationen in der DevOps Guru-Konsole einsehen. DevOps Guru analysiert die folgenden Daten, um Probleme zu finden und Erkenntnisse zu gewinnen.
   - Individuelle CloudWatch Amazon-Metriken, die von Ihren AWS Ressourcen ausgegeben werden. Wenn ein Problem identifiziert wird, sammelt DevOps Guru diese Metriken zusammen.
   - Protokollieren Sie Anomalien aus CloudWatch Amazon-Protokollgruppen. Wenn Sie die Erkennung von Protokollanomalien aktivieren, zeigt DevOps Guru entsprechende Protokollanomalien an, wenn ein Problem auftritt.
   - DevOpsGuru ruft die Anreicherungsdaten aus den AWS CloudTrail Verwaltungsprotokollen ab, um Ereignisse zu finden, die mit den gesammelten Metriken zusammenhängen. Bei den Ereignissen kann es sich um Ereignisse im Zusammenhang mit der Bereitstellung von Ressourcen und um Konfigurationsänderungen handeln.
   - Wenn Sie es verwenden AWS CodeDeploy, analysiert DevOps Guru Bereitstellungsereignisse, um Erkenntnisse zu gewinnen. Ereignisse für alle Arten von CodeDeploy Bereitstellungen (lokaler Server, Amazon EC2-Server, Lambda oder Amazon EC2) werden analysiert.
   - Wenn DevOps Guru ein bestimmtes Muster findet, generiert es eine oder mehrere Empfehlungen, um das identifizierte Problem zu mildern oder zu beheben. Die Empfehlungen werden in einem Insight zusammengefasst. Der Einblick enthält auch eine Liste der Kennzahlen und Ereignisse, die sich auf das Problem beziehen. Sie verwenden die Insight-Daten, um das identifizierte Problem anzugehen und zu verstehen.
3. Im dritten Schritt integriert DevOps Guru die Insight-Benachrichtigung in Ihren Arbeitsablauf, um Ihnen zu helfen, Probleme zu verwalten und schnell zu beheben.
   - Die in Ihrem AWS Konto generierten Erkenntnisse werden zu dem Thema Amazon Simple Notification Service (Amazon SNS) veröffentlicht, das Sie bei der DevOps Guru-Setup ausgewählt haben. Auf diese Weise werden Sie benachrichtigt, sobald ein Insight erstellt wurde. Weitere Informationen finden Sie unter Aktualisierung deiner Benachrichtigungen in DevOps Guru.
   - Wenn du es AWS Systems Manager während der DevOps Guru-Setup aktiviert hast, erstellt jeder Insight einen entsprechenden OpsItem , der dir hilft, die entdeckten Probleme zu verfolgen und zu verwalten. Weitere Informationen finden Sie unter Aktualisierung der AWS Systems Manager Integration in Guru DevOps.

Detaillierter DevOps Guru-Arbeitsablauf

Der DevOps Guru-Workflow lässt sich in mehrere AWS Dienste integrieren, darunter Amazon CloudWatch AWS CloudTrail, Amazon Simple Notification Service und AWS Systems Manager. Das folgende Diagramm zeigt einen detaillierten Arbeitsablauf, der zeigt, wie er mit anderen AWS Diensten funktioniert.



Dieses Diagramm zeigt ein Szenario, in dem die DevOps Guru-Abdeckung durch die AWS Ressourcen spezifiziert wird, die in AWS CloudFormation Stapeln oder mithilfe von AWS Tags definiert sind. Wenn keine Stacks oder Tags ausgewählt werden, analysiert DevOps Guru Coverage alle AWS Ressourcen in deinem Konto. Weitere Informationen erhalten Sie unter Definieren von Anwendungen mithilfe von AWS Ressourcen und Ermitteln Sie den Versicherungsschutz für DevOps Guru.

1. Während der Einrichtung geben Sie ein oder zwei Amazon SNS-Themen an, anhand derer Sie über wichtige DevOps Guru-Ereignisse informiert werden, z. B. wenn ein Einblick erstellt wird. Als Nächstes können Sie AWS CloudFormation Stacks angeben, die die Ressourcen definieren, die analysiert werden sollen. Sie können Systems Manager auch so einrichten, dass OpsItem für jeden Einblick eine generiert wird, um Sie bei der Verwaltung Ihrer Erkenntnisse zu unterstützen.

2. Nachdem DevOps Guru konfiguriert ist, beginnt es mit der Analyse von CloudWatch Metriken, Protokollgruppen und Ereignissen, die von Ihren Ressourcen und AWS CloudTrail Daten zu den CloudWatch Metriken ausgegeben werden. Wenn Ihr Betrieb CodeDeploy Bereitstellungen beinhaltet, analysiert DevOps Guru auch Bereitstellungsereignisse.

   DevOpsGuru gewinnt Erkenntnisse, wenn es ungewöhnliches, anomales Verhalten in den analysierten Daten identifiziert. Jeder Einblick enthält eine oder mehrere Empfehlungen, eine Liste der Metriken, die zur Generierung der Erkenntnisse verwendet wurden, eine Liste verwandter Protokollgruppen und eine Liste der Ereignisse, die zur Generierung der Erkenntnisse verwendet wurden. Verwenden Sie diese Informationen, um das identifizierte Problem zu lösen.
3. Nachdem jeder Einblick erstellt wurde, sendet DevOps Guru eine Benachrichtigung unter Verwendung des Amazon SNS-Themas oder der Themen, die bei der Einrichtung von DevOps Guru angegeben wurden. Wenn Sie DevOps Guru aktiviert haben, um einen OpsItem In-Systems Manager zu generieren OpsCenter, löst jeder Insight auch einen neuen Systems Manager OpsItem aus. Sie können den Systems Manager verwenden, um Ihre Erkenntnisse zu verwalten OpsItems.

Wie fange ich mit DevOps Guru an?

Wir empfehlen, dass Sie zuerst die folgenden Schritte ausführen:

1. Erfahren Sie mehr über DevOps Guru, indem Sie die Informationen unter lesenDevOpsGuru-Konzepte.
2. Richten Sie Ihr AWS Konto AWS CLI, den und einen Administratorbenutzer ein, indem Sie den Schritten unter folgenAmazon einrichten DevOps Guru.
3. Benutze DevOps Guru und befolge dabei die Anweisungen unterErste Schritte mit DevOps Guru.

Wie kann ich verhindern, dass DevOps Guru-Gebühren anfallen?

Um Amazon DevOps Guru zu deaktivieren, sodass keine Gebühren für die Analyse von Ressourcen in Ihrem AWS Konto und Ihrer Region anfallen, aktualisieren Sie Ihre Deckungseinstellungen, sodass Ressourcen nicht analysiert werden. Folgen Sie dazu den Schritten unter Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps und wählen Sie in Schritt 4 die Option Keine aus. Du musst dies für jedes AWS Konto und jede Region tun, in der DevOps Guru Ressourcen analysiert.

> **Note**
>
> Wenn du deine Berichterstattung aktualisierst, um die Analyse von Ressourcen einzustellen, fallen möglicherweise weiterhin geringfügige Gebühren an, wenn du bestehende Erkenntnisse, die DevOps Guru in der Vergangenheit generiert hat, überprüfst. Diese Gebühren fallen im Zusammenhang mit API-Aufrufen an, die zum Abrufen und Anzeigen von Insight-Informationen verwendet werden. Weitere Informationen finden Sie unter Amazon DevOps Guru-Preise.

DevOpsGuru-Konzepte

Die folgenden Konzepte sind wichtig, um zu verstehen, wie Amazon DevOps Guru funktioniert.

Topics

- Anomalie
- Insight
- Kennzahlen und betriebliche Ereignisse
- Gruppen protokollieren und Anomalien protokollieren
- Empfehlungen

Anomalie

Eine Anomalie steht für eine oder mehrere verwandte Metriken, die von DevOps Guru erkannt wurden und die unerwartet oder ungewöhnlich sind. DevOpsGuru generiert Anomalien, indem er mithilfe von maschinellem Lernen Metriken und Betriebsdaten analysiert, die sich auf Ihre Ressourcen beziehen. AWS Sie geben bei der Einrichtung von Amazon DevOps Guru die AWS Ressourcen an, die analysiert werden sollen. Weitere Informationen finden Sie unter Amazon einrichten DevOps Guru.

Insight

Ein Insight ist eine Sammlung von Anomalien, die bei der Analyse der AWS Ressourcen entstehen, die Sie bei der Einrichtung DevOps von Guru angegeben haben. Jeder Einblick enthält Beobachtungen, Empfehlungen und Analysedaten, anhand derer Sie Ihre betriebliche Leistung verbessern können. Es gibt zwei Arten von Erkenntnissen:

- Reaktiv: Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Es enthält Anomalien mit Empfehlungen, zugehörigen Kennzahlen und Ereignissen, damit Sie die Probleme sofort verstehen und beheben können.
- Proaktiv: Ein proaktiver Einblick informiert Sie über anomales Verhalten, bevor es auftritt. Es enthält Anomalien mit Empfehlungen, die Ihnen helfen sollen, die Probleme zu beheben, bevor sie voraussichtlich auftreten.

Kennzahlen und betriebliche Ereignisse

Die Anomalien, die einen Einblick ausmachen, werden durch die Analyse der von Amazon zurückgegebenen Metriken CloudWatch und der von Ihren AWS Ressourcen ausgegebenen Betriebsereignisse generiert. Sie können sich die Kennzahlen und betrieblichen Ereignisse ansehen, die Ihnen einen Einblick geben und Ihnen helfen, Probleme in Ihrer Anwendung besser zu verstehen.

Gruppen protokollieren und Anomalien protokollieren

Wenn Sie die Erkennung von Protokollanomalien aktivieren, werden die entsprechenden Protokollgruppen auf den DevOps Guru Insight-Seiten in der DevOps Guru-Konsole angezeigt. Eine Protokollgruppe informiert Sie über wichtige Diagnoseinformationen darüber, wie eine Ressource funktioniert und wie darauf zugegriffen wird.

Eine Protokollanomalie stellt eine Gruppe ähnlicher anomaler Protokollereignisse dar, die innerhalb einer Protokollgruppe gefunden wurden. Beispiele für ungewöhnliche Protokollereignisse, die in DevOps Guru angezeigt werden können, sind Stichwortanomalien, Formatanomalien, HTTP-Code-Anomalien und mehr.

Sie können Protokollanomalien verwenden, um die Ursache eines Betriebsproblems zu diagnostizieren. DevOpsGuru verweist in Insight-Empfehlungen auch auf Protokollzeilen, um mehr Kontext für empfohlene Lösungen bereitzustellen.

> **Note**
>
> DevOpsGuru arbeitet mit Amazon zusammen CloudWatch , um die Erkennung von Protokollanomalien zu ermöglichen. Wenn Sie die Erkennung von Protokollanomalien aktivieren, fügt DevOps Guru Ihren CloudWatch Protokollgruppen Tags hinzu. Wenn Sie die Erkennung von Protokollanomalien deaktivieren, entfernt DevOps Guru Tags aus Ihren CloudWatch Protokollgruppen.

Darüber hinaus sollten Administratoren sicherstellen, dass nur Benutzer mit Berechtigungen zum Anzeigen von Protokollen berechtigt sind, ungewöhnliche CloudWatch CloudWatch Protokolle einzusehen. Wir empfehlen, dass Sie IAM-Richtlinien verwenden, um den Zugriff auf den Vorgang zuzulassen oder zu verweigern. `ListAnomalousLogs` Weitere Informationen finden Sie unter Identity and Access Management für DevOps Guru.

Empfehlungen

Jeder Einblick enthält Empfehlungen mit Vorschlägen, mit denen Sie die Leistung Ihrer Anwendung verbessern können. Die Empfehlung beinhaltet Folgendes:

- Eine Beschreibung der empfohlenen Maßnahmen zur Behebung der Anomalien, die den Erkenntnissen zugrunde liegen.
- Eine Liste der analysierten Metriken, bei denen DevOps Guru ungewöhnliches Verhalten festgestellt hat. Jede Metrik enthält den Namen des CloudFormation Stacks, der die den Metriken zugeordnete Ressource generiert hat, den Namen der Ressource und den Namen des AWS Dienstes, der der Ressource zugeordnet ist.
- Eine Liste der Ereignisse, die sich auf die mit den Erkenntnissen verknüpften anomalen Metriken beziehen. Jedes zugehörige Ereignis enthält den Namen des CloudFormation Stacks, der die dem Ereignis zugeordnete Ressource generiert hat, den Namen der Ressource, die das Ereignis generiert hat, und den Namen des AWS Dienstes, der dem Ereignis zugeordnet ist.
- Eine Liste von Protokollgruppen, die sich auf das mit dem Insight verbundene anomale Verhalten beziehen. Jede Protokollgruppe enthält ein Beispiel für eine Protokollnachricht, Informationen über die Arten der gemeldeten Protokollanomalien, die Häufigkeit, zu der die Protokollanomalien aufgetreten sind, und einen Link, über den die Protokollzeilen angezeigt werden können. CloudWatch

DevOpsGuru-Berichterstattung

DevOpsGuru befasst sich mit einer Reihe verschiedener AWS Dienste und erstellt daraus Erkenntnisse. Für jeden Dienst, für den DevOps Guru Erkenntnisse generiert, zeigt DevOps Guru eine Vielzahl von analysierten Metriken und generierten Erkenntnissen an.

Beispiel für einen Anwendungsfall für reaktive Erkenntnisse:

Service-Name	Anwendungsfall	Beispiele	Kennzahlen
AWS Lambda	Erkennen Sie Latenz- oder Daueranomalien für Lambda-Funktionen, die auf verschiedene Ursachen wie Kaltstarts, erhöhte Anfragen, Downstream-Drosselung oder Codebereitstellungen zurückzuführen sind. Empfehlen Sie Möglichkeiten zur schnellen Problembehebung.	Codebereitstellung: Die Amazon API Gateway Latenz wird durch einen Anstieg der Lambda-Latenz nach einer kürzlichen Lambda-Code-Bereitstellung beeinträchtigt. Downstream-Drosselung: Der Bediener reduziert die Kapazität der Leseeinheiten für DynamoDB, was zu vermehrten Wiederholungsversuchen führte. Dies führt zu einer Drosselung. Kaltstart: Die Lambda-Funktion ist unzureichend bereitgestellt, sodass Lambda länger braucht, wenn Anfragen gestellt werden.	Dauer Drosselungen

Beispiel für einen Anwendungsfall für proaktive Einblicke:

Service-Name	Anwendungsfall	Kennzahlen
Amazon DynamoDB	Bei der verbrauchten Kapazität der DynamoDB-Tabelle besteht die Gefahr, dass das Tabellenlimit	ConsumedReadCapacityUnits

Service-Name	Anwendungsfall	Kennzahlen
	erreicht wird. Empfohlen e Maßnahme: Wenn Sie den Modus für bereitges tellte Kapazität verwenden, verwenden Sie Auto Scaling, um die Durchsatzkapazität für Tabellen aktiv zu verwalten, oder erwerben Sie im Voraus reservierte Kapazität für Tabellen. Wechseln Sie in den On-Demand-Kapazitä tsmodus, um pro Leseanfor derung zu zahlen und nur für das zu bezahlen, was tatsächli ch genutzt wird. Erkennung szeit: 6 Tage	

Liste der Serviceabdeckungen

Für einige Dienste generiert DevOps Guru reaktive Erkenntnisse. Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Es enthält Anomalien mit Empfehlungen, zugehörigen Kennzahlen und Ereignissen, damit Sie die Probleme sofort verstehen und lösen können.

Für einige Dienste erstellt DevOps Guru proaktive Einblicke. Ein proaktiver Einblick informiert Sie über anomales Verhalten, bevor es auftritt. Es enthält Anomalien mit Empfehlungen, die Ihnen helfen sollen, die Probleme zu beheben, bevor sie voraussichtlich auftreten.

DevOpsGuru erstellt reaktive Erkenntnisse für Dienste wie die folgenden:

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsDie Guru-Überwachung erfolgt auf Auto Scaling Scaling-Gruppenebene und nicht auf Einzelinstanzebene.

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru liefert proaktive Einblicke für Dienste wie die folgenden:

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

Ende des Supports für Amazon DevOps Guru

-Übersicht

Nach reiflicher Überlegung haben wir beschlossen, den Support für Amazon DevOps Guru mit Wirkung zum 30. September 2027 einzustellen. Amazon DevOps Guru akzeptiert ab dem 29. Oktober 2026 keine neuen Kunden mehr. Als Bestandskunde mit einem Konto, das vor dem 29. Oktober 2026 für den Service angemeldet wurde, können Sie die Funktionen von Amazon DevOps Guru weiterhin nutzen. Nach dem 30. September 2027 können Sie Amazon DevOps Guru nicht mehr verwenden.

Wir empfehlen Kunden, ihre Anforderungen an Warnmeldungen und die Erkennung von Anomalien auf Amazon zu verlagern und Amazon Agent zu CloudWatch nutzen, um AI-assisted betriebliche Untersuchungen durchzuführen und Einblicke zu gewinnen. DevOps Details dazu finden Sie unter Alternative Lösungen.

Servicestatus bis 30. September 2027

Bis zum 30. September 2027 können bestehende Amazon DevOps Guru-Kunden den Service weiterhin normal nutzen. Während dieses Zeitraums AWS wird:

1. Bereitstellung von Sicherheitspatches und kritischen Bugfixes
2. Sorgen Sie für Serviceverfügbarkeit und Leistung
3. Bieten Sie weiterhin Support über AWS Support-Kanäle an
4. Fügen Sie dem Service keine neuen Funktionen hinzu

Was passiert mit Ihren Ressourcen nach dem 30. September 2027

Nach dem 30. September 2027:

- Sie werden nicht mehr auf die Amazon DevOps Guru-Konsole zugreifen können.
- DevOpsDer Amazon Guru-API-Betrieb wird nicht mehr verfügbar sein. Jede Anwendung, jedes Skript oder jede Pipeline, die die Amazon DevOps Guru-API aufruft, muss vor diesem Datum aktualisiert werden. Siehe Was bedeutet das für dich.

- Die Amazon DevOps Guru-Ressourcentypen werden zurückgezogen, und AWS CloudFormation AWS CLI-Operationen, die diese Ressourcentypen erstellen oder aktualisieren, schlagen fehl. Siehe Migrieren Sie die Infrastruktur als Code und CLI-Nutzung.
- Erkenntnisse, die zuvor von Amazon DevOps Guru generiert wurden, können nicht mehr abgerufen werden.

Was bedeutet das für dich

Die Auswirkungen dieser Änderung hängen davon ab, wie Sie Amazon DevOps Guru verwenden. Da Amazon DevOps Guru ein Überwachungstool ist, unterbricht der Verlust die laufenden Workloads nicht. Kunden, die Automatisierung, Infrastruktur als Code oder nachgelagerte Tools auf Amazon DevOps Guru aufgebaut haben, müssen vor dem 30. September 2027 Maßnahmen ergreifen, um jegliche Auswirkungen zu vermeiden.

Wenn Sie Amazon DevOps Guru-Ressourcen in der Infrastruktur als Code (AWS CloudFormation, AWS CDK, Terraform) oder über die CLI deklarieren. AWS Vorlagen und Stacks, die auf die Ressourcentypen verweisen `AWS::DevOpsGuru::ResourceCollection` oder nicht erstellt oder aktualisiert `AWS::DevOpsGuru::NotificationChannel` werden können, sobald die Ressourcentypen zurückgezogen wurden. Da eine einzelne ausgefallene Ressource einen gesamten Stack-Vorgang blockieren kann, ist dies die schwerste Auswirkung. Entfernen Sie diese Ressourcen aus Ihren Vorlagen, bevor der Support endet. Siehe Migrieren Sie die Infrastruktur als Code und CLI-Nutzung.

Wenn Sie die Amazon DevOps Guru-API von Ihren eigenen Tools aus aufrufen. Wenn Sie über die Amazon DevOps Guru-API Einblicke in interne Entwicklertools, Dashboards oder Ticketsysteme erhalten, geben diese Integrationen nach Ablauf des Supports keine Daten mehr zurück. Aktualisieren Sie sie, um die entsprechenden Signale von Amazon zu beziehen. CloudWatch Siehe Migrieren Sie API-Integrationen.

Den richtigen Migrationspfad wählen

Verwenden Sie die folgende Anleitung, um zu entscheiden, wohin Sie wechseln möchten, wie Sie Amazon DevOps Guru heute verwenden.

- Sie verwenden Amazon DevOps Guru in erster Linie zur Erkennung von Anomalien und zur Alarmierung von Kennzahlen. Wechseln Sie zu Amazon CloudWatch. Siehe Amazon CloudWatch.

- Sie verwenden Amazon DevOps Guru, um betriebliche Probleme anzureichern, zu korrelieren oder zu untersuchen. Entdecken Sie Amazon DevOps Agent. Siehe DevOps Amazon-Vertreter.

Alternative Lösungen

Wir haben die folgenden Alternativen zu Amazon DevOps Guru identifiziert, mit denen Sie die betriebliche Transparenz und die Erkennung von Anomalien aufrechterhalten können.

Amazon CloudWatch

Ideal für: Kunden, die Amazon DevOps Guru für die Erkennung von metrischen Anomalien und Betriebswarnungen verwenden.

Amazon CloudWatch bietet metrische Überwachung, Alarme und Erkennung von Anomalien für Ihre AWS Ressourcen und Anwendungen.

Die wichtigsten Vorteile:

1. Systemeigene Anomalieerkennung bei CloudWatch Metriken mit Alarmen, die Sie benachrichtigen, wenn Metriken von den erwarteten Mustern abweichen.
2. Umfassende Berichterstattung über AWS Services und benutzerdefinierte Metriken aus erster Hand.
3. Integriert in die umfassendere CloudWatch Observability-Suite (Metriken, Protokolle, Dashboards).

Erfahren Sie mehr: CloudWatch Amazon-Dokumentation.

DevOps Amazon-Vertreter

Ideal für: Kunden, die sich auf Amazon DevOps Guru verlassen, um betriebliche Probleme zu ergänzen, zu korrelieren und zu untersuchen.

Erfahren Sie mehr: Amazon DevOps Agent-Dokumentation.

Schritte zur Migration

In den folgenden Abschnitten wird beschrieben, wie Sie Ihre Infrastruktur als Code, CLI-Nutzung und API-Integrationen vor dem 30. September 2027 von Amazon DevOps Guru migrieren.

Migrieren Sie die Infrastruktur als Code und CLI-Nutzung

Wenn Sie Amazon DevOps Guru-Ressourcen in AWS CDK AWS CloudFormation, Terraform deklarieren oder über die AWS CLI erstellen, entfernen Sie diese Ressourcen vor dem 30. September 2027, um fehlgeschlagene Stack-Operationen zu vermeiden.

Amazon DevOps Guru macht die folgenden Ressourcentypen verfügbar:

- `AWS::DevOpsGuru::ResourceCollection`
- `AWS::DevOpsGuru::NotificationChannel`

1. Inventarisieren Sie die Vorlagen und Stacks, die auf die vorherigen Ressourcentypen verweisen.
2. Richten Sie die entsprechende CloudWatch Amazon-Konfiguration ein (z. B. die Alarme und Benachrichtigungen, die Ihren Amazon DevOps Guru-Benachrichtigungskanal ersetzen).
3. Entfernen Sie die Amazon DevOps Guru-Ressourcen aus Ihren Vorlagen und implementieren Sie die Änderung, sodass die Ressourcen nicht mehr von Ihren Stacks verwaltet werden.

Migrieren Sie API-Integrationen

Wenn Ihr Tool die Amazon DevOps Guru-API aufruft, aktualisieren Sie sie, um CloudWatch vor Ende des Supports äquivalente Signale von Amazon zu erhalten.

Offboarding-Schritte: Exportieren Sie Ihre Daten

Die Erkenntnisse von Amazon DevOps Guru können nach dem 30. September 2027 nicht mehr abgerufen werden. Wenn Sie Ihre Erkenntnisse aufzeichnen möchten, exportieren Sie sie vor diesem Datum. Dazu gibt es zwei Möglichkeiten, und wir empfehlen den meisten Kunden, beide zu verwenden: einen Amazon SNS-Benachrichtigungskanal, um die Erkenntnisse von jetzt an bis zum Ende des Supports zu erfassen, und die Amazon DevOps Guru-API, um die bereits gesammelten Erkenntnisse zu exportieren.

Löschen Sie Ihre Amazon DevOps Guru-Ressourcen

Um vor Ende des Supports die Analyse zu beenden und keine Gebühren mehr anfallen zu lassen, setzen Sie Ihren Analyseumfang für jedes Konto und jede Region, in der Amazon DevOps Guru aktiviert ist, auf Keine. Wählen Sie in der Konsole „Einstellungen“, dann

„DevOps Guru Analysis Coverage“, „Manage“ und dann „Keine“ aus. Du kannst auch anrufen`UpdateResourceCollection`, um die CloudFormation Stapel oder Tags zu entfernen, die deine Abdeckungsgrenze definieren. Schließen Sie den Datenexport ab, bevor Sie dies tun.

Um einen Benachrichtigungskanal zu entfernen, rufen Sie ihn auf `RemoveNotificationChannel` oder löschen Sie ihn in den Einstellungen in der Konsole. Durch das Entfernen des Kanals wird weder das Amazon SNS-Thema noch etwas gelöscht, das Sie bereits damit archiviert haben.

Wenn Sie Amazon DevOps Guru-Ressourcen in der Infrastruktur als Code deklarieren, entfernen Sie sie aus Ihren Vorlagen, anstatt sie out-Band zu löschen, damit Ihre Stacks und Vorlagen übereinstimmen. Siehe Migrieren Sie die Infrastruktur als Code und CLI-Nutzung.

Häufig gestellte Fragen

Funktionieren meine Anwendungen oder Datenbanken nach dem 30. September 2027 nicht mehr?

> Nein. Amazon DevOps Guru ist ein Überwachungsdienst: Er beobachtet die Ressourcen, die Sie ausführen, er hostet sie nicht. Nach dem Ende des Supports verlieren Sie die Sichtbarkeit und die Empfehlungen von Amazon DevOps Guru, aber Ihre Anwendungen, Datenbanken und Infrastruktur laufen weiter.

Was passiert, wenn ich nicht bis zum 30. September 2027 migriere?

> Nach dem 30. September 2027 können Sie nicht mehr auf die Amazon DevOps Guru-Konsole oder -API zugreifen, und die Amazon DevOps Guru-Ressourcentypen AWS CloudFormation und die AWS CLI schlagen fehl.

Weitere Ressourcen

Weitere Informationen finden Sie in den folgenden Ressourcen.

- Amazon-Dokumentation CloudWatch
- Dokumentation für Amazon DevOps Agents
- Preisgestaltung bei Amazon DevOps Guru
- AWS Support

Wenn Sie weitere Fragen haben, wenden Sie sich an den AWS Support.

Übergang von Amazon DevOps Guru zu Amazon CloudWatch und Amazon DevOps Agent

Amazonas DevOps Guru erreicht am 30. September 2027 das Ende der Unterstützung. Nach diesem Datum DevOps Guru analysiert deine Ressourcen nicht mehr und zuvor generierte Erkenntnisse sind nicht mehr verfügbar. Ihr Basiswert AWS Infrastruktur und Workloads sind nicht betroffen. Nur die DevOps Die Guru-Überwachungsebene wurde entfernt.

Dieser Leitfaden hilft Ihnen zu verstehen, was sich ändert und welche Maßnahmen Sie ergreifen müssen. Amazon CloudWatch bietet Anomalieerkennung und Warnmeldungen für Ihre Ressourcen und Amazon DevOps Der Agent bietet AI-assisted Untersuchung. Ihre Workloads bleiben an Ort und Stelle, ohne dass eine Migration erforderlich ist.

Topics

- Wie DevOps Guru und seine Nachfolger unterscheiden sich
- So funktioniert der Übergang
- Wie wir Sie bei der Umstellung unterstützen
- Wer muss handeln und bis wann
- Was ändert sich auf einen Blick
- Erkennung von metrischen Anomalien und Warnmeldungen
- Erkennung von Anomalien protokollieren
- Erkennung von Datenbankanomalien
- Untersuchung und Ursachenanalyse
- Proaktive Einblicke
- Infrastruktur als Code und CLI-Nutzung
- API-Integrationen
- Exportiere deine Daten
- Löschen Sie Ihre DevOps Guru-Ressourcen
- Zeitplan und Support
- Checkliste für den Übergang
- Häufig gestellte Fragen
- Zugehörige Ressourcen

Wie DevOps Guru und seine Nachfolger unterscheiden sich

Amazon DevOps Guru verwendet ein verwaltetes Modell: Sie fügen Ressourcen zu seiner Berichterstattung hinzu, und es lernt deren normales Verhalten, erkennt Anomalien, gruppiert verwandte Anomalien zu Erkenntnissen und empfiehlt Maßnahmen. Du entscheidest nicht, welche Metriken du analysieren oder Schwellenwerte konfigurieren möchtest.

Amazon CloudWatch verwendet ein konfiguriertes Modell: Sie wählen die zu überwachenden Metriken und Protokollgruppen aus und erstellen die Anomaliedetektoren, Alarme und Benachrichtigungsaktionen. Dies erfordert eine einmalige Einrichtung und Sie haben die direkte Kontrolle darüber, was überwacht wird, wie empfindlich jeder Alarm ist und wohin Benachrichtigungen gesendet werden. Amazon DevOps Der Agent führt die Untersuchung und Ursachenanalyse durch DevOps Guru-Einblicke wurden bereitgestellt, angefangen mit einem CloudWatch Alarm oder auf Anfrage.

Sie können beide zusammen verwenden: CloudWatch erkennt und alarmiert, und Amazon DevOps Der Agent hilft Ihnen dabei, die Ursache zu untersuchen und zu finden.

So funktioniert der Übergang

Wir migrieren Ihre Workloads nicht. Ihre Anwendungen, Datenbanken und Infrastruktur bleiben genau dort, wo sie sind. Dies ist eine Änderung der Überwachungskonfiguration, keine Workload-Migration.

Die Umstellung besteht aus vier Teilen:

1. Reproduzieren Sie die Erkennung und Alarmierung, auf die Sie sich in Amazon verlassen CloudWatch.
2. Richten Sie Amazon ein DevOps Agent für Ermittlungen.
3. Entfernen DevOps Guru aus Ihrer Infrastruktur als Code-Vorlagen und API-Integrationen.
4. Exportieren Sie alle Erkenntnisse, die Sie behalten möchten, und setzen Sie dann Ihre Analyseabdeckung auf Keine.

Sie können jeweils ein Konto oder eine Anwendung nach der anderen wechseln, und Sie können Folgendes ausführen DevOps Guru und CloudWatch Seite an Seite, während Sie Ihre neue Konfiguration validieren. Weil DevOps Guru hostet deine Workloads nicht, es gibt keine Ausfallzeiten während des Übergangs. Eine Anleitung dazu, auf welchen Dienst die einzelnen Anwendungsfälle

verschoben werden sollten, finden Sie unter Den richtigen Migrationspfad wählen am Ende der Support-Seite.

Wie wir Sie bei der Umstellung unterstützen

Bis zum 30. September 2027, DevOps Guru arbeitet weiterhin normal. Wir bieten weiterhin Sicherheitspatches, kritische Bugfixes und Support über AWS Support-Kanäle und wir sorgen für die Verfügbarkeit unserer Dienste. Es werden keine neuen Funktionen hinzugefügt.

Die Ende des Supports für Amazon DevOps Guru Die Seite ist die verwaltete Referenz für Daten und Migrationsschritte. Wenn Sie während der Umstellung Fragen haben, wenden Sie sich an AWS Unterstützung. Wir empfehlen, die Umstellung bis zum 30. Juni 2027 abzuschließen, um einen Puffer vor Ablauf des Supports am 30. September 2027 zu haben.

Wer muss handeln und bis wann

Die Auswirkungen dieser Änderung hängen davon ab, wie Sie sie verwenden DevOps Guru.

Wenn Sie	Was passiert am Ende des Supports	Priorität
Deklarieren DevOps Guru-Ressourcen in AWS CloudFormation, AWS CDK- oder Terraform-Vorlagen	Stack-Operationen, die auf die zurückgezogenen Ressourcentypen verweisen, schlagen fehl. Eine einzelne ausgefallene Ressource kann ein gesamtes Stack-Update blockieren.	Am höchsten. Schließe das zuerst ab.
Rufen Sie den DevOps Guru-API von Dashboards, Ticketsystemen oder internen Tools	Integrationen geben keine Daten mehr zurück.	Hoch
Benutze den DevOps Guru-Konsole für Einblicke und Benachrichtigungen, einschließlich DevOps Guru für Amazon RDS	Sie verlieren die Erkennung von Anomalien und die Empfehlungen für die abgedeckten Ressourcen.	Mittel
Sie möchten vergangene Erkenntnisse aufzeichnen	Erkenntnisse sind nicht mehr verfügbar. Exportieren Sie sie,	Bevor Sie von Bord gehen

Wenn Sie	Was passiert am Ende des Supports	Priorität
	bevor Sie den Versicherungsschutz entfernen.	

Schließe alle Aktionen vor dem 30. September 2027 ab. Wir empfehlen, Ihre Umstellung bis zum 30. Juni 2027 abzuschließen, damit Sie Ihre CloudWatch und Amazon DevOps Agentenkonfiguration während DevOps Guru ist immer noch zum Vergleich verfügbar.

Was ändert sich auf einen Blick

Die folgende Tabelle fasst zusammen, was nach der Umstellung verfügbar ist und was sich von DevOps Guru.

Funktion	Nach der Umstellung verfügbar?	Was ist anders
Erkennung metrischer Anomalien	Ja, vom Kunden konfiguriert	CloudWatch Bei der Anomalieerkennung wird der erwartete Bereich jeder Metrik automatisch ermittelt. Sie wählen aus, für welche Metriken sie aktiviert werden soll.
Betriebliche Warnmeldungen	Ja, vom Kunden konfiguriert	Verwenden Sie Alarme zur Erkennung von Anomalien und zusammengesetzte Alarme und leiten Sie Änderunge n des Alarmstatus an Amazon SNS oder Amazon weiter EventBridge. Sie definieren die Alarme, anstatt sie automatisch zu empfangen.
Erkennung von Anomalien protokollieren	Ja, gleiche Berichterstattung	Aktivieren Sie die Anomalieerkennung direkt auf Ihrem CloudWatch Loggt Gruppen auf und untersucht sie mit CloudWatch Protokolliert Einblicke.
Erkennung von Datenbank anomalien (DevOps Guru	Ja, gleiche Berichterstattung	CloudWatch Database Insights zeigt dieselbe Datenbank last, dasselbe Wartungsereignis und dieselben Top-SQL-Daten wie DevOps Guru für Amazon RDS analysiert. Erstellen Sie eine CloudWatch Alarm bei der Erkennung von Anomalien für die dbLoad-Metrik, um über eine

Funktion	Nach der Umstellung verfügbar?	Was ist anders
(für Amazon RDS)		abnormale Auslastung informiert zu werden. Führen Sie dann eine On-Demand-Leistungsanalyse in Database Insights für den Alarmzeitraum durch, um die Ursache zu ermitteln.
CloudWatch Alarme, zu denen Sie hinzugefügt haben DevOps Guru	Ja, gleiche Berichterstattung	Ihre Alarme sind unverändert. Verwenden Sie sie, um eine Untersuchung einzuleiten in AWS DevOps Agent oder CloudWatch.
Gruppierte Einblicke mit Ursachenanalyse	Ja, vom Kunden initiiert	Amazon DevOps Agent und CloudWatch Untersuchungen korrelieren Metriken, Protokolle, Änderungsereignisse und Ablaufverfolgungen, um die Ursache zu ermitteln. Untersuchungen beginnen bei einem Alarm oder bei Bedarf und laufen nicht kontinuierlich ab.
Kontext der Dienstabhängigkeit	Ja, vom Kunden konfiguriert	Aktivieren AWS X-Ray und CloudWatch Anwendungssignale, damit Untersuchungen die Serviceverhältnisse abbilden können.
Empfehlungen und Abhilfemaßnahmen	Ja, vom Kunden initiiert	DevOps Guru fügte jeder Einsicht eine Empfehlung bei. Amazon DevOps Der Agent generiert während einer Untersuchung Empfehlungen und AWS Systems Manager Die Automatisierung führt die von Ihnen definierten Wartungs-Runbooks aus.
Benachrichtigungen	Ja, gleicher Versicherungsschutz	Amazon SNS, Amazon EventBridgeund Systemmanager OpsCenter sind die gleichen Ziele DevOps Guru benutzt. Du verbindest sie mit CloudWatch Alarme.

Funktion	Nach der Umstellung verfügbar?	Was ist anders
Proaktive Einblicke	Nicht verfügbar	DevOps Die proaktiven Einblicke von Guru enden mit dem Service. Für die Ressourcen, bei denen Frühwarnung für Sie wichtig ist, können Sie Folgendes erstellen CloudWatch Alarme zu Nutzungsschwellenwerten und Alarme zur Nutzung von Servicekontingenten für Ihre Kontokontingente.

Erkennung von metrischen Anomalien und Warnmeldungen

In DevOps Guru, die Erkennung von Anomalien in den Metriken einer Ressource beginnt automatisch, wenn die Ressource abgedeckt ist. In CloudWatch, aktivieren Sie die Anomalieerkennung für die von Ihnen ausgewählten Metriken und erstellen Alarme für sie.

Was müssen Sie tun

1. Identifizieren Sie die Kennzahlen, auf die Sie sich verlassen haben DevOps Guru zum Analysieren, z. B. CPU-Auslastung, Anzahl der Anfragen, 4XX- und 5XX-Fehlerraten, Latenz, Anzahl fehlerhafter Hosts, Arbeitsspeicher und Festplatte.
2. Aktiviere CloudWatch Erkennung von Anomalien bei diesen Metriken. CloudWatch ermittelt anhand ihrer Historie den erwarteten Bereich jeder Metrik.
3. Erstellen Sie Alarme zur Erkennung von Anomalien. Verwenden Sie zusammengesetzte Alarme, um verwandte Alarme zu kombinieren und Geräusche zu reduzieren.
4. Fügen Sie Alarmaktionen hinzu, die Benachrichtigungen an Ihre bestehenden Amazon SNS-Themen oder Amazon senden EventBridge Regeln.

Was ändert sich

Die Erkennung bezieht sich auf die von Ihnen ausgewählten Metriken und nicht auf jede Ressource innerhalb einer Abdeckungsgrenze. Sie steuern die Alarmempfindlichkeit, die Testzeiträume und die Weiterleitung von Benachrichtigungen.

Erkennung von Anomalien protokollieren

In DevOps Guru, in einer Einsicht tauchen Log-Anomalien zusammen mit den metrischen Anomalien auf. In CloudWatch, aktivieren Sie die Anomalieerkennung für jede Protokollgruppe und sehen sich Anomalien in CloudWatch Konsole „Protokolle“.

Was müssen Sie tun

1. Aktiviere CloudWatch Protokolliert die Erkennung von Anomalien in Ihren kritischen Protokollgruppen.
2. Verwenden CloudWatch Logs Insights, um die Protokollereignisse abzufragen und zu untersuchen, die hinter einer Anomalie stehen.
3. Wenn Sie das deklariert haben `AWS::DevOpsGuru::LogAnomalyDetectionIntegration` Ressourcentyp, entfernen Sie ihn aus Ihren Vorlagen. Siehe Infrastruktur als Code und CLI-Nutzung.

Was ändert sich

Protokollanomalien werden pro Protokollgruppe in angezeigt CloudWatch anstatt in einer Gruppe zu gruppieren DevOps Einblick in den Guru. Um Log-Anomalien mit metrischen Anomalien zu korrelieren, starten Sie Amazon DevOps Untersuchung durch einen Agenten.

Erkennung von Datenbankanomalien

In DevOps Guru für Amazon RDS, Anomalien bei der Datenbankauslastung für Ihre Amazon Relational Database Service- und Amazon Aurora-Datenbanken wurden als Erkenntnisse mit Empfehlungen für die damit verbundenen Warteereignisse gemeldet. In CloudWatch, Database Insights stellt dieselben Performance Insights-Daten bereit, und Sie erstellen Alarme für Warnmeldungen.

Was müssen Sie tun

1. Aktiviere CloudWatch Einblicke in die Datenbank für die Datenbanken, die DevOps Guru für Amazon RDS ist abgedeckt.
2. Erstellen CloudWatch Alarme auf der `DBLoad` Metrik und die Warteereignis-Metriken, die für Ihre Arbeitslast von Bedeutung sind.
3. Integrieren Sie Datenbankalarme in Ihr Amazon-Konto DevOps Neben Ihren Anwendungsalarmen werden auch Ermittlungen von Agenten durchgeführt.

Was ändert sich

Database Insights bietet Dashboards auf Flottenebene und Analysen der wichtigsten Mitwirkenden zur Datenbankbelastung. Die Erkennung von Anomalien beim Laden der Datenbank wird zu einem Alarm, den Sie konfigurieren, und nicht zu einem Einblick, DevOps Guru hat für dich geöffnet.

Untersuchung und Ursachenanalyse

In DevOps Guru, verwandte Anomalien wurden zu einem Einblick mit einer Empfehlung zusammengefasst. AWS DevOps Der Agent bietet AI-assisted Untersuchung, bei der Metriken, Protokolle, Ablaufverfolgungen und aktuelle Bereitstellungen und Konfigurationsänderungen miteinander in Beziehung gesetzt werden, um die eigentliche Ursache zu ermitteln. CloudWatch Untersuchungen bieten dieselbe Art von Untersuchung innerhalb der CloudWatch Konsole.

Was musst du tun

1. Richten Sie Amazon ein DevOps Agent für Ihre Konten.
2. Aktiviere AWS X-Ray und CloudWatch Die Anwendung signalisiert, dass Untersuchungen eine Diensttopologie und einen Verfolgungskontext haben.
3. Konfigurieren CloudWatch Alarme, um eine Untersuchung einzuleiten, oder starten Sie eine bei Bedarf, wenn ein Problem auftritt.

Was ändert sich

Ermittlungen beginnen mit einem Alarm oder auf Anfrage und laufen nicht ununterbrochen ab. Sie erhalten Ursachenhypothesen, die Sie überprüfen und entsprechend handeln können, und Sie können die von Ihnen definierten Behebungs-Runbooks ausführen AWS Systems Manager Automatisierung.

Proaktive Einblicke

In DevOps Guru, proaktive Einblicke warnten dich vor Bedingungen, die zu einem Problem führen könnten, wie z. B. eine Ressource, die ihre Kapazitätsgrenze erreicht, oder eine Konfiguration, die das Risiko erhöht. Proaktive Einblicke sind nicht Teil von CloudWatch oder Amazon DevOps Agent, und sie enden mit dem Service.

Für die Ressourcen, bei denen Frühwarnung für Sie wichtig ist, erstellen Sie CloudWatch Alarme, die Sie benachrichtigen, bevor ein Limit erreicht wird:

1. Erstellen Sie Alarme für Nutzungskennzahlen, deren Schwellenwert unter dem Grenzwert liegt, z. B. bei 80 Prozent der bereitgestellten Kapazität, mit einem Testzeitraum, der lang genug ist, um kurze Spitzen zu ignorieren.
2. Erstellen Sie Alarme zur Nutzung von Servicekontingenten für die Kontingente auf Kontoebene, von denen Ihre Workloads abhängen, wie z. B. gleichzeitige Lambda-Ausführungen und DynamoDB-Kontokapazität. Weitere Informationen finden Sie unter Erstellen CloudWatch Alarme für Dienstkontingente.

Was ändert sich

Sie definieren die Bedingungen, die Sie warnen, und Sie wählen die Ressourcen aus, für die sie gelten. DevOps Guru hat die Bedingungen und Ressourcen für dich ausgewählt.

Infrastruktur als Code und CLI-Nutzung

Vorlagen und Stacks, die auf die folgenden Ressourcentypen verweisen, können nicht erstellt oder aktualisiert werden, nachdem die Ressourcentypen entfernt wurden:

- `AWS::DevOpsGuru::ResourceCollection`
- `AWS::DevOpsGuru::NotificationChannel`
- `AWS::DevOpsGuru::LogAnomalyDetectionIntegration`

Die Terraform AWS Der Anbieter stellt das Äquivalent zur Verfügung `aws_devopsguru_resource_collection`, `aws_devopsguru_notification_channel`, `aws_devopsguru_event_sources_config`, und `aws_devopsguru_service_integration` Ressourcen.

Was musst du tun

1. Inventarisieren Sie die AWS CloudFormation, AWS CDK- und Terraform-Vorlagen und die AWS CLI-Skripte, die auf diese Ressourcentypen verweisen.
2. Erstellen Sie das Äquivalent CloudWatch Konfiguration: die Alarme, Amazon SNS-Themen und Amazon EventBridge Regeln, die deine ersetzen DevOps Guru-Benachrichtigungskanal und Berichterstattung sowie CloudWatch Protokolliert Anomaliedetektoren, die die Integration zur Erkennung von Protokollanomalien ersetzen.

3. Entfernen Sie den DevOps Nutze Ressourcen aus deinen Vorlagen und setze die Änderung so ein, dass die Ressourcen nicht mehr von deinen Stacks verwaltet werden. Entferne sie aus deinen Vorlagen, anstatt sie sofort zu löschen, damit deine Stapel und Vorlagen immer im Einklang sind.

Was ändert sich

Da eine einzelne ausgefallene Ressource einen gesamten Stack-Vorgang blockieren kann, ist dies die schwerste Auswirkung. Vervollständigen Sie es zuerst.

API-Integrationen

Wenn Ihre Dashboards, Ticketsysteme oder internen Tools den aufrufen DevOps Guru-API, aktualisiere sie, um das Äquivalent zu verwenden CloudWatch API-Operationen vor dem Ende des Supports. Nach dem Ende des Supports DevOps Guru-API-Operationen sind nicht mehr verfügbar.

Wenn Ihre Tools aufrufen	Stattdessen verwenden
`ListInsights` , `DescribeInsight` , `ListAnomaliesForInsight`	CloudWatch `DescribeAlarms` , `DescribeAlarmHistory` , und `GetMetricData` ; CloudWatch Logs `ListLogAnomalyDetectors` und `ListAnomalies`
`ListRecommendations`	Amazon DevOps Ergebnisse der Untersuchung durch den Agenten
`DescribeAccountHealth` , `DescribeResourceCollectionHealth`	CloudWatch `DescribeAlarms` gefiltert nach Alarmstatus oder einem kombinierten Alarm für jede Anwendung
`ListNotificationChannels` , `AddNotificationChannel`	Amazon SNS-Themen und Amazon EventBridge Regeln für CloudWatch Änderungen des Alarmzustands

API-Details finden Sie in der Amazon DevOps Guru API-Referenz und die Amazon CloudWatch API-Referenz.

Exportiere deine Daten

DevOps Guru-Einblicke sind nach dem 30. September 2027 nicht mehr verfügbar. Wenn du deine Erkenntnisse aufzeichnen möchtest, exportiere sie vor diesem Datum. Wir empfehlen den meisten Kunden, beide der folgenden Schritte zu tun:

1. Erfassen Sie bis zum Ende des Supports neue Erkenntnisse. Konfigurieren Sie einen Amazon SNS-Benachrichtigungskanal, sodass jeder neue Einblick zu einem Thema bereitgestellt wird, das Sie archivieren können.
2. Exportieren Sie die Erkenntnisse, die Sie bereits gesammelt haben. Rufen Sie an `ListInsights` um sie aufzulisten, dann ruf an `DescribeInsight`, `ListAnomaliesForInsight`, und `ListRecommendations` für jede Einsicht, die du behalten möchtest. Speichern Sie die Antworten in Amazon S3 oder Ihrem Ticketsystem.

Schließen Sie Ihren Export ab, bevor Sie den Versicherungsschutz reduzieren oder Ressourcen entfernen.

Löschen Sie Ihre DevOps Guru-Ressourcen

Wenn Sie vor Ende des Supports die Analyse beenden und keine Gebühren mehr anfallen möchten, entfernen Sie Ihren Servicebereich und Ihre Benachrichtigungskanäle, nachdem Sie Ihre Daten exportiert und Ihr CloudWatch Konfiguration.

1. Stellen Sie Ihren Analyseumfang ein auf Keine für jedes Konto und AWS Region wo DevOps Guru ist aktiviert. Wählen Sie in der Konsole Einstellungen, dann DevOps Berichterstattung über die Guru-Analyse, dann Managen, dann Keine. Du kannst auch anrufen `UpdateResourceCollection` um das zu entfernen CloudFormation Stapel oder Tags, die Ihre Abdeckungsgrenze definieren.
2. Entferne deine Benachrichtigungskanäle. Rufen Sie an `RemoveNotificationChannel`, oder lösche sie von Einstellungen in der Konsole. Durch das Entfernen eines Kanals wird weder das Amazon SNS-Thema noch etwas gelöscht, das Sie bereits über diesen Kanal archiviert haben.
3. Wenn du erklärst DevOps Guru-Ressourcen in der Infrastruktur als Code, entfernen Sie sie aus Ihren Vorlagen, anstatt sie Out-of-Band zu löschen. Siehe Infrastruktur als Code und CLI-Nutzung.

Zeitplan und Support

Meilenstein	Date
Ankündigung	29. September 2026
Keine neuen Kunden	29. Oktober 2026
Empfohlener Abschluss der Umstellung	30. Juni 2027
Ende des Supports	30. September 2027

Wir empfehlen, Ihre Umstellung bis zum 30. Juni 2027 abzuschließen, damit Sie Ihre CloudWatch und Amazon DevOps Agentenkonfiguration gegen Live-Betrieb während DevOps Guru ist immer noch zum Vergleich verfügbar. Wenn Sie während der Umstellung Fragen haben, wenden Sie sich an AWS Unterstützung.

Checkliste für den Übergang

- Inventar AWS CloudFormation, AWS CDK, Terraform und AWS CLI-Verwendung von `AWS::DevOpsGuru::ResourceCollection`, `AWS::DevOpsGuru::NotificationChannel`, und `AWS::DevOpsGuru::LogAnomalyDetectionIntegration`.
- Identifizieren Sie jede API-Integration, die liest DevOps Einblicke in Gurus.
- Aktiviere CloudWatch Erkennung von Anomalien anhand Ihrer wichtigsten Kennzahlen und Erstellen von Alarmen.
- Aktiviere CloudWatch Protokolliert die Erkennung von Anomalien in Ihren kritischen Protokollgruppen.
- Aktivieren CloudWatch Database Insights für die Datenbanken, die DevOps Guru für Amazon RDS ist abgedeckt.
- Aktiviere AWS X-Ray und CloudWatch Anwendungssignale.
- Richten Sie Amazon ein DevOps Beauftragter für Ermittlungen.
- Konfigurieren Sie Benachrichtigungen mit Amazon SNS, Amazon EventBridge, oder Systems Manager OpsCenter.
- Exportieren DevOps Guru-Einblicke über einen Amazon SNS-Benachrichtigungskanal und die API.

- Entfernen DevOps Nutzen Sie die Ressourcen aus Ihren Vorlagen und setzen Sie die Analyseabdeckung auf Keine.

Häufig gestellte Fragen

Funktionieren meine Anwendungen oder Datenbanken nach dem Ende des Supports nicht mehr?

Nein. DevOps Guru ist ein Überwachungsdienst. Er beobachtet die Ressourcen, die Sie ausführen, er hostet sie nicht. Nach Ende des Supports verlieren Sie DevOps Gurus Sichtbarkeit und Empfehlungen, aber deine Workloads laufen weiter.

Was passiert, wenn ich nicht rechtzeitig migriere?

Sie werden nicht mehr auf das zugreifen können DevOps Guru-Konsole oder API und DevOps Guru-Ressourcentypen werden fehlschlagen AWS CloudFormation und der AWS CLIP. Insights wird nicht mehr verfügbar sein.

Kann ich es weiter verwenden DevOps Guru bis zum Ende des Supports?

Ja, wenn Ihr Konto vor dem 29. Oktober 2026 registriert wurde. Bis zum Ende des Supports bieten wir Sicherheitspatches, kritische Fehlerkorrekturen, Support und ständige Verfügbarkeit. Es werden keine neuen Funktionen hinzugefügt.

Gibt es einen einzigen Dienst, der ersetzt DevOps Guru eins zu eins?

Nein. DevOps Karten zur Erkennung und Alarmierung durch Guru an Amazon CloudWatch, und seine Untersuchung und Ursachenanalyse sind Amazon zuzuordnen DevOps Bevollmächtigter. Sie können beide zusammen verwenden.

Was passiert mit DevOps Guru für Amazon RDS?

Es endet mit dem Rest des Dienstes. CloudWatch Database Insights bietet dieselben Performance Insights-Daten. Erstellen Sie beim Laden der Datenbank Alarme zur Alarmierung.

Zugehörige Ressourcen

- Ende des Supports für Amazon DevOps Guru
- Dienstleistungen in Sunset in der AWS Allgemeine Referenz
- Amazon CloudWatch Benutzerleitfaden
- Verwenden CloudWatch Erkennung von Anomalien

- CloudWatch Protokolliert die Erkennung von Anomalien
- CloudWatch Database Insights
- CloudWatch Untersuchungen
- Amazon DevOps Benutzerhandbuch für Agenten
- Amazon CloudWatch Preisgestaltung
- AWS Support

Amazon einrichten DevOps Guru

Erledigen Sie die Aufgaben in diesem Abschnitt, um Amazon einzurichten DevOps Guru zum ersten Mal. Wenn du schon eine hast AWS Konto, weißt du welches AWS Konto oder Konten, die Sie analysieren möchten und für die Sie ein Amazon Simple Notification Service-Thema haben, das Sie für Insight-Benachrichtigungen verwenden können, können Sie direkt zu Erste Schritte mit DevOps Guru.

Optional können Sie Quick Setup verwenden, eine Funktion von AWS Systems Manager, zum Einrichten DevOps Guru und konfiguriere schnell seine Optionen. Sie können Quick Setup zur Einrichtung verwenden DevOps Guru für ein eigenständiges Konto oder eine Organisation. So verwenden Sie Quick Setup im Systems Manager zur Einrichtung DevOps Guru für eine Organisation, du musst die folgenden Voraussetzungen erfüllen:

- Eine Organisation mit AWS Organizations. Weitere Informationen finden Sie unter AWS Organizations Terminologie und Konzepte in der AWS Organizations Benutzerleitfaden.
- Zwei oder mehr Organisationseinheiten (OUs).
- Ein oder mehrere Ziele AWS Konten in jeder OU.
- Ein Administratorkonto mit Rechten zur Verwaltung der Zielkonten.

Um zu erfahren, wie man es einrichtet DevOps Guru, der Quick Setup verwendet, siehe Konfigurieren DevOps Guru mit Schnelleinrichtung in der AWS Systems Manager Benutzerleitfaden.

Verwenden Sie die folgenden Schritte zur Einrichtung DevOps Guru ohne Quick Setup.

- Schritt 1 — Melde dich an für AWS
- Schritt 2 — Ermitteln Sie den Versicherungsschutz für DevOps Guru
- Schritt 3 — Identifizieren Sie Ihr Thema für Amazon SNS-Benachrichtigungen

Schritt 1 — Melde dich an für AWS

Melde dich für einen an AWS-Konto

Um loszulegen mit AWS, du brauchst eine AWS-Konto. Es gibt zwei Möglichkeiten, sich anzumelden AWS. Wenn Sie die vollständige Kontrolle über die Kontokonfiguration und den Speicherort Ihrer

Inhalte haben möchten oder wenn Sie regulierte Workloads wie HIPAA oder FedRAMP haben, verwenden Sie Melden Sie sich an für AWS (fortgeschritten). Wenn Sie ein neuer Benutzer sind und ein Konto verwenden möchten, das Sie bereits besitzen, um sich anzumelden AWS und erstellen Sie eine AWS Umgebung mit vorkonfigurierten Standardwerten in select AWS-Regionen, verwenden Melde dich an für AWS.

Schritt 2 — Ermitteln Sie den Versicherungsschutz für DevOps Guru

Ihre Grenzabdeckung bestimmt die AWS Ressourcen, die von Amazon analysiert werden DevOps Guru für anomales Verhalten. Wir empfehlen Ihnen, Ihre Ressourcen in Ihre betrieblichen Anwendungen zu gruppieren. Alle Ressourcen innerhalb Ihrer Ressourcengrenze sollten eine oder mehrere Ihrer Anwendungen umfassen. Wenn Sie eine betriebsbereite Lösung haben, sollte Ihre Abdeckungsgrenze alle Ressourcen umfassen. Wenn Sie mehrere Anwendungen haben, wählen Sie die Ressourcen aus, aus denen sich jede Lösung zusammensetzt, und gruppieren Sie sie mithilfe von CloudFormation Stapel oder AWS Schlagworte. Alle kombinierten Ressourcen, die Sie angeben, werden analysiert, unabhängig davon, ob sie eine oder mehrere Anwendungen definieren DevOps Guru und lege seine Deckungsgrenze fest.

Verwenden Sie eine der folgenden Methoden, um die Ressourcen in Ihren Betriebslösungen anzugeben.

- Wählen Sie Ihre AWS Region und Konto definieren Ihre Deckungsgrenze. Mit dieser Option DevOps Guru analysiert alle Ressourcen in deinem Konto und deiner Region. Dies ist eine gute Option, wenn du dein Konto nur für eine Anwendung verwendest.
- Benutzen CloudFormation Stacks, um die Ressourcen in Ihrer betrieblichen Anwendung zu definieren. CloudFormation Vorlagen definieren und generieren Ihre Ressourcen für Sie. Geben Sie bei der Konfiguration die Stacks an, die Ihre Anwendungsressourcen erstellen DevOps Guru. Du kannst deine Stacks jederzeit aktualisieren. Alle Ressourcen in den von Ihnen ausgewählten Stacks definieren Ihre Grenzabdeckung. Weitere Informationen finden Sie unter Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- Verwenden AWS zu spezifizierende Stichwörter AWS Ressourcen in Ihren Anwendungen. DevOps Guru analysiert nur die Ressourcen, die die von Ihnen ausgewählten Tags enthalten. Diese Ressourcen bilden deine Grenze.

  Ein AWS Tag besteht aus einem Tag Schlüssel und ein Etikett Wert. Sie können ein Tag angeben Schlüssel und Sie können einen oder mehrere angeben Werte damit Schlüssel. Benutze einen

Wert für alle Ressourcen in einer Ihrer Anwendungen. Wenn Sie mehrere Anwendungen haben, verwenden Sie ein Tag mit demselben Schlüssel für alle und gruppieren Sie die Ressourcen mithilfe der Tags in Ihren Anwendungen Werte. Alle Ressourcen mit den von Ihnen ausgewählten Tags bilden die Deckungsgrenze für DevOps Guru. Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.

Wenn Ihr Geltungsbereich Ressourcen umfasst, aus denen mehr als eine Anwendung besteht, können Sie Ihre Erkenntnisse mithilfe von Tags filtern, sodass sie jeweils von einer Anwendung angezeigt werden. Weitere Informationen finden Sie in Schritt 4 unter Einblicke von DevOps Guru anzeigen.

Weitere Informationen finden Sie unter Definieren von Anwendungen mithilfe von AWS Ressourcen. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preisgestaltung.

Schritt 3 — Identifizieren Sie Ihr Thema für Amazon SNS-Benachrichtigungen

Sie verwenden ein oder zwei Amazon SNS-Themen, um Benachrichtigungen über wichtige Themen zu generieren DevOps Guru-Ereignisse, z. B. wenn eine Einsicht entsteht. Dadurch wird sichergestellt, dass Sie über Probleme informiert sind, die DevOps Guru findet so schnell wie möglich. Halte deine Themen bereit, wenn du sie einrichtest DevOps Guru. Wenn du den benutzt DevOps Guru-Konsole zum Einrichten DevOps Guru, du gibst ein Benachrichtigungsthema mit seinem Namen oder seinem Amazon-Ressourcennamen (ARN) an. Weitere Informationen finden Sie unter Aktiviere DevOps Guru. Sie können die Amazon SNS-Konsole verwenden, um den Namen und den ARN für jedes Ihrer Themen einzusehen. Wenn Sie kein Thema haben, können Sie eines erstellen, wenn Sie es aktivieren DevOps Guru benutzt den DevOps Guru-Konsole. Weitere Informationen finden Sie unter Ein Thema erstellen in der Amazon Simple Notification Service — Entwicklerhandbuch.

Ihrem Amazon SNS-Thema wurden Berechtigungen hinzugefügt

Ein Amazon SNS-Thema ist eine Ressource, die eine enthält AWS Identity and Access Management (IAM) -Ressourcenrichtlinie. Wenn Sie hier ein Thema angeben, DevOps Guru fügt seiner Ressourcenrichtlinie die folgenden Berechtigungen hinzu.

```
{
```

```
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

Diese Berechtigungen sind erforderlich für DevOps Guru, um Benachrichtigungen zu einem Thema zu veröffentlichen. Wenn du es vorziehst, diese Berechtigungen für das Thema nicht zu haben, kannst du sie getrost entfernen und das Thema funktioniert weiterhin so, wie es war, bevor du es ausgewählt hast. Wenn diese angehängten Berechtigungen jedoch entfernt werden, DevOps Guru kann das Thema nicht verwenden, um Benachrichtigungen zu generieren.

Schätzung der Kosten für die Amazon DevOps Guru-Ressourcenanalyse

Sie können Ihre monatlichen Kosten für Amazon DevOps Guru für die Analyse Ihrer AWS-Ressourcen schätzen. Sie zahlen für die Anzahl der analysierten Stunden für jede aktive AWS-Ressource im Rahmen Ihrer angegebenen Ressourcenabdeckung. Eine Ressource ist aktiv, wenn sie innerhalb einer Stunde Metriken, Ereignisse oder Protokolle generiert.

DevOps Guru scannt deine ausgewählten Ressourcen, um einen monatlichen Kostenvoranschlag zu erstellen. Du kannst dir die Ressourcen, ihren fakturierbaren Stundenpreis und ihre geschätzte monatliche Gebühr ansehen. Der Kostenschätzer geht standardmäßig davon aus, dass die analysierten aktiven Ressourcen zu 100 Prozent genutzt werden. Sie können diesen Prozentsatz für jeden analysierten Service auf der Grundlage Ihrer geschätzten Nutzung ändern, um eine aktualisierte monatliche Kostenschätzung zu erstellen. Die Schätzung bezieht sich auf die Kosten für die Analyse Ihrer Ressourcen und beinhaltet keine Kosten im Zusammenhang mit DevOps Guru-API-Aufrufen.

Sie können jeweils einen Kostenvoranschlag erstellen. Wie lange es dauert, einen Kostenvoranschlag zu erstellen, hängt von der Anzahl der Ressourcen ab, die Sie bei der Erstellung des Kostenvoranschlags angeben. Wenn Sie einige Ressourcen angeben, kann es 1 bis 2 Stunden dauern, bis der Vorgang abgeschlossen ist. Wenn Sie viele Ressourcen angeben, kann es bis zu 4 Stunden dauern, bis der Vorgang abgeschlossen ist. Ihre tatsächlichen Kosten variieren und hängen davon ab, wie viel Zeit Ihre analysierten aktiven Ressourcen genutzt werden.

> **Note**
>
> Für eine Kostenschätzung können Sie nur einen CloudFormation Stapel angeben. Für Ihre tatsächliche Deckungsgrenze können Sie bis zu 1000 Stapel angeben.

Um eine monatliche Kostenschätzung für eine Ressourcenanalyse zu erstellen

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich die Option Cost Estimator aus.
3. Wenn Sie DevOps Guru nicht aktiviert haben, müssen Sie eine IAM-Rolle erstellen. Wählen Sie im daraufhin angezeigten Popup-Fenster „IAM-Rolle für DevOps Guru erstellen“ die Option

Zustimmen, um die IAM-Rolle zu erstellen. Auf diese Weise kann DevOps Guru eine mit dem Service verknüpfte IAM-Rolle für Sie erstellen, wenn Sie mit der Kostenvoranschlagsanalyse beginnen oder Guru verwenden möchten. DevOps Auf diese Weise verfügt DevOps Guru über die erforderlichen Berechtigungen, um den Kostenvoranschlag zu erstellen. Wenn Sie DevOps Guru bereits aktiviert haben, wurde die Rolle bereits erstellt und diese Option wird nicht angezeigt.

4. Wählen Sie die Ressourcen aus, die Sie für die Erstellung Ihrer Schätzung verwenden möchten.

   - Gehen Sie wie folgt vor, wenn Sie die Kosten abschätzen möchten, die DevOps Guru für die Analyse der durch einen CloudFormation Stapel definierten Ressourcen benötigt.
     1. Wählen Sie den CloudFormation Stapel in der aktuellen Region aus.
     2. Wählen Sie unter CloudFormation Stapel auswählen den Namen eines CloudFormation Stacks in Ihrem AWS Konto aus. Sie können auch den Namen eines Stacks eingeben, um ihn schnell zu finden. Informationen zum Arbeiten mit und Anzeigen Ihrer Stacks finden Sie unter Arbeiten mit Stacks im CloudFormation Benutzerhandbuch.
     3. (Optional) Wenn Sie einen CloudFormation Stack verwenden, den Sie derzeit nicht analysieren, wählen Sie „Ressourcenanalyse aktivieren“, damit DevOps Guru mit der Analyse seiner Ressourcen beginnen kann. Diese Option ist nicht verfügbar, wenn Sie DevOps Guru nicht aktiviert haben oder wenn Sie bereits die Ressourcen im Stack analysieren.
   - Wenn Sie die Kosten abschätzen möchten, die DevOps Guru für die Analyse von Ressourcen mit einem Tag benötigt, gehen Sie wie folgt vor.
     1. Wähle „Tags“ AWS für Ressourcen in der aktuellen Region
     2. Wählen Sie unter Tag-Schlüssel den Schlüssel Ihres Tags
     3. Wählen Sie unter Tag-Wert (alle Werte) oder wählen Sie einen Wert aus.
   - Wenn du die Kosten schätzen möchtest, die DevOps Guru für die Analyse der Ressource in deinem AWS Konto und deiner Region benötigt, wähle „AWS Konto in der aktuellen Region“.
5. Wähle „Monatliche Kosten schätzen“.
6. (Optional) Geben Sie in der Spalte Aktive Ressourcenauslastung% einen aktualisierten Prozentwert für einen oder mehrere AWS-Services ein. Die Standardeinstellung für die aktive Ressourcenauslastung in% ist 100%. Das bedeutet, dass DevOps Guru die Schätzung für den AWS-Service generiert, indem er die Kosten einer Stunde für die Analyse seiner Ressourcen berechnet und diese dann über 30 Tage hochrechnet, was insgesamt 720 Stunden ergibt. Wenn ein Service zu weniger als 100% der Zeit aktiv ist, können Sie den Prozentsatz auf der Grundlage Ihrer geschätzten Nutzung aktualisieren, um eine genauere Schätzung zu erhalten.

Wenn Sie beispielsweise die aktive Ressourcenauslastung eines Dienstes auf 75% aktualisieren, werden die Kosten für eine Stunde für die Analyse der Ressourcen auf (720 x 0,75) Stunden oder 540 Stunden extrapoliert.

Wenn Ihre Schätzung bei null Dollar liegt, enthalten die von Ihnen ausgewählten Ressourcen wahrscheinlich keine Ressourcen, die von Guru unterstützt werden. DevOps Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

Erste Schritte mit DevOps Guru

In diesem Abschnitt erfahren Sie, wie Sie mit Amazon beginnen DevOps Guru, damit es die Betriebsdaten und Metriken Ihrer Anwendung analysieren kann, um Erkenntnisse zu gewinnen.

Themen

- Schritt 1: Richten Sie sich ein
- Schritt 2: Aktivieren DevOps Guru
- Schritt 3: Geben Sie Ihre an DevOps Berichterstattung über Guru-Ressourcen

Schritt 1: Richten Sie sich ein

Bevor Sie beginnen, bereiten Sie sich vor, indem Sie die Schritte unter durchgehen Amazon einrichten DevOps Guru.

Schritt 2: Aktivieren DevOps Guru

Um Amazon zu konfigurieren DevOps Guru zum ersten Mal verwenden, du musst wählen, wie du es einrichten möchtest DevOps Guru. Sie können entweder Anwendungen in Ihrem gesamten Unternehmen oder Anwendungen in Ihrem Girokonto überwachen.

Sie können entweder Ihre Anwendungen in Ihrem gesamten Unternehmen überwachen oder aktivieren DevOps Guru ausschließlich für das Girokonto. In den folgenden Verfahren werden verschiedene Einrichtungsmöglichkeiten beschrieben DevOps Guru, der auf deine Bedürfnisse zugeschnitten ist.

Überwachen Sie Konten in Ihrer gesamten Organisation

Wenn Sie sich dafür entscheiden, Anwendungen in Ihrem gesamten Unternehmen zu überwachen, melden Sie sich bei Ihrem Organisationsverwaltungskonto an. Sie können optional ein Mitgliedskonto einer Organisation als einrichten delegierter Administrator. Sie können jeweils nur einen delegierten Administrator haben und die Administratoreinstellungen später ändern. Sowohl das Verwaltungskonto als auch das Konto für delegierte Administratoren, die Sie eingerichtet haben, haben Zugriff auf alle Einblicke in allen Konten in Ihrer Organisation.

Sie können entweder mithilfe der Konsole kontoübergreifende Unterstützung für Ihre Organisation hinzufügen, oder Sie können dies tun, indem Sie AWS CLI.

An Bord mit dem DevOps Guru-Konsole

Sie können die Konsole verwenden, um Unterstützung für Konten in Ihrer gesamten Organisation hinzuzufügen.

Verwenden Sie die Konsole, um Folgendes zu aktivieren DevOps Guru zum Ansehen aggregierter Erkenntnisse

1. Öffne den Amazonas DevOps Guru-Konsole bei https://console.aws.amazon.com/devops-guru/.
2. Wählen Überwachen Sie Anwendungen in Ihren Organisationen als Setup-Typ.
3. Wählen Sie aus, welches Konto Sie als delegierten Administrator verwenden möchten. Wählen Sie dann Registrieren Sie den delegierten Administrator. Dies bietet Zugriff auf eine konsolidierte Ansicht für jedes Konto, das DevOps Guru aktiviert. Der delegierte Administrator hat eine konsolidierte Ansicht aller DevOps Einblicke und Kennzahlen von Guru in Ihrem gesamten Unternehmen. Sie können andere Konten mit SSM Quick Setup aktivieren oder AWS CloudFormation Sätze stapeln. Weitere Informationen zur Schnelleinrichtung finden Sie unter Konfigurieren DevOps Guru mit Schnelleinrichtung. Weitere Informationen zum Einrichten mit Stack-Sets finden Sie unter Mit Stapeln arbeiten in der CloudFormation Benutzerleitfaden, und Schritt 2 — Ermitteln Sie den Versicherungsschutz für DevOps Guru. und Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

An Bord mit dem AWS CLI

Sie können das benutzen AWS CLI zum Aktivieren DevOps Guru, um aggregierte Erkenntnisse zu sehen. Führen Sie die folgenden Befehle aus.

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

In der folgenden Tabelle werden die Befehle beschrieben.

Befehl	Description
`create-service-linked-role`	Gibt DevOps Erlaubnis von Guru, Informati onen über Ihre Organisation zu sammeln. Fahren Sie nicht fort, wenn dieser Schritt nicht erfolgreich ist.
`enable-aws-service-access`	Integriert Ihr Unternehmen in DevOps Guru.
`register-delegated-administrator`	Ermöglicht den Zugriff auf das Mitgliedskonto, um Einblicke einzusehen.

Überwachen Sie Ihr Girokonto

Wenn Sie sich dafür entscheiden, Anwendungen in Ihrem aktuellen Konto zu überwachen AWS Konto, wählen Sie welches AWS Ressourcen in Ihrem Konto und Ihrer Region werden behandelt oder analysiert und geben ein oder zwei Amazon Simple Notification Service-Themen an, anhand derer Sie benachrichtigt werden, wenn ein Einblick erstellt wird. Sie können diese Einstellungen später bei Bedarf aktualisieren.

Aktiviere DevOps Guru zur Überwachung von Anwendungen in Ihrem aktuellen AWS Konto

1. Öffne den Amazonas DevOps Guru-Konsole bei https://console.aws.amazon.com/devops-guru/.
2. Wählen Überwachen Sie Anwendungen im aktuellen AWS Konto als Setup-Typ.
3. In DevOps Berichterstattung über die Guru-Analyse, wählen Sie eine der folgenden Optionen.
   - Analysieren Sie alles AWS Ressourcen im aktuellen AWS Konto: DevOps Guru analysiert alles AWS Ressourcen in deinem Konto.
   - Wählen Sie AWS-Ressourcen aus, um sie später zu analysieren: Sie wählen Ihre Analysegrenze später aus. Weitere Informationen erhalten Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru und Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps.

DevOps Guru kann jede Ressource analysieren, die mit dem verknüpft ist AWS Konto, das es unterstützt. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preisgestaltung.

4. Sie können bis zu zwei Themen hinzufügen. DevOps Guru verwendet das Thema oder die Themen, um dich über wichtige Informationen zu informieren DevOps Guru-Ereignisse, wie die Schaffung einer neuen Einsicht. Wenn Sie jetzt kein Thema angeben, können Sie später eines hinzufügen, indem Sie Einstellungen im Navigationsbereich.

   a. In Geben Sie ein Amazon SNS-Thema an, wählen Sie ein zu verwendendes Thema aus.

   b. Gehen Sie wie folgt vor, um ein Amazon SNS-Thema hinzuzufügen.

      - Wählen Sie Generieren Sie ein neues SNS-Thema per E-Mail. Dann, von Geben Sie die E-Mail-Adresse an, geben Sie die E-Mail-Adresse ein, an die Sie Benachrichtigungen erhalten möchten. Um weitere E-Mail-Adressen einzugeben, wählen Sie Neue E-Mail hinzufügen.
      - Wählen Verwenden Sie ein vorhandenes SNS-Thema. Dann, von Wähle ein Thema in deinem AWS Konto, wählen Sie das Thema, das Sie verwenden möchten.
      - Wählen Sie Verwenden Sie einen vorhandenen SNS-Thema-ARN, um ein vorhandenes Thema aus einem anderen Konto anzugeben. Dann, in Geben Sie einen ARN für ein Thema ein, geben Sie den Themen-ARN ein. Der ARN ist der Amazon-Ressourcenname des Themas. Sie können ein Thema in einem anderen Konto angeben. Wenn Sie ein Thema in einem anderen Konto verwenden, müssen Sie dem Thema eine Ressourcenrichtlinie hinzufügen. Weitere Informationen finden Sie unter Berechtigungen für Amazon SNS-Themen.

5. Wählen Sie Enable (Aktivieren) aus.

Um Amazon zu konfigurieren DevOps Guru, den du zum ersten Mal benutzen möchtest, musst du wählen, welchen AWS Ressourcen in Ihrem Konto und Ihrer Region werden behandelt oder analysiert. Geben Sie ein oder zwei Amazon Simple Notification Service-Themen an, anhand derer Sie benachrichtigt werden, wenn ein Einblick erstellt wird. Sie können diese Einstellungen später bei Bedarf aktualisieren.

Schritt 3: Geben Sie Ihre an DevOps Berichterstattung über Guru-Ressourcen

Wenn Sie angeben möchten AWS Ressourcen, die Sie später aktiviert haben DevOps Guru, du musst das wählen CloudFormation Stapel in deinem AWS Konto, das die Ressourcen erstellt, die Sie analysieren möchten. Ein CloudFormation Stack ist eine Sammlung von AWS Ressourcen, die Sie als eine Einheit verwalten. Sie können einen oder mehrere Stacks verwenden, um alle Ressourcen einzubeziehen, die für die Ausführung Ihrer betrieblichen Anwendungen erforderlich sind, und sie dann so spezifizieren, dass sie von DevOps Guru. Wenn Sie keine Stapel angeben, dann DevOps Guru analysiert alle AWS Ressourcen in Ihrem Konto. Weitere Informationen finden Sie unter Mit Stapeln arbeiten in der CloudFormation Benutzerleitfaden, und Ermitteln Sie den Versicherungsschutz für DevOps Guru. und Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

> **Note**
>
> Weitere Informationen zu unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preisgestaltung.

Spezifizieren DevOps Berichterstattung über Guru-Ressourcen

1. Öffne den Amazonas DevOps Guru-Konsole bei https://console.aws.amazon.com/devops-guru/.
2. Erweitern Einstellungen im Navigationsbereich.
3. In Analysierte Ressourcen, wähle Analysierte Ressourcen bearbeiten.
4. Wählen Sie eine der folgenden Deckungsoptionen.

   - Wählen Sie Alle Kontoressourcen wenn du willst DevOps Guru zur Analyse aller unterstützten Ressourcen in Ihrem AWS Konto und Region. Wenn Sie diese Option wählen, wird Ihr AWS Konto ist die Grenze für den Geltungsbereich der Ressourcenanalyse. Alle Ressourcen in jedem Stack in Ihrem Konto sind in einer eigenen Anwendung gruppiert. Alle verbleibenden Ressourcen, die sich nicht in einem Stapel befinden, werden in einer eigenen Anwendung gruppiert.
   - Wählen Sie CloudFormation Stapel wenn du willst DevOps Guru, um die Ressourcen zu analysieren, die sich in Stapeln befinden, die Sie auswählen, und wählen Sie dann eine der folgenden Optionen.

- Alle Ressourcen — Alle Ressourcen, die sich in Ihrem Konto in Stapeln befinden, werden analysiert. Die Ressourcen in jedem Stapel werden in einer eigenen Anwendung gruppiert. Alle Ressourcen in Ihrem Konto, die sich nicht in einem Stapel befinden, werden nicht analysiert.
- Wähle Stapel aus — Wählen Sie die gewünschten Stapel aus DevOps Guru zum Analysieren. Die Ressourcen in jedem Stack, den Sie auswählen, sind in einer eigenen Anwendung gruppiert. Sie können den Namen eines Stacks in eingeben Finde Stapel um schnell einen bestimmten Stapel zu finden. Sie können bis zu 1.000 Stapel auswählen.

Weitere Informationen finden Sie unter Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

- Wählen Sie Schlagworte wenn du willst DevOps Guru, um alle Ressourcen zu analysieren, die die von Ihnen ausgewählten Tags enthalten. Wähle eine Schlüssel, wählen Sie dann eine der folgenden Optionen.
  - Alle Kontoressourcen — Analysiert alle AWS-Ressourcen in der aktuellen Region und im aktuellen Konto. Ressourcen mit dem ausgewählten Tag-Schlüssel werden nach Tag-Werten gruppiert, falls vorhanden. Ressourcen ohne diesen Tag-Schlüssel werden gruppiert und separat analysiert.
  - Wählen Sie bestimmte Tag-Werte — Alle Ressourcen, die ein Tag mit dem Schlüssel die Sie ausgewählt haben, werden analysiert. DevOps Guru gruppiert deine Ressourcen nach deinen Stichwörtern in Anwendungen Werte.

  Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.
- Wählen Keine wenn du nicht willst DevOps Guru, um alle Ressourcen zu analysieren. Diese Option deaktiviert DevOps Guru, damit Ihnen keine Kosten für die Ressourcenanalyse entstehen.

5. Wählen Sie Speichern.

Aktivierung von AWS Diensten für die DevOps Guru-Analyse

Amazon DevOps Guru kann die Leistung jeder AWS Ressource analysieren, die es unterstützt. Wenn es ein ungewöhnliches Verhalten feststellt, generiert es einen Einblick mit Details über das Verhalten und darüber, wie es behoben werden kann. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

DevOpsGuru verwendet CloudWatch Amazon-Metriken, AWS CloudTrail Ereignisse und mehr, um Ressourcen zu analysieren. Die meisten der unterstützten Ressourcen generieren die für die DevOps Guru-Analyse erforderlichen Metriken automatisch. Bei einigen AWS Diensten sind jedoch zusätzliche Maßnahmen erforderlich, um die erforderlichen Metriken zu generieren. Bei einigen Diensten bietet die Aktivierung dieser Metriken eine zusätzliche Analyse der bestehenden DevOps Guru-Berichterstattung. Bei anderen ist eine Analyse erst möglich, wenn Sie diese Metriken aktivieren. Weitere Informationen erhalten Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru und Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps.

Dienste, bei denen Maßnahmen für die DevOps Guru-Analyse erforderlich sind

- Amazon Elastic Container Service — Um zusätzliche Metriken zu generieren, mit denen DevOps Guru seine Ressourcen besser abdeckt, folgen Sie den Schritten unter Container Insights auf Amazon ECS einrichten. Dadurch können CloudWatch Amazon-Gebühren anfallen.
- Amazon Elastic Kubernetes Service — Um Metriken für DevOps Guru zur Analyse zu generieren, folgen Sie den Schritten unter Container-Insights auf Amazon EKS und Kubernetes einrichten. DevOpsGuru analysiert keine Amazon EKS-Ressourcen, bis die Generierung dieser Metriken eingerichtet ist. Dadurch können CloudWatch Amazon-Gebühren anfallen.
- Amazon Simple Storage Service — Um Metriken für DevOps Guru zur Analyse zu generieren, müssen Sie Metriken anfordern aktivieren. Folgen Sie den Schritten unter CloudWatch Metrikkonfiguration für alle Objekte in Ihrem Bucket erstellen. DevOps Guru analysiert keine Amazon S3 S3-Ressourcen, bis die Generierung dieser Metriken eingerichtet ist. Dadurch können Gebühren CloudWatch für Amazon S3 anfallen.

Weitere Informationen finden Sie unter CloudWatch Amazon-Preise.

Mit Erkenntnissen in DevOps Guru arbeiten

Amazon DevOps Guru generiert Erkenntnisse, wenn es anomales Verhalten in Ihren betrieblichen Anwendungen erkennt. DevOpsGuru analysiert die Metriken, Ereignisse und mehr in den AWS Ressourcen, die Sie bei der Einrichtung DevOps von Guru angegeben haben. Jeder Einblick enthält eine oder mehrere Empfehlungen, anhand derer Sie das Problem beheben können. Es enthält auch eine Liste der Metriken, eine Liste der Protokollgruppen und eine Liste der Ereignisse, anhand derer das ungewöhnliche Verhalten identifiziert wurde.

Es gibt zwei Arten von Erkenntnissen.

- Reaktive Einblicke enthalten Empfehlungen, mit denen Sie Probleme lösen können, die gerade auftreten.
- Proaktive Einblicke enthalten Empfehlungen, die sich mit Problemen befassen, von denen DevOps Guru prognostiziert, dass sie in future auftreten werden.

Themen

- Einblicke von DevOps Guru anzeigen
- Einblicke in der DevOps Guru-Konsole verstehen
- Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden
- Den Schweregrad von Erkenntnissen verstehen

Einblicke von DevOps Guru anzeigen

Sie können Ihre Erkenntnisse mit dem einsehen AWS-Managementkonsole.

Sehen Sie sich Ihre DevOps Guru-Erkenntnisse an

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und wählen Sie dann Insights.
3. Auf der Registerkarte Reactive sehen Sie eine Liste mit reaktiven Erkenntnissen. Auf der Registerkarte Proaktiv sehen Sie eine Liste mit proaktiven Erkenntnissen.
4. (Optional) Verwenden Sie einen oder mehrere der folgenden Filter, um die gewünschten Erkenntnisse zu finden.

- Wählen Sie je nach Art der Informationen, nach denen Sie suchen, die Registerkarte „Reaktiv“ oder „Proaktiv“.
- Wählen Sie „Einblicke filtern“ und anschließend eine Option aus, um einen Filter anzugeben. Sie können eine Kombination aus Status-, Schweregrad-, Ressourcen- und Tagfiltern hinzufügen. Verwenden Sie einen AWS Tag-Filter, um Erkenntnisse anzuzeigen, die nur von Ressourcen mit bestimmten Tags generiert wurden. Weitere Informationen hierzu finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.

> **Note**
>
> DevOpsGuru kann die folgenden Ressourcen analysieren, ihre Erkenntnisse jedoch nicht anhand von Tags filtern.
>
> - Amazon API Gateway Gateway-Pfade und -Routen
> - Amazon DynamoDB Streams
> - Amazon EC2 Auto Scaling Scaling-Gruppeninstanzen
> - AWS Elastic Beanstalk Umgebungen
> - Amazon Redshift Redshift-Knoten

- Wählen Sie einen Zeitraum aus, um nach der Zeit der Erstellung von Erkenntnissen zu filtern, oder geben Sie einen Zeitraum an.
  - 12h zeigt Erkenntnisse, die in den letzten 12 Stunden erstellt wurden.
  - 1d zeigt Erkenntnisse, die am vergangenen Tag erstellt wurden.
  - 1w zeigt Erkenntnisse, die in der letzten Woche erstellt wurden.
  - 1m zeigt Erkenntnisse, die im letzten Monat erstellt wurden.
  - Mit Benutzerdefiniert können Sie einen anderen Zeitraum angeben. Der maximale Zeitraum, den Sie zum Filtern von Erkenntnissen verwenden können, beträgt 180 Tage.

5. Um Details zu einem Einblick anzuzeigen, wählen Sie seinen Namen aus.

Einblicke in der DevOps Guru-Konsole verstehen

Verwenden Sie die Amazon DevOps Guru-Konsole, um nützliche Informationen in Ihren Insights einzusehen, die Ihnen helfen, anomales Verhalten zu diagnostizieren und zu beheben. Wenn DevOps Guru Ihre Ressourcen analysiert und verwandte CloudWatch Amazon-Metriken, AWS CloudTrail Ereignisse und Betriebsdaten findet, die auf ungewöhnliches Verhalten hinweisen, erstellt es einen Einblick, der Empfehlungen zur Behebung des Problems sowie Informationen zu den zugehörigen Kennzahlen und Ereignissen enthält. Verwenden Sie Insight-Daten mitBewährte Methoden in DevOps Guru, um von DevOps Guru festgestellte betriebliche Probleme zu beheben.

Um sich einen Einblick anzusehen, folgen Sie den Schritten unter, Einblicke ansehen um einen zu finden, und wählen Sie dann seinen Namen aus. Die Insight-Seite enthält die folgenden Details.

Überblick über Einblicke

Verwenden Sie diesen Abschnitt, um sich einen allgemeinen Überblick über die Erkenntnisse zu verschaffen. Sie können den Status des Insights (In Bearbeitung oder Abgeschlossen), die Anzahl der betroffenen CloudFormation Stapel, wann der Insight gestartet, beendet und zuletzt aktualisiert wurde, sowie den zugehörigen Vorgang, falls vorhanden, einsehen.

Wenn ein Insight auf Stack-Ebene gruppiert ist, können Sie die Anzahl der betroffenen Stacks auswählen, um deren Namen zu sehen. Das ungewöhnliche Verhalten, das zu diesem Einblick geführt hat, trat bei Ressourcen auf, die von den betroffenen Stacks erzeugt wurden. Wenn ein Insight auf Kontoebene gruppiert ist, ist die Zahl Null oder wird nicht angezeigt.

Weitere Informationen finden Sie unter Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden.

Insight-Name

Der Name eines Insights hängt davon ab, ob er auf Stack- oder Kontoebene gruppiert ist.

- Zu den Insights auf Stack-Ebene gehört der Name des Stacks, der die Ressource mit ihrem anomalen Verhalten enthält.
- Insight-Namen auf Kontoebene enthalten keinen Stack-Namen.

Weitere Informationen finden Sie unter Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden.

Aggregierte Metriken

Wählen Sie den Tab Aggregierte Metriken, um Metriken anzuzeigen, die sich auf die Erkenntnisse beziehen. In der Tabelle steht jede Zeile für eine Metrik. Sie können sehen, welcher CloudFormation Stack die Ressource erstellt hat, die die Metrik ausgegeben hat, den Namen der Ressource und ihren Typ. Nicht alle Metriken sind einem CloudFormation Stack zugeordnet oder haben einen Namen.

Wenn mehrere Ressourcen gleichzeitig anomal sind, aggregiert die Zeitleistenansicht die Ressourcen und präsentiert ihre anomalen Metriken zur einfachen Analyse in einer einzigen Zeitleiste. Die roten Linien auf einer Zeitleiste geben Zeiträume an, in denen eine Metrik ungewöhnliche Werte ausgab. Um die Ansicht zu vergrößern, wählen Sie mit der Maus einen bestimmten Zeitraum aus. Sie können auch die Lupensymbole verwenden, um die Ansicht zu vergrößern und zu verkleinern.

Wählen Sie eine rote Linie in der Timeline, um detaillierte Informationen anzuzeigen. In dem sich öffnenden Fenster können Sie:

- Wählen Sie Anzeigen in CloudWatch, um zu sehen, wie die Metrik in der CloudWatch Konsole aussieht. Weitere Informationen finden Sie unter Statistiken und Dimensionen im CloudWatch Amazon-Benutzerhandbuch.
- Bewegen Sie den Mauszeiger über das Diagramm, um Details zu den anomalen Metrikdaten und zu dem Zeitpunkt, zu dem sie aufgetreten sind, anzuzeigen.
- Wählen Sie das Feld mit dem Abwärtspfeil aus, um ein PNG-Bild des Diagramms herunterzuladen.

Anomalien grafisch dargestellt

Wählen Sie die Registerkarte Graphische Anomalien, um detaillierte Grafiken für jede der Anomalien des Insights anzuzeigen. Für jede Anomalie wird eine Kachel mit Details zu ungewöhnlichem Verhalten angezeigt, das in verwandten Metriken festgestellt wurde. Sie können eine Anomalie auf Ressourcenebene und pro Statistik untersuchen und betrachten. Die Grafiken sind nach dem Namen der Metrik gruppiert. In jeder Kachel können Sie in der Zeitleiste einen bestimmten Zeitraum zum Zoomen auswählen. Sie können auch die Lupensymbole verwenden, um die Ansicht zu vergrößern und zu verkleinern, oder Sie können eine vordefinierte Dauer in Stunden, Tagen oder Wochen wählen (1H, 3H, 12H, 1D, 3D, 1W oder 2W).

Wählen Sie Alle Statistiken und Dimensionen anzeigen, um Details zur Anomalie anzuzeigen. In dem sich öffnenden Fenster können Sie:

- Wählen Sie Anzeigen in CloudWatch, um zu sehen, wie die Metrik in der CloudWatch Konsole aussieht.
- Zeigen Sie mit der Maus auf das Diagramm, um Details zu den anomalen Metrikdaten und zu dem Zeitpunkt, zu dem sie aufgetreten sind, anzuzeigen.
- Wählen Sie Statistik oder Dimension, um die Anzeige des Diagramms anzupassen. Weitere Informationen finden Sie unter Statistiken und Dimensionen im CloudWatch Amazon-Benutzerhandbuch.

Protokollgruppen

Wenn Sie die Erkennung von Protokollanomalien aktivieren, DevOps markiert Guru Ihre CloudWatch Protokollgruppen, sodass Sie Protokollgruppen im Zusammenhang mit Ihren Erkenntnissen einsehen können. Im Abschnitt Protokollgruppen auf der Seite mit den Insight-Details steht jede Zeile in der Tabelle für eine Protokollgruppe und listet die zugehörige Ressource auf.

Wenn mehrere anomale Protokollgruppen gleichzeitig vorhanden sind, werden sie in der Zeitleistenansicht zusammengefasst und zur einfachen Analyse in einer einzigen Zeitleiste dargestellt. Die violetten Linien auf einer Zeitleiste geben Zeiträume an, in denen bei einer Protokollgruppe Protokollanomalien aufgetreten sind.

Wählen Sie eine violette Linie in der Zeitleiste, um eine Stichprobe von Informationen zu Protokollanomalien wie Stichwort-Ausnahmen und numerische Abweichungen anzuzeigen. Wählen Sie Log-Gruppendetails anzeigen, um Log-Anomalien anzuzeigen. In dem sich öffnenden Fenster können Sie:

- Ein Diagramm mit Protokollanomalien und relevanten Ereignissen anzeigen.
- Zeigen Sie mit der Maus auf das Diagramm, um Details zu den anomalen Protokolldaten und zu dem Zeitpunkt, zu dem sie aufgetreten sind, anzuzeigen.
- Lassen Sie sich die Protokollanomalien detailliert mit Beispielmeldungen, der Häufigkeit des Auftretens, den entsprechenden Empfehlungen und dem Zeitpunkt des Auftretens anzeigen.
- Klicken Sie auf Details anzeigen in CloudWatch, um die Protokollzeilen einer Protokollanomalie anzuzeigen.

Zugehörige Ereignisse

Sehen Sie sich unter Verwandte Ereignisse die AWS CloudTrail Ereignisse an, die sich auf Ihre Erkenntnisse beziehen. Verwenden Sie diese Ereignisse, um die Ursache des anomalen Verhaltens besser zu verstehen, zu diagnostizieren und zu beheben.

Empfehlungen

Unter Empfehlungen finden Sie Vorschläge, die Ihnen bei der Lösung des zugrundeliegenden Problems helfen könnten. Wenn DevOps Guru ungewöhnliches Verhalten feststellt, versucht er, Empfehlungen zu erstellen. Ein Einblick kann eine, mehrere oder keine Empfehlungen enthalten.

Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden

Ein Einblick wird auf Stack- oder Kontoebene gruppiert. Wenn ein Einblick für eine Ressource generiert wird, die sich in einem AWS CloudFormation Stack befindet, handelt es sich um einen Einblick auf Stack-Ebene. Andernfalls handelt es sich um einen Einblick auf Kontoebene.

Wie ein Stack gruppiert wird, kann davon abhängen, wie Sie Ihre Ressourcenanalyseabdeckung in Amazon DevOps Guru konfiguriert haben.

Wenn Ihre Abdeckung durch CloudFormation Stapel definiert ist

Alle Ressourcen, die in den von Ihnen ausgewählten Stacks enthalten sind, werden analysiert, und alle erkannten Erkenntnisse werden auf Stack-Ebene gruppiert.

Wenn es sich bei Ihrem Versicherungsschutz um Ihr AWS Girokonto und Ihre Region handelt

Alle Ressourcen in Ihrem Konto und Ihrer Region werden analysiert, und es gibt drei mögliche Gruppierungsszenarien für erkannte Erkenntnisse.

- Ein aus einer Ressource generierter Einblick, der nicht Teil eines Stacks ist, wird auf Kontoebene gruppiert.
- Ein aus einer Ressource generierter Einblick, der sich in einem der ersten 10.000 analysierten Stacks befindet, wird auf Stack-Ebene gruppiert.
- Ein aus einer Ressource generierter Einblick, der sich nicht in einem der ersten 10.000 analysierten Stacks befindet, wird auf Kontoebene gruppiert. Beispielsweise werden Erkenntnisse, die für eine Ressource im 10.001. analysierten Stapel generiert wurden, auf Kontoebene gruppiert.

Weitere Informationen finden Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru.

Den Schweregrad von Erkenntnissen verstehen

Ein Einblick kann einen von drei Schweregraden haben: hoch, mittel oder niedrig. Ein Insight wird von Amazon DevOps Guru erstellt, nachdem es verwandte Anomalien erkannt und jeder Anomalie einen Schweregrad zugewiesen hat. DevOpsGuru weist einer Anomalie anhand von Fachwissen und jahrelanger kollektiver Erfahrung einen Schweregrad von hoch, mittel oder niedrig zu. Der Schweregrad einer Erkenntnis wird durch die schwerwiegendste Anomalie bestimmt, die zur Entstehung der Erkenntnisse beigetragen hat.

- Wenn der Schweregrad aller Anomalien, die zu den Erkenntnissen geführt haben, gering ist, dann ist auch der Schweregrad der Erkenntnisse gering.
- Wenn der höchste Schweregrad aller Anomalien, die zu den Erkenntnissen geführt haben, mittel ist, dann ist der Schweregrad der Erkenntnisse mittel. Der Schweregrad einiger Anomalien, die zu den Erkenntnissen geführt haben, könnte gering sein.
- Wenn der Schweregrad aller Anomalien, die zu den Erkenntnissen geführt haben, hoch ist, dann ist der Schweregrad der Erkenntnisse hoch. Der Schweregrad einiger Anomalien, die zu den Erkenntnissen geführt haben, kann gering oder mittel sein.

Datenbanken mit DevOps Guru überwachen

DevOpsGuru bietet einen erheblichen Mehrwert für den Betrieb von Datenbanken. AWS Durch die Nutzung seiner Algorithmen für maschinelles Lernen kann DevOps Guru dazu beitragen, die Datenbankleistung zu optimieren, die Zuverlässigkeit zu verbessern und den Betriebsaufwand zu reduzieren. Dieser Abschnitt des Benutzerhandbuchs bietet einen allgemeinen Überblick über diese Datenbankfunktionen, einschließlich spezifischer DevOps Guru-Anwendungsfälle für verschiedene AWS Datenbankdienste.

DevOpsGuru kann Einblicke für relationale Datenbanken wie Amazon RDS und Amazon Redshift geben. Es kann auch Einblicke in nicht-relationale oder NoSQL-Datenbanken wie und liefern. Amazon DynamoDB Amazon ElastiCache

Themen

- Überwachung relationaler Datenbanken mit Guru DevOps
- Überwachung nicht-relationaler Datenbanken mit Guru DevOps

Überwachung relationaler Datenbanken mit Guru DevOps

DevOpsGuru nutzt zwei primäre Datenquellen, um nach Erkenntnissen und Anomalien in relationalen Datenbanken zu suchen. Für Amazon RDS und Amazon Redshift werden CloudWatch Verkaufsmetriken für alle Instance-Typen analysiert. Für Amazon RDS werden Performance Insights Insights-Daten auch für die folgenden Engine-Typen erfasst: RDS for PostgreSQL, Aurora PostgreSQL und Aurora MySQL.

Überwachung von Datenbankoperationen in Amazon RDS

Dieser Abschnitt enthält spezifische Informationen zu Anwendungsfällen und Metriken, die in DevOps Guru for RDS überwacht werden, einschließlich Daten aus verkauften CloudWatch Metriken und Performance Insights. Weitere Informationen zu DevOps Guru for RDS, einschließlich der wichtigsten Konzepte, Konfigurationen und Vorteile, finden Sie unterthe section called “Arbeiten mit Anomalien in Guru für RDS DevOps”.

Überwachung von RDS mithilfe von Daten aus CloudWatch veräußerten Metriken

DevOpsGuru ist in der Lage, jede Art von RDS-Instance zu überwachen, indem CloudWatch Standardmetriken wie CPU-Auslastung und Latenz bei Lese- und Schreibvorgängen erfasst werden.

Da diese Metriken standardmäßig verkauft werden, ist bei der Überwachung Ihrer RDS-Instances mit DevOps Guru keine weitere Konfiguration erforderlich, um Erkenntnisse zu gewinnen. DevOpsGuru erstellt auf der Grundlage historischer Muster automatisch eine Ausgangsbasis für diese Metriken und vergleicht sie mit Echtzeitdaten, um Anomalien und potenzielle Probleme in Ihrer Datenbank zu erkennen.

Die folgende Tabelle zeigt eine Liste potenzieller reaktiver Erkenntnisse für Amazon RDS aus verkauften CloudWatch Metriken.

AWS Von Guru überwachte DevOps Ressource	Szenario, das DevOps Guru identifiziert	CloudWatch überwachte Metriken
Amazon RDS (alle Instance-Typen)	CPU oder Arbeitsspeicher stoßen an ihre Grenzen	DBLoad, DBLoad CPU
RDS für PostgreSQL	Hohe Verzögerung beim Replikationssteckplatz	OldestReplicationSlotLag

Zusätzliche CloudWatch Verkaufsmetriken von Amazon RDS-Instances, die DevOps Guru überwacht:

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- Fehlgeschlagen SQLServer AgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Überwachung von RDS mithilfe von Daten aus Performance Insights

Für bestimmte Typen von Amazon RDS-Instances, wie Aurora PostgreSQL, Aurora MySQL und RDS for PostgreSQL, können Sie mehr Funktionen von DevOps Guru Monitoring nutzen, indem Sie sicherstellen, dass Performance Insights auf diesen Instances aktiviert ist.

DevOpsGuru bietet reaktive Einblicke für eine Vielzahl von Situationen, einschließlich der folgenden Szenarien:

Szenario, das DevOps Guru identifiziert, um reaktive Erkenntnisse zu generieren
Problem beim Sperren eines Konflikts
Fehlender Index
Fehlkonfiguration des Anwendungspools
Suboptimale JDBC-Standardeinstellungen

DevOpsGuru bietet proaktive Einblicke für eine Vielzahl von Situationen, einschließlich der folgenden Szenarien:

AWS von DevOps Guru überwachte Ressource	Szenario, das DevOps Guru identifiziert, um proaktive Einblicke zu gewinnen
Aurora MySQL	Die InnoDB-Verlaufsliste wird zu umfangrei ch, was zu Leistungseinbußen führen kann, z. B. zu einem längeren Herunterfahren der Datenbank
Aurora MySQL	Eine Zunahme von temporären Tabellen, die auf der Festplatte erstellt werden, was sich auf die Datenbankleistung auswirken kann
RDS für PostgreSQL, Aurora PostgreSQL	Eine Verbindung, deren Transaktion zu lange inaktiv war. Mögliche Auswirkungen, wenn Sperren bestehen bleiben, andere Abfragen blockiert werden und verhindert wird, dass Vacuum (einschließlich Autovacuum) tote Zeilen entfernt

Überwachung von Datenbankvorgängen in Amazon Redshift

DevOpsGuru ist in der Lage, Ihre Amazon Redshift Ressourcen zu überwachen, indem es CloudWatch Standardmetriken wie die CPU-Auslastung und den Prozentsatz des verwendeten Festplattenspeichers erfasst. Da diese Messwerte standardmäßig bereitgestellt werden, ist keine weitere Konfiguration erforderlich, damit DevOps Guru Ihre Amazon Redshift Ressourcen automatisch überwacht. DevOpsGuru erstellt auf der Grundlage historischer Muster eine Ausgangsbasis für diese Metriken und vergleicht sie mit Echtzeitdaten, um Anomalien zu erkennen.

Szenario, das Guru identifiziert DevOps	CloudWatch überwachte Metriken
Erkennen Sie eine hohe CPU-Auslastung einer Amazon Redshift Instanz, die auf Faktoren wie Cluster-Workload, verzerrte und unsortier te Daten oder Aufgaben von Leader-Nodes zurückzuführen ist	CPUUtilization
Ermitteln Sie, wenn einer Amazon Redshift Instanz aufgrund von Problemen mit der Abfrageverarbeitung, der Verteilung und Sortierung von Schlüsseln, Wartungsvorgängen oder Tombstone-Blöcken der Speicherplatz ausgeht	PercentageDiskSpaceUsed

Zusätzliche CloudWatch Verkaufsmetriken von Amazon Redshift Instances, die DevOps Guru überwacht:

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS

- ReadLatency
- WLMQueueLänge
- WLMQueueWaitTime
- WLMQueryDauer
- WriteLatency

Arbeiten mit Anomalien in DevOps Guru for RDS

DevOpsGuru erkennt, analysiert und gibt Empfehlungen für unterstützte AWS Ressourcen, einschließlich Amazon RDS-Engines. Für Amazon Aurora- und RDS for PostgreSQL-Datenbank-Instances mit aktivierter Performance Insights bietet DevOps Guru for RDS detaillierte, datenbankspezifische Analysen von Leistungsproblemen und empfiehlt Abhilfemaßnahmen.

Themen

- Überblick über Guru for RDS DevOps
- DevOpsGuru für RDS aktivieren
- Analyse von Anomalien in Amazon RDS

Überblick über Guru for RDS DevOps

Im Folgenden finden Sie eine Zusammenfassung der wichtigsten Vorteile und Funktionen von DevOps Guru for RDS. Hintergrundinformationen zu Erkenntnissen und Anomalien finden Sie unter. DevOpsGuru-Konzepte

Themen

- Vorteile von DevOps Guru for RDS
- Wichtige Konzepte für die Optimierung der Datenbankleistung
- Die wichtigsten Konzepte für DevOps Guru for RDS
- So DevOps funktioniert Guru for RDS
- Unterstützte Datenbank-Engines

Vorteile von DevOps Guru for RDS

Wenn Sie für eine Amazon RDS-Datenbank verantwortlich sind, wissen Sie möglicherweise nicht, dass ein Ereignis oder eine Regression stattfindet, das sich auf diese Datenbank auswirkt. Wenn Sie

von dem Problem erfahren, wissen Sie möglicherweise nicht, warum es auftritt und was Sie dagegen tun können. Anstatt sich an einen Datenbankadministrator (DBA) zu wenden, um Hilfe zu erhalten oder sich auf Tools von Drittanbietern zu verlassen, können Sie den Empfehlungen von DevOps Guru for RDS folgen.

Die detaillierte Analyse von DevOps Guru for RDS bietet Ihnen die folgenden Vorteile:

Schnelle Diagnose

DevOpsGuru for RDS überwacht und analysiert kontinuierlich die Datenbanktelemetrie. Performance Insights, Enhanced Monitoring und Amazon CloudWatch sammeln Telemetriedaten für Ihre Datenbank-Instances. DevOpsGuru for RDS verwendet statistische und maschinelle Lerntechniken, um diese Daten zu analysieren und Anomalien zu erkennen. Weitere Informationen zu Telemetriedaten für Amazon Aurora-Datenbanken finden Sie unter Überwachen der DB-Auslastung mit Performance Insights auf Amazon Aurora und Überwachen des Betriebssystems mithilfe von Enhanced Monitoring im Amazon Aurora-Benutzerhandbuch. Weitere Informationen zu Telemetriedaten für andere Amazon RDS-Datenbanken finden Sie unter Überwachen der DB-Auslastung mit Performance Insights on Amazon Relational Database Service und Überwachen von Betriebssystem-Metriken mit Enhanced Monitoring im Amazon RDS-Benutzerhandbuch.

Schnelle Auflösung

Jede Anomalie identifiziert das Leistungsproblem und schlägt Möglichkeiten für Untersuchungen oder Korrekturmaßnahmen vor. DevOpsGuru for RDS könnte Ihnen beispielsweise empfehlen, bestimmte Warteereignisse zu untersuchen. Oder es empfiehlt sich, Ihre Anwendungspooleinstellungen zu optimieren, um die Anzahl der Datenbankverbindungen zu begrenzen. Basierend auf diesen Empfehlungen können Sie Leistungsprobleme schneller beheben als durch eine manuelle Fehlerbehebung.

Proaktive Einblicke

DevOpsGuru for RDS verwendet Metriken aus Ihren Ressourcen, um potenziell problematisches Verhalten zu erkennen, bevor es zu einem größeren Problem wird. Es kann beispielsweise erkennen, wenn Sitzungen, die mit der Datenbank verbunden sind, keine aktive Arbeit verrichten und möglicherweise Datenbankressourcen blockieren. DevOps Guru gibt dann Empfehlungen, mit denen Sie Probleme lösen können, bevor sie zu größeren Problemen werden.

Fundierte Kenntnisse der Amazon-Ingenieure und Machine Learning

Um Leistungsprobleme zu erkennen und Ihnen bei der Behebung von Engpässen zu helfen, setzt DevOps Guru for RDS auf maschinelles Lernen (ML) und fortschrittliche statistische Analysen.

Die Datenbankingenieure von Amazon haben an der Entwicklung von DevOps Guru for RDS mitgewirkt, die das Ergebnis vieler Jahre der Verwaltung von Hunderttausenden von Datenbanken sind. Auf der Grundlage dieses kollektiven Wissens kann DevOps Guru for RDS Ihnen bewährte Methoden vermitteln.

Wichtige Konzepte für die Optimierung der Datenbankleistung

DevOpsGuru for RDS geht davon aus, dass Sie mit einigen wichtigen Leistungskonzepten vertraut sind. Weitere Informationen zu diesen Konzepten finden Sie unter Überblick über Performance Insights im Amazon Aurora-Benutzerhandbuch oder unter Überblick über Performance Insights im Amazon RDS-Benutzerhandbuch.

Themen

- Metriken
- Erkennung von Problemen
- DB-Auslastung
- Warteereignisse

Metriken

Eine Metrik stellt einen chronologisch sortierten Satz von Datenpunkten dar. Sie können sich eine Metrik als eine zu überwachende Variable und die Datenpunkte als die Werte dieser Variablen im Laufe der Zeit vorstellen. Amazon RDS stellt in Echtzeit Metriken für die Datenbank und für das Betriebssystem (OS) bereit, auf dem Ihre DB-Instance läuft. Sie können alle Systemmetriken und Prozessinformationen für Ihre Amazon RDS-DB-Instances auf der Amazon RDS-Konsole einsehen. DevOps Guru for RDS überwacht und liefert Einblicke in einige dieser Metriken. Weitere Informationen finden Sie unter Überwachen von Metriken in einem Amazon Aurora-Cluster oder Überwachen von Metriken in einer Amazon Relational Database Service-Instance.

Erkennung von Problemen

DevOpsGuru for RDS verwendet Datenbank- und Betriebssystem-Metriken, um kritische Datenbankleistungsprobleme zu erkennen, unabhängig davon, ob diese Probleme unmittelbar bevorstehen oder andauern. DevOpsGuru for RDS-Problemerkennung funktioniert hauptsächlich auf zwei Arten:

- Mithilfe von Schwellenwerten

- Verwendung von Anomalien

Erkennung von Problemen mit Schwellenwerten

Schwellenwerte sind die Grenzwerte, anhand derer die überwachten Metriken bewertet werden. Sie können sich einen Schwellenwert als eine horizontale Linie in einem Metrikdiagramm vorstellen, die normales Verhalten von potenziell problematischem Verhalten trennt. DevOps Guru for RDS überwacht bestimmte Metriken und erstellt Schwellenwerte, indem analysiert wird, welche Stufen für eine bestimmte Ressource als potenziell problematisch angesehen werden. DevOpsGuru for RDS erstellt dann in der DevOps Guru-Konsole auf konsistenter Basis Einblicke, wenn neue Metrikwerte über einen bestimmten Zeitraum einen bestimmten Schwellenwert überschreiten. Die Erkenntnisse enthalten Empfehlungen, um zukünftige Auswirkungen auf die Datenbankleistung zu verhindern.

DevOpsGuru for RDS könnte beispielsweise die Anzahl der temporären Tabellen, die die Festplatte nutzen, über einen Zeitraum von 15 Minuten überwachen und daraus Erkenntnisse gewinnen, wenn die Rate temporärer Tabellen, die Festplatte pro Sekunde nutzen, ungewöhnlich hoch ist. Eine erhöhte Nutzung temporärer Tabellen auf der Festplatte kann sich auf die Datenbankleistung auswirken. DevOpsGuru for RDS deckt diese Situation auf, bevor sie kritisch wird, und hilft Ihnen, Korrekturmaßnahmen zu ergreifen, um Probleme zu vermeiden.

Erkennung von Problemen mit Anomalien

Schwellenwerte bieten zwar eine einfache und effektive Möglichkeit, Datenbankprobleme zu erkennen, in manchen Situationen reichen sie jedoch nicht aus. Stellen Sie sich einen Fall vor, in dem die Metrikwerte aufgrund eines bekannten Prozesses, z. B. einer täglichen Berichtsarbeit, regelmäßig in potenziell problematisches Verhalten übergehen. Da solche Spitzen zu erwarten sind, wäre es kontraproduktiv, für jeden einzelnen von ihnen Erkenntnisse und Benachrichtigungen zu erstellen, was wahrscheinlich zu einer Übermüdung der Alarmmeldungen führen würde.

Es ist jedoch immer noch notwendig, äußerst ungewöhnliche Spitzen zu erkennen, da Metriken, die viel höher sind als die anderen oder viel länger andauern, echte Probleme mit der Datenbankleistung darstellen könnten. Um dieses Problem auszuräumen, überwacht DevOps Guru for RDS bestimmte Metriken, um zu erkennen, wann das Verhalten einer Metrik äußerst ungewöhnlich oder anomal wird. DevOpsGuru berichtet dann über diese Anomalien in Form von Insights.

DevOpsGuru for RDS kann beispielsweise Erkenntnisse gewinnen, wenn die DB-Auslastung nicht nur hoch ist, sondern auch erheblich vom üblichen Verhalten abweicht, was auf eine erhebliche unerwartete Verlangsamung der Datenbankoperationen hindeutet. DevOpsGuru for RDS erkennt nur

die anomalen DB-Lastspitzen und ermöglicht es Ihnen, sich auf die wirklich wichtigen Probleme zu konzentrieren.

DB-Auslastung

Das Schlüsselkonzept für die Datenbankoptimierung ist die Metrik zur Datenbanklast (DB-Last). Die DB-Auslastung gibt an, wie stark Ihre Datenbank zu einem bestimmten Zeitpunkt ausgelastet ist. Eine Erhöhung der DB-Auslastung bedeutet eine Zunahme der Datenbankaktivität.

Eine Datenbank-Sitzung repräsentiert den Dialog einer Anwendung mit einer relationalen Datenbank. Eine aktive Sitzung ist eine Sitzung, die gerade eine Datenbankanforderung ausführt. Eine Sitzung ist aktiv, wenn sie entweder auf der CPU läuft oder darauf wartet, dass eine Ressource verfügbar wird, damit sie fortfahren kann. Beispielsweise kann eine aktive Sitzung warten, bis eine Seite in den Speicher eingelesen wird, und verbraucht dann CPU, während sie Daten von der Seite liest.

Die `DBLoad` Metrik in Performance Insights wird in durchschnittlich aktiven Sitzungen (AAS) gemessen. Um AAS zu berechnen, erfasst Performance Insights jede Sekunde die Anzahl der aktiven Sitzungen. Für einen bestimmten Zeitraum ist die AAS die Gesamtzahl der aktiven Sitzungen geteilt durch die Gesamtzahl der Stichproben. Ein AAS-Wert von 2 bedeutet, dass im Durchschnitt 2 Sitzungen zu einem bestimmten Zeitpunkt in Anfragen aktiv waren.

Eine Analogie zur DB-Last ist die Aktivität in einem Lager. Angenommen, das Lager beschäftigt 100 Mitarbeiter. Wenn eine Bestellung eingeht, erfüllt 1 Mitarbeiter die Bestellung, während die anderen Mitarbeiter im Leerlauf sind. Wenn 100 oder mehr Bestellungen eingehen, führen alle 100 Mitarbeiter Bestellungen gleichzeitig aus. Wenn Sie regelmäßig prüfen, wie viele Mitarbeiter über einen bestimmten Zeitraum aktiv sind, können Sie die durchschnittliche Anzahl aktiver Mitarbeiter berechnen. Die Berechnung zeigt, dass im Durchschnitt N Arbeitnehmer zu jedem beliebigen Zeitpunkt damit beschäftigt sind, Bestellungen zu erfüllen. Wenn der Durchschnitt gestern 50 Arbeitnehmer und heute 75 Arbeitnehmer betrug, stieg das Aktivitätsniveau im Lager. In gleicher Weise steigt die DB-Last mit zunehmender Sitzungsaktivität.

Weitere Informationen finden Sie unter Database load im Amazon Aurora User Guide oder Database load im Amazon RDS User Guide.

Warteereignisse

Ein Wait-Event ist eine Art von Datenbank-Instrumentierung, die Ihnen mitteilt, auf welche Ressource eine Datenbanksitzung wartet, damit sie fortgesetzt werden kann. Wenn Performance Insights aktive Sitzungen zählt, um die Datenbanklast zu berechnen, zeichnet es auch die

Warteereignisse auf, die dazu führen, dass die aktiven Sitzungen warten. Mit dieser Technik kann Performance Insights Ihnen zeigen, welche Warteereignisse zur DB-Auslastung beitragen.

Jede aktive Sitzung läuft entweder auf der CPU oder wartet. Beispielsweise verbrauchen Sitzungen die CPU, wenn sie den Speicher durchsuchen, eine Berechnung durchführen oder prozeduralen Code ausführen. Wenn Sitzungen keine CPU beanspruchen, warten sie möglicherweise darauf, dass eine Datendatei gelesen oder in ein Protokoll geschrieben wird. Je mehr Zeit eine Sitzung auf Ressourcen wartet, desto weniger Zeit läuft sie auf der CPU.

Wenn Sie eine Datenbank optimieren, versuchen Sie oft, die Ressourcen zu finden, auf die Sitzungen warten. Beispielsweise können zwei oder drei Warteereignisse 90% der DB-Auslastung ausmachen. Diese Maßnahme bedeutet, dass aktive Sitzungen im Durchschnitt die meiste Zeit damit verbringen, auf eine kleine Anzahl von Ressourcen zu warten. Wenn Sie die Ursache für diese Wartezeiten herausfinden können, können Sie versuchen, das Problem zu beheben.

Betrachten Sie die Analogie eines Lagerarbeiters. Es kommt eine Bestellung für ein Buch. Der Arbeitnehmer kann sich bei der Ausführung der Bestellung verzögern. Beispielsweise ist möglicherweise gerade ein anderer Mitarbeiter dabei, die Regale wieder aufzufüllen, oder es ist möglicherweise kein Rollwagen verfügbar. Oder das System, mit dem der Bestellstatus eingegeben wurde, ist möglicherweise langsam. Je länger die Arbeitskraft wartet, desto länger dauert es, bis die Bestellung ausgeführt wird. Warten ist ein natürlicher Teil des Arbeitsablaufs im Lager, aber wenn die Wartezeiten zu lang werden, sinkt die Produktivität. Auf die gleiche Weise können wiederholte oder langwierige Sitzungswartungen die Datenbankleistung beeinträchtigen.

Weitere Informationen zu Warteereignissen in Amazon Aurora finden Sie unter Tuning with wait events for Aurora PostgreSQL und Tuning with wait events for Aurora MySQL im Amazon Aurora-Benutzerhandbuch.

Weitere Informationen zu Wait-Ereignissen in anderen Amazon RDS-Datenbanken finden Sie unter Tuning with wait events for RDS for PostgreSQL im Amazon RDS-Benutzerhandbuch.

Die wichtigsten Konzepte für DevOps Guru for RDS

DevOpsGuru generiert Erkenntnisse, wenn es anomales oder problematisches Verhalten in Ihren betrieblichen Anwendungen feststellt. Ein Einblick enthält Anomalien für eine oder mehrere Ressourcen. Eine Anomalie steht für eine oder mehrere verwandte Metriken, die von DevOps Guru entdeckt wurden und die unerwartet oder ungewöhnlich sind.

Eine Erkenntnis hat den Schweregrad „Hoch“, „Mittel“ oder „Niedrig“. Der Schweregrad der Erkenntnisse wird durch die schwerwiegendste Anomalie bestimmt, die zur Erstellung der

Erkenntnisse beigetragen hat. Wenn der Einblick AWS-ECS _ MemoryUtilization _and_others beispielsweise eine Anomalie mit niedrigem Schweregrad und eine weitere mit hohem Schweregrad enthält, ist der Schweregrad der Erkenntnis insgesamt hoch.

Wenn Performance Insights bei Amazon RDS-DB-Instances aktiviert ist, bietet DevOps Guru for RDS detaillierte Analysen und Empfehlungen zu den Anomalien für diese Instances. Um eine Anomalie zu identifizieren, entwickelt DevOps Guru for RDS eine Basislinie für Datenbank-Metrikwerte. DevOpsGuru for RDS vergleicht dann die aktuellen Metrikwerte mit den historischen Basiswerten.

Themen

- Proaktive Einblicke
- Reaktive Einblicke
- Empfehlungen

Proaktive Einblicke

Ein proaktiver Einblick informiert Sie über problematisches Verhalten, bevor es auftritt. Es enthält Anomalien mit Empfehlungen und zugehörigen Metriken, die Ihnen helfen, die Probleme zu lösen, bevor sie zu größeren Problemen werden.

Jede Seite mit proaktiven Einblicken enthält Details zu einer Anomalie.

Reaktive Einblicke

Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Sie enthält Auffälligkeiten mit Empfehlungen, zugehörigen Kennzahlen und Ereignissen, damit Sie die Probleme jetzt besser verstehen und beheben können.

Kausale Anomalien

Eine kausale Anomalie ist eine Anomalie der obersten Ebene innerhalb eines Einblicks. Sie wird auf der Seite mit den Anomaliedetails in der Guru-Konsole als primäre Metrik angezeigt. DevOps Die Datenbanklast (DB-Last) ist die ursächliche Anomalie für DevOps Guru for RDS. Zum Beispiel könnte der Insight AWS-ECS _ MemoryUtilization _and_others mehrere metrische Anomalien aufweisen, von denen eine die Datenbanklast (DB-Auslastung) für die Ressource ist. AWS/RDS

Innerhalb eines Einblicks kann die anomale Datenbanklast (DB-Last) für mehrere Amazon RDS-DB-Instances auftreten. Der Schweregrad der Anomalie kann für jede DB-Instance unterschiedlich sein.

Beispielsweise kann der Schweregrad für eine DB-Instance hoch sein, während der Schweregrad für die anderen niedrig ist. Die Konsole verwendet standardmäßig die Anomalie mit dem höchsten Schweregrad.

Kontextbezogene Anomalien

Eine kontextbezogene Anomalie ist ein Befund innerhalb der Datenbanklast (DB-Last), der zu einem reaktiven Einblick gehört. Sie wird im Abschnitt „Verwandte Metriken“ auf der Seite mit den Anomaliedetails in der DevOps Guru-Konsole angezeigt. Jede kontextuelle Anomalie beschreibt ein bestimmtes Amazon RDS-Leistungsproblem, das untersucht werden muss. Eine kausale Anomalie kann beispielsweise die folgenden kontextuellen Anomalien umfassen:

- CPU-Kapazität überschritten — Die CPU-Ausführungswarteschlange oder die CPU-Auslastung liegen über dem Normalwert.
- Zu wenig Datenbankspeicher — Prozesse haben nicht genug Speicher.
- Spitzenwerte bei den Datenbankverbindungen — Die Anzahl der Datenbankverbindungen liegt über dem Normalwert.

Empfehlungen

Für jede Erkenntnis wird mindestens eine Aktion vorgeschlagen. Die folgenden Beispiele sind Empfehlungen, die von DevOps Guru für RDS generiert wurden:

- Optimieren Sie die SQL-IDs, *`list_of_IDs`* um die CPU-Auslastung zu reduzieren, oder aktualisieren Sie den Instance-Typ, um die CPU-Kapazität zu erhöhen.
- Prüfen Sie den damit verbundenen Anstieg der aktuellen Datenbankverbindungen. Erwägen Sie, die Anwendungspooleinstellungen zu optimieren, um eine häufige dynamische Zuweisung neuer Datenbankverbindungen zu vermeiden.
- Halten Sie Ausschau nach SQL-Anweisungen, die übermäßig viele Speicheroperationen ausführen, z. B. speicherinterne Sortierungen oder umfangreiche Verknüpfungen.
- Untersuchen Sie die starke I/O Nutzung der folgenden SQL-IDs:*`list_of_IDs`*.
- Suchen Sie nach Anweisungen, die große Mengen temporärer Daten erzeugen, z. B. solche, die umfangreiche Sortierungen durchführen oder große temporäre Tabellen verwenden.
- Überprüfen Sie die Anwendungen, um festzustellen, was die erhöhte Datenbank-Arbeitslast verursacht.
- Erwägen Sie, das MySQL-Leistungsschema zu aktivieren.

- Suchen Sie nach Transaktionen mit langer Laufzeit und beenden Sie sie mit einem Commit oder Rollback.
- Konfigurieren Sie den Parameter idle_in_transaction_session_timeout so, dass jede Sitzung beendet wird, die sich länger als die angegebene Zeit im Status „Idle in transaction“ befindet.

So DevOps funktioniert Guru for RDS

DevOpsGuru for RDS sammelt Metrikdaten, analysiert sie und veröffentlicht dann Anomalien im Dashboard.

Themen

- Datenerfassung und Analyse
- Veröffentlichung im Zusammenhang mit Anomalien

Datenerfassung und Analyse

DevOpsGuru for RDS sammelt Daten über Ihre Amazon RDS-Datenbanken von Amazon RDS Performance Insights. Diese Funktion überwacht Amazon RDS-DB-Instances, sammelt Metriken und ermöglicht es Ihnen, die Metriken in einem Diagramm zu untersuchen. Die wichtigste Leistungsmetrik ist`DBLoad`. DevOpsGuru for RDS verwendet Performance Insights-Metriken und analysiert sie, um Anomalien zu erkennen. Weitere Informationen zu Performance Insights finden Sie unter Überwachen der DB-Auslastung mit Performance Insights auf Amazon Aurora im Amazon Aurora-Benutzerhandbuch oder Überwachen der DB-Auslastung mit Performance Insights auf Amazon RDS im Amazon RDS-Benutzerhandbuch.

DevOpsGuru for RDS verwendet maschinelles Lernen und erweiterte statistische Analysen, um die von Performance Insights gesammelten Daten zu analysieren. Wenn DevOps Guru for RDS Leistungsprobleme feststellt, fährt es mit dem nächsten Schritt fort.

Veröffentlichung im Zusammenhang mit Anomalien

Ein Problem mit der Datenbankleistung, wie z. B. eine hohe DB-Belastung, kann die Servicequalität Ihrer Datenbank beeinträchtigen. Wenn DevOps Guru ein Problem in einer RDS-Datenbank entdeckt, veröffentlicht es einen Einblick im Dashboard. Der Einblick enthält eine Anomalie für die Ressource AWS/RDS.

Wenn Performance Insights für Ihre Instances aktiviert ist, enthält die Anomalie eine detaillierte Analyse des Problems. DevOps Guru for RDS empfiehlt außerdem, dass Sie eine Untersuchung oder

bestimmte Korrekturmaßnahmen durchführen. Die Empfehlung könnte beispielsweise lauten, eine bestimmte SQL-Anweisung mit hoher Auslastung zu untersuchen, eine Erhöhung der CPU-Kapazität in Betracht zu ziehen oder Sitzungen zu schließen, die während einer Transaktion im Leerlauf laufen.

Unterstützte Datenbank-Engines

DevOpsGuru for RDS wird für die folgenden Datenbank-Engines unterstützt:

Amazon Aurora mit MySQL-Kompatibilität

Weitere Informationen zu dieser Engine finden Sie unter Arbeiten mit Amazon Aurora MySQL im Amazon Aurora-Benutzerhandbuch.

Amazon Aurora mit PostgreSQL-Kompatibilität

Weitere Informationen zu dieser Engine finden Sie unter Arbeiten mit Amazon Aurora PostgreSQL im Amazon Aurora-Benutzerhandbuch.

Amazon RDS für PostgreSQL-Kompatibilität

Weitere Informationen zu dieser Engine finden Sie Amazon RDS for PostgreSQL im Amazon RDS-Benutzerhandbuch.

DevOpsGuru meldet Anomalien und bietet grundlegende Analysen für andere Datenbank-Engines. DevOpsGuru for RDS bietet detaillierte Analysen und Empfehlungen nur für Amazon Aurora und RDS für PostgreSQL-Instances.

DevOpsGuru für RDS aktivieren

Wenn Sie DevOps Guru für RDS aktivieren, ermöglichen Sie DevOps Guru, Anomalien in Ressourcen wie DB-Instances zu analysieren. Amazon RDS macht es einfach, empfohlene Funktionen für eine RDS-DB-Instance oder einen DB-Cluster zu erkennen und zu aktivieren. Um dies zu erreichen, führt RDS API-Aufrufe an andere Dienste wie Amazon EC2, DevOps Guru und IAM durch. Wenn die RDS-Konsole diese API-Aufrufe tätigt, werden sie aus Gründen der AWS CloudTrail Sichtbarkeit protokolliert.

Damit DevOps Guru Erkenntnisse für eine Amazon RDS-Datenbank veröffentlichen kann, führen Sie die Aufgaben in den folgenden Abschnitten aus.

Themen

- Performance Insights für Ihre Amazon RDS-DB-Instances aktivieren

- Konfiguration der Zugriffsrichtlinien für DevOps Guru for RDS
- Hinzufügen von Amazon RDS-DB-Instances zu Ihrer DevOps Guru-Abdeckung

Performance Insights für Ihre Amazon RDS-DB-Instances aktivieren

Damit DevOps Guru for RDS Anomalien auf einer DB-Instance analysieren kann, stellen Sie sicher, dass Performance Insights aktiviert ist. Wenn Performance Insights für eine DB-Instance nicht aktiviert ist, benachrichtigt DevOps Guru for RDS Sie an den folgenden Stellen:

Dashboard

Wenn du dir Einblicke nach Ressourcentyp ansiehst, weist dich die RDS-Kachel darauf hin, dass Performance Insights nicht aktiviert ist. Wählen Sie den Link, um Performance Insights in der Amazon RDS-Konsole zu aktivieren.

Insights

Wählen Sie im Abschnitt Empfehlungen unten auf der Seite die Option Amazon RDS Performance Insights aktivieren aus.

Einstellungen

Wählen Sie im Abschnitt Service: Amazon RDS den Link aus, um Performance Insights in der Amazon RDS-Konsole zu aktivieren.

Weitere Informationen finden Sie im Amazon Aurora-Benutzerhandbuch unter Ein- und Ausschalten von Performance Insights oder im Amazon RDS-Benutzerhandbuch unter Ein- und Ausschalten von Performance Insights.

Konfiguration der Zugriffsrichtlinien für DevOps Guru for RDS

Damit ein Benutzer auf DevOps Guru for RDS zugreifen kann, muss er über Berechtigungen aus einer der folgenden Richtlinien verfügen:

- Die AWS verwaltete Richtlinie `AmazonRDSFullAccess`
- Eine vom Kunden verwaltete Richtlinie, welche die folgenden Aktionen erlaubt:
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

Weitere Informationen finden Sie unter Konfiguration der Zugriffsrichtlinien für Performance Insights im Amazon Aurora-Benutzerhandbuch oder unter Konfiguration der Zugriffsrichtlinien für Performance Insights im Amazon RDS-Benutzerhandbuch.

Hinzufügen von Amazon RDS-DB-Instances zu Ihrer DevOps Guru-Abdeckung

Sie können DevOps Guru so konfigurieren, dass Ihre Amazon RDS-Datenbanken entweder in der DevOps Guru-Konsole oder der Amazon RDS-Konsole überwacht werden.

In der DevOps Guru-Konsole haben Sie die folgenden Optionen:

- Schalte DevOps Guru auf Kontoebene ein. Das ist die Standardeinstellung. Wenn Sie diese Option wählen, analysiert DevOps Guru alle unterstützten AWS Ressourcen in Ihrem AWS-Region Land AWS-Konto, einschließlich Amazon RDS-Datenbanken.
- Geben Sie AWS CloudFormation Stacks für DevOps Guru for RDS an.

  Weitere Informationen finden Sie unter Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- Taggen Sie Ihre Amazon RDS-Ressourcen.

  Ein Tag ist eine benutzerdefinierte Attributbezeichnung, die Sie einer AWS Ressource zuweisen. Verwenden Sie Tags, um die AWS Ressourcen zu identifizieren, aus denen Ihre Anwendung besteht. Anschließend können Sie Ihre Erkenntnisse nach Tags filtern, um nur die von Ihrer Anwendung erstellten zu sehen. Um nur Erkenntnisse anzuzeigen, die von den Amazon RDS-Ressourcen in Ihrer Anwendung generiert wurden, fügen Sie Ihren Amazon RDS-Ressourcen-Tags einen Wert hinzu. `Devops-guru-rds` Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.

  > **Note**
  >
  > Wenn Sie Amazon RDS-Ressourcen taggen, müssen Sie die Datenbank-Instance und nicht den Cluster taggen.

Informationen zum Aktivieren der DevOps Guru-Überwachung von der Amazon RDS-Konsole aus finden Sie unter DevOps Guru in der RDS-Konsole einschalten. Beachten Sie, dass Sie Tags verwenden müssen, um DevOps Guru von der Amazon RDS-Konsole aus zu aktivieren. Weitere Informationen zu Tags erhalten Sie unter the section called “Verwenden Sie Tags, um Ressourcen in Ihren Anwendungen zu identifizieren”.

Analyse von Anomalien in Amazon RDS

Wenn DevOps Guru for RDS eine Leistungsanomalie im Dashboard veröffentlicht, führen Sie normalerweise die folgenden Schritte aus:

1. Sehen Sie sich den Einblick im DevOps Guru-Dashboard an. DevOpsGuru for RDS berichtet sowohl über reaktive als auch über proaktive Erkenntnisse.

   Weitere Informationen finden Sie unter Einblicke anzeigen.
2. Sehen Sie sich Anomalien für AWS/RDS Ressourcen an.

   Weitere Informationen erhalten Sie unter Anzeige reaktiver Anomalien und Anzeige proaktiver Anomalien.
3. Fragen Sie DevOps Guru nach RDS-Empfehlungen.

   Weitere Informationen finden Sie unter Reagieren auf -Empfehlungen.
4. Überwachen Sie den Zustand Ihrer DB-Instances, um sicherzustellen, dass gelöste Leistungsprobleme nicht erneut auftreten.

   Weitere Informationen finden Sie unter Überwachung von Metriken in einem Amazon Aurora-DB-Cluster im Amazon Aurora-Benutzerhandbuch und unter Überwachung von Metriken in einer Amazon RDS-Instance im Amazon RDS-Benutzerhandbuch.

Einblicke anzeigen

Rufen Sie die Insights-Seite in der DevOps Guru-Konsole auf, um reaktive und proaktive Einblicke zu erhalten. Von dort aus können Sie einen Einblick aus der Liste auswählen, um eine detaillierte Seite mit Kennzahlen, Empfehlungen und weiteren Informationen zu dem Einblick aufzurufen.

Um einen Einblick anzusehen

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und wählen Sie dann Insights aus.
3. Wählen Sie den Tab Reaktiv, um reaktive Erkenntnisse anzuzeigen, oder wählen Sie Proaktiv, um proaktive Erkenntnisse anzuzeigen.
4. Wählen Sie den Namen eines Insights und priorisieren Sie ihn nach Status und Schweregrad.

Die Seite mit den detaillierten Einblicken wird angezeigt.

Anzeige reaktiver Anomalien

Im Rahmen eines Einblicks können Sie Anomalien für Amazon RDS-Ressourcen einsehen. Auf einer Seite mit reaktiven Erkenntnissen können Sie im Abschnitt Aggregierte Metriken eine Liste der Anomalien mit den entsprechenden Zeitplänen einsehen. Es gibt auch Abschnitte, in denen Informationen zu Protokollgruppen und Ereignissen im Zusammenhang mit den Anomalien angezeigt werden. Kausale Anomalien in einem reaktiven Einblick haben jeweils eine entsprechende Seite mit Details zur Anomalie.

Anzeige der detaillierten Analyse einer reaktiven RDS-Anomalie

In dieser Phase gehen Sie näher auf die Anomalie ein, um detaillierte Analysen und Empfehlungen für Ihre Amazon RDS-DB-Instances zu erhalten.

Die detaillierte Analyse ist nur für Amazon RDS-DB-Instances verfügbar, bei denen Performance Insights aktiviert ist.

Um einen Drilldown zur Seite mit den Anomaliedetails durchzuführen

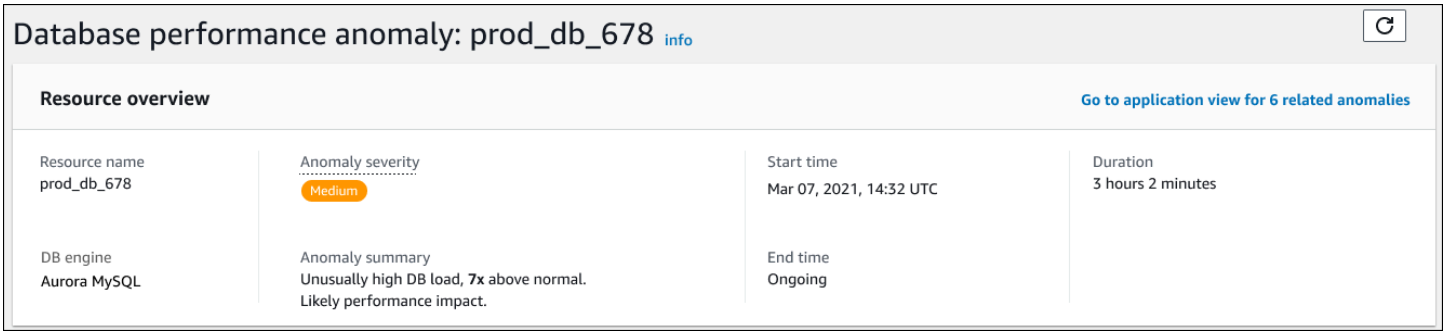
1. Suchen Sie auf der Insight-Seite nach einer aggregierten Metrik mit dem Ressourcentyp AWS/RDS.
2. Wählen Sie die Option Details anzeigen aus.

   Die Seite mit den Details zur Anomalie wird angezeigt. Der Titel beginnt mit „Datenbank-Performance-Anomalie“ und benennt die angezeigte Ressource. Die Konsole verwendet standardmäßig die Anomalie mit dem höchsten Schweregrad, unabhängig davon, wann die Anomalie aufgetreten ist.
3. (Optional) Wenn mehrere Ressourcen betroffen sind, wählen Sie eine andere Ressource aus der Liste oben auf der Seite aus.

Im Folgenden finden Sie Beschreibungen für die Komponenten der Detailseite.

Übersicht über Ressourcen

Im oberen Bereich der Detailseite befindet sich die Ressourcenübersicht. In diesem Abschnitt wird die Leistungsanomalie zusammengefasst, die bei Ihrer Amazon RDS-DB-Instance aufgetreten ist.

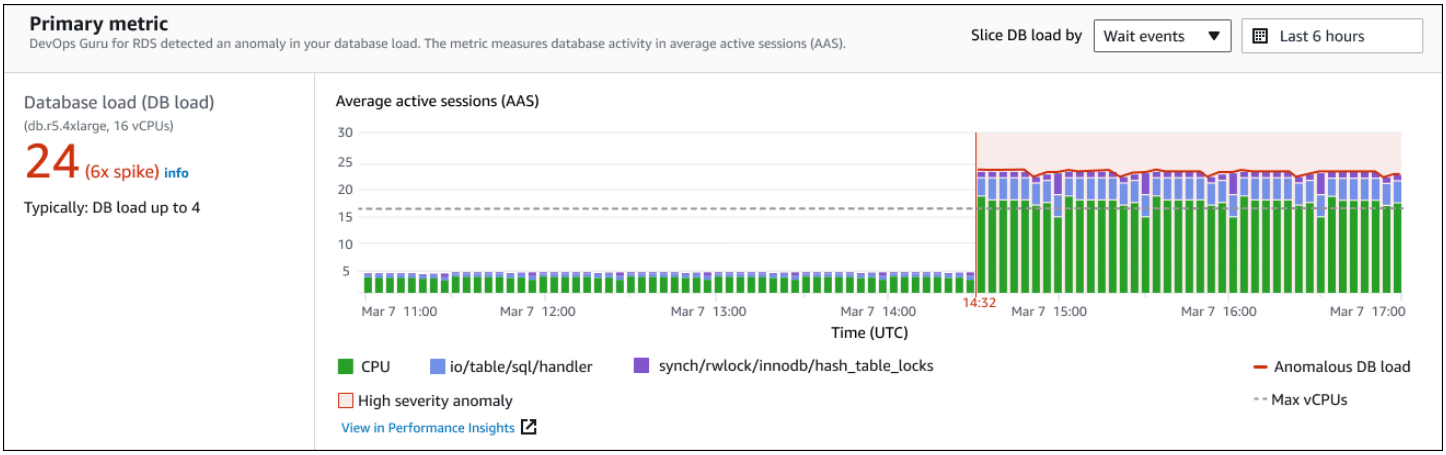


Dieser Abschnitt enthält die folgenden Felder:

- Ressourcenname — Der Name der DB-Instance, bei der die Anomalie auftritt. In diesem Beispiel heißt die Ressource prod_db_678.
- DB-Engine — Der Name der DB-Instance, bei der die Anomalie auftritt. In diesem Beispiel ist die Engine Aurora MySQL.
- Schweregrad der Anomalie — Das Maß für die negativen Auswirkungen der Anomalie auf Ihre Instance. Mögliche Schweregrade sind „Hoch“, „Mittel“ und „Niedrig“.
- Zusammenfassung der Anomalie — Eine kurze Zusammenfassung des Problems. Eine typische Zusammenfassung lautet Ungewöhnlich hohe DB-Auslastung.
- Startzeit und Endzeit — Die Uhrzeit, zu der die Anomalie begann und endete. Wenn die Endzeit fortlaufend ist, tritt die Anomalie immer noch auf.
- Dauer — Die Dauer des anomalen Verhaltens. In diesem Beispiel dauert die Anomalie an und besteht seit 3 Stunden und 2 Minuten.

Primäre Metrik

Im Abschnitt Primäre Metrik wird die zufällige Anomalie zusammengefasst, bei der es sich um die höchste Anomalie innerhalb der Erkenntnisse handelt. Sie können sich die kausale Anomalie als das allgemeine Problem vorstellen, mit dem Ihre DB-Instance konfrontiert ist.



Im linken Bereich finden Sie weitere Informationen zu dem Problem. In diesem Beispiel enthält die Zusammenfassung die folgenden Informationen:

- Datenbanklast (DB-Load) — Eine Kategorisierung der Anomalie als Problem beim Laden der Datenbank. Die entsprechende Metrik in Performance Insights lautet. `DBLoad` Diese Metrik wird auch bei Amazon veröffentlicht CloudWatch.
- db.r5.4xlarge — Die DB-Instance-Klasse. Die Anzahl der vCPUs, in diesem Beispiel 16, entspricht der gepunkteten Linie im Diagramm „Durchschnittliche aktive Sitzungen“ (AAS).
- 24 (6-fache Spitze) — Die DB-Auslastung, gemessen in durchschnittlich aktiven Sitzungen (AAS) während des im Insight angegebenen Zeitintervalls. Somit waren zu jedem beliebigen Zeitpunkt während des Zeitraums der Anomalie durchschnittlich 24 Sitzungen in der Datenbank aktiv. Die DB-Last beträgt das Sechsfache der normalen DB-Last für diese Instance.
- Normalerweise: DB-Last bis zu 4 — Der Basiswert der DB-Auslastung, gemessen in AAS, während einer typischen Arbeitslast. Der Wert 4 bedeutet, dass bei normalem Betrieb zu einem bestimmten Zeitpunkt durchschnittlich 4 oder weniger Sitzungen in der Datenbank aktiv sind.

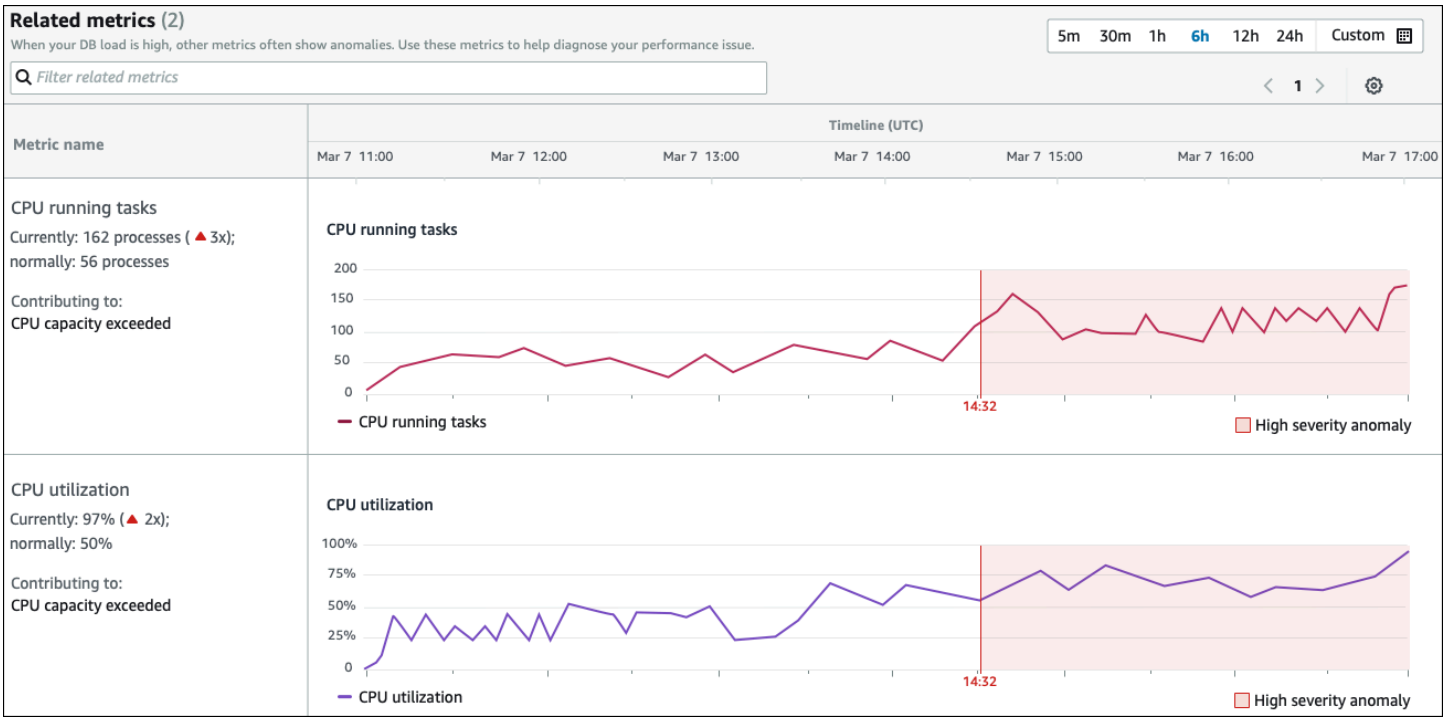
Standardmäßig ist das Lastdiagramm nach Warteereignissen unterteilt. Das bedeutet, dass für jeden Balken im Diagramm der größte farbige Bereich das Warte-Ereignis darstellt, das am meisten zur gesamten DB-Auslastung beiträgt. Das Diagramm zeigt den Zeitpunkt (in rot), zu dem das Problem auftrat. Konzentrieren Sie sich auf die Warteereignisse, die den meisten Platz in der Leiste einnehmen:

- `CPU`
- `IO:wait/io/sql/table/handler`

Die vorangegangenen Warteereignisse erscheinen für diese Aurora MySQL-Datenbank häufiger als normal. Informationen zur Leistungsoptimierung mithilfe von Warteereignissen in Amazon Aurora finden Sie unter Tuning with wait events for Aurora MySQL und Tuning with wait events for Aurora PostgreSQL im Amazon Aurora-Benutzerhandbuch. Informationen zum Optimieren der Leistung mithilfe von Warteereignissen in RDS for PostgreSQL finden Sie im Amazon RDS-Benutzerhandbuch unter Tuning with wait events for RDS for PostgreSQL.

Verwandte Metriken

Im Abschnitt „Verwandte Metriken“ sind die kontextuellen Anomalien aufgeführt, bei denen es sich um spezifische Ergebnisse innerhalb der kausalen Anomalie handelt. Diese Ergebnisse enthalten zusätzliche Informationen zu den Leistungsproblemen.



Die Tabelle „Verwandte Metriken“ hat zwei Spalten: „Name der Metrik“ und „Zeitplan“ (UTC). Jede Zeile in der Tabelle entspricht einer bestimmten Metrik.

Die erste Spalte jeder Zeile enthält die folgenden Informationen:

- ***Name***— Der Name der Metrik. Die erste Zeile identifiziert die Metrik als CPU-ausgeführte Aufgaben.
- Aktuell — Der aktuelle Wert der Metrik. In der ersten Zeile beträgt der aktuelle Wert 162 Prozesse (3x).

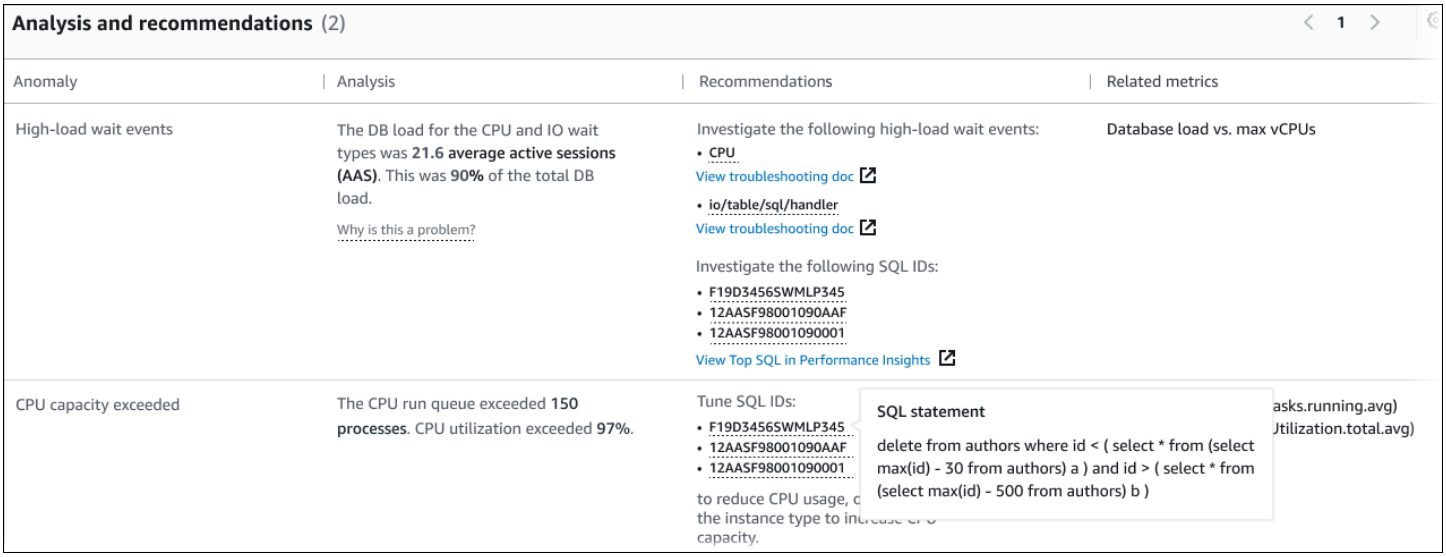
- Normalerweise — Die Basislinie dieser Metrik für diese Datenbank, wenn sie normal funktioniert. DevOpsGuru for RDS berechnet den Basiswert als den 95. Perzentilwert für einen Zeitraum von einer Woche. Die erste Zeile gibt an, dass in der Regel 56 Prozesse auf der CPU laufen.
- Beitrag dazu — Das mit dieser Metrik verknüpfte Ergebnis. In der ersten Zeile ist die Metrik „CPU-Ausführung von Aufgaben“ mit der Anomalie bei Überschreitung der CPU-Kapazität verknüpft.

Die Zeitleistenspalte zeigt ein Liniendiagramm für die Metrik. Der schattierte Bereich zeigt das Zeitintervall, in dem DevOps Guru for RDS den Befund als schwerwiegend eingestuft hat.

Analyse und Empfehlungen

Während die kausale Anomalie das Gesamtproblem beschreibt, beschreibt eine kontextuelle Anomalie einen bestimmten Befund, der untersucht werden muss. Jedes Ergebnis entspricht einer Reihe verwandter Metriken.

Im folgenden Beispiel eines Abschnitts „Analyse und Empfehlungen“ wurden für die Anomalie bei hoher DB-Auslastung zwei Ergebnisse gefunden.



Diese Tabelle hat die folgenden Spalten:

- Anomalie — Eine allgemeine Beschreibung dieser kontextuellen Anomalie. In diesem Beispiel handelt es sich bei der ersten Anomalie um Warteereignisse mit hoher Auslastung und bei der zweiten um eine Überschreitung der CPU-Kapazität.
- Analyse — Eine detaillierte Erklärung der Anomalie.

Bei der ersten Anomalie tragen drei Wartetypen zu 90% der DB-Auslastung bei. Bei der zweiten Anomalie überstieg die CPU-Ausführungswarteschlange 150, was bedeutet, dass zu einem bestimmten Zeitpunkt mehr als 150 Sitzungen auf CPU-Zeit warteten. Die CPU-Auslastung lag bei über 97%, was bedeutet, dass die CPU während der Dauer des Problems zu 97% der Zeit ausgelastet war. Somit war die CPU fast ununterbrochen ausgelastet, während durchschnittlich 150 Sitzungen darauf warteten, auf der CPU ausgeführt zu werden.

- Empfehlungen — Die empfohlene Reaktion des Benutzers auf die Anomalie.

  Bei der ersten Anomalie empfiehlt DevOps Guru for RDS, dass Sie die Warteereignisse `cpu` untersuchen und. `io/table/sql/handler` Um zu erfahren, wie Sie Ihre Datenbankleistung auf der Grundlage dieser Ereignisse optimieren können, finden Sie unter cpu io/table und/ sql/handler im Amazon Aurora-Benutzerhandbuch.

  Bei der zweiten Anomalie empfiehlt DevOps Guru for RDS, dass Sie den CPU-Verbrauch reduzieren, indem Sie drei SQL-Anweisungen optimieren. Sie können den Mauszeiger über die Links bewegen, um den SQL-Text zu sehen.

- Verwandte Metriken — Metriken, die Ihnen spezifische Messwerte für die Anomalie geben. Weitere Informationen zu diesen Metriken finden Sie unter Metriken-Referenz für Amazon Aurora im Amazon Aurora-Benutzerhandbuch oder Metriken-Referenz für Amazon RDS im Amazon RDS-Benutzerhandbuch.

  Bei der ersten Anomalie empfiehlt DevOps Guru for RDS, die DB-Auslastung mit der maximalen CPU-Auslastung für Ihre Instance zu vergleichen. Bei der zweiten Anomalie wird empfohlen, sich die CPU-Ausführungswarteschlange, die CPU-Auslastung und die SQL-Ausführungsrate anzusehen.

Anzeige proaktiver Anomalien

In Insights können Sie Anomalien für Amazon RDS-Ressourcen einsehen. Jeder proaktive Einblick enthält Details zu einer proaktiven Anomalie. Auf einer Seite mit proaktiven Erkenntnissen finden Sie einen Überblick über die Erkenntnisse, detaillierte Kennzahlen zur Anomalie und Empfehlungen zur Vermeidung künftiger Probleme. Um sich eine proaktive Anomalie anzusehen, rufen Sie die Seite „Proactive Insight“ auf.

Überblick über Einblicke

Der Abschnitt „Insight-Überblick“ enthält Einzelheiten darüber, warum der Insight erstellt wurde. Er zeigt den Schweregrad des Einblicks sowie eine Beschreibung der Anomalie und einen Zeitrahmen für das Auftreten der Anomalie an. Es listet auch die Anzahl der betroffenen Dienste und Anwendungen auf, die von Guru erkannt wurden. DevOps

Metriken

Der Abschnitt „Metriken“ enthält Grafiken der Anomalie. Jedes Diagramm zeigt einen Schwellenwert, der durch das Basisverhalten der Ressource bestimmt wird, sowie Daten der Metrik, die ab dem Zeitpunkt der Anomalie gemeldet wurden.

Empfehlungen für aggregierte Ressourcen

In diesem Abschnitt werden Maßnahmen vorgeschlagen, die Sie ergreifen können, um die gemeldeten Probleme zu beheben, bevor sie zu einem größeren Problem werden. Die Maßnahmen, die Sie ergreifen können, werden in der Spalte Empfohlene benutzerdefinierte Änderung aufgeführt. Die Gründe für die Empfehlungen finden Sie im Abschnitt Warum empfiehlt DevOps Guru das? Spalte. Weitere Informationen darüber, wie Sie auf Empfehlungen reagieren, finden Sie unterthe section called “Reagieren auf -Empfehlungen”.

Reagieren auf -Empfehlungen

Empfehlungen sind der wichtigste Teil der Erkenntnisse. In dieser Phase der Analyse handeln Sie, um das Leistungsproblem zu lösen. In der Regel führen Sie die folgenden Schritte aus:

1. Entscheiden Sie, ob das gemeldete Leistungsproblem auf ein echtes Problem hindeutet.

   In einigen Fällen kann ein Problem erwartet werden und es kann sein, dass es sich um ein harmloses Problem handelt. Wenn Sie beispielsweise eine Testdatenbank einer extremen DB-Belastung aussetzen, meldet DevOps Guru for RDS die Belastung als Leistungsanomalie. Sie müssen diese Anomalie jedoch nicht beheben, da dies ein erwartetes Ergebnis Ihrer Tests ist.

   Wenn Sie feststellen, dass das Problem behoben werden muss, fahren Sie mit dem nächsten Schritt fort.
2. Entscheiden Sie, ob die Empfehlung umgesetzt werden soll.

   In der Empfehlungstabelle werden in einer Spalte die empfohlenen Maßnahmen angezeigt. Für reaktive Erkenntnisse ist dies die Spalte Was wir empfehlen auf einer Detailseite zu reaktiven

Anomalien. Für proaktive Einblicke ist dies die Spalte Empfohlene benutzerdefinierte Änderung auf einer proaktiven Insight-Seite.

DevOpsGuru for RDS bietet eine Liste mit Empfehlungen, die mehrere potenzielle problematische Szenarien abdecken. Stellen Sie nach Durchsicht dieser Liste fest, welche Empfehlung für Ihre aktuelle Situation relevanter ist, und erwägen Sie, sie anzuwenden. Wenn eine Empfehlung für Ihre Situation geeignet ist, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, überspringen Sie den verbleibenden Schritt und beheben Sie das Problem mithilfe manueller Techniken.

3. Führen Sie die empfohlenen Maßnahmen aus.

   DevOpsGuru for RDS empfiehlt, dass Sie eine der folgenden Aktionen ausführen:

   - Führen Sie eine bestimmte Korrekturmaßnahme durch.

     DevOpsGuru for RDS könnte beispielsweise empfehlen, die CPU-Kapazität zu aktualisieren, die Einstellungen des Anwendungspols zu optimieren oder das Leistungsschema zu aktivieren.

   - Untersuchen Sie die Ursache des Problems.

     In der Regel empfiehlt DevOps Guru for RDS, dass Sie bestimmte SQL-Anweisungen oder Warteereignisse untersuchen. Eine Empfehlung könnte beispielsweise darin bestehen, das Warte-Ereignis zu untersuchen`io/table/sql/handler`. Suchen Sie im Amazon Aurora-Benutzerhandbuch unter Tuning with wait events for Aurora PostgreSQL oder Tuning with wait events for Aurora MySQL im Amazon Aurora-Benutzerhandbuch oder unter Tuning with wait events for RDS for PostgreSQL im Amazon RDS-Benutzerhandbuch nach. Führen Sie dann die empfohlenen Aktionen aus.

     > **Important**
     >
     > Wir empfehlen Ihnen alle Änderungen in einer Test-Instance zu prüfen, bevor Sie eine produktive Instance ändern. Auf diese Weise verstehen Sie die Auswirkungen der Änderung.

Überwachung nicht-relationaler Datenbanken mit Guru DevOps

DevOpsGuru ist in der Lage, Erkenntnisse für Ihre nicht-relationalen oder NoSQL-Datenbanken zu generieren, die Ihnen helfen, Ihre Ressourcen gemäß den Best Practices zu konfigurieren. DevOpsGuru kann Ihnen beispielsweise dabei helfen, den Überblick über die Kapazitätsplanung zu

behalten, indem er den future Bedarf auf der Grundlage des vorhandenen Verkehrs prognostiziert. DevOpsGuru kann erkennen, ob Sie weniger Ressourcen verbrauchen als Sie konfiguriert haben, und anhand Ihrer bisherigen Nutzung Empfehlungen zur Verbesserung der Anwendungsverfügbarkeit geben. Dies kann Ihnen helfen, unnötige Kosten zu reduzieren.

Neben der Kapazitätsplanung erkennt DevOps Guru betriebliche Probleme wie Drosselung, Transaktionskonflikte, Fehler bei der bedingten Überprüfung und hilft Ihnen bei der Behebung von Verbesserungsmöglichkeiten bei den SDK-Parametern. Datenbanken sind in der Regel mit mehreren Diensten und Ressourcen verbunden, und DevOps Guru kann Ihre Anwendungsstruktur für Analysen anhand von Gruppen, die auf Tagging oder Aggregation basieren, korrelieren. CloudFormation Anomalien können mehrere Ressourcen betreffen, die alle von derselben Lösung betroffen sind. DevOps Guru ist in der Lage, verschiedene Ressourcenmetriken, Konfigurationen, Protokolle und Ereignisse zu korrelieren. DevOpsGuru kann beispielsweise Daten aus einer Lambda-Funktion analysieren und miteinander verknüpfen, die Daten aus einer Amazon DynamoDB Tabelle liest oder schreibt. Auf diese Weise überwacht DevOps Guru mehrere verwandte Ressourcen, um Anomalien zu erkennen und nützliche Erkenntnisse für Ihre Datenbanklösungen zu gewinnen.

Überwachung von Datenbankoperationen in Amazon DynamoDB

Die folgende Tabelle zeigt Beispielszenarien und Erkenntnisse, nach denen DevOps Guru Ausschau hält Amazon DynamoDB.

Amazon DynamoDB Anwendungsfall	Beispiele	Kennzahlen
Erkennt, wenn ein großer Prozentsatz von AccountProvisionedReadCapacityUtilization und AccountProvisionedWriteCapacityUtilization aufgrund einer großen Anzahl von Lese- und Schreibanforderungen verwendet wird.	Amazon DynamoDB Die Kapazität des Tabellenverbrauchs für Lese- oder Schreibanforderungen erreicht die Grenzwerte auf Tabellenebene.	AccountProvisionedReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
Erkennt Fehler bei der bedingten Prüfung in Amazon DynamoDB Anfragen, die darauf zurückzuführen sind,	Fehler bei der bedingten Prüfung werden durch fehlerhafte Daten in Ihrer Tabelle, durch einen strikten	ConditionalCheckFailedRequests

Amazon DynamoDB Anwendungsfall	Beispiele	Kennzahlen
dass ein bereitgestellter Bedingungsausdruck nicht den Erwartungen in der Datenbank entspricht.	Bedingungsausdruck oder durch Rennbedingungen verursacht.	

Überwachung von Datenbankoperationen in Amazon ElastiCache

Die folgende Tabelle zeigt Beispielszenarien und Erkenntnisse, nach denen DevOps Guru Ausschau hält Amazon ElastiCache.

Szenario, das DevOps Guru identifiziert	CloudWatch überwachte Metriken
Ermitteln Sie, wann ein Amazon ElastiCache Cluster aufgrund sich ändernder Anforderungen an Ihre Cluster sein Rechenlimit für Redis oder Memcached erreicht.	CPUUtilization, Engine, Räumungen CPUUtilization

Integration mit CodeGuru Profiler

Dieser Abschnitt bietet einen Überblick darüber, wie Amazon DevOps Guru in Amazon CodeGuru Profiler integriert wird. In der DevOps Guru-Konsole können Sie sich Empfehlungen von CodeGuru Profiler als Einblicke ansehen.

Amazon DevOps Guru lässt sich mit einer EventBridge verwalteten Regel in Amazon CodeGuru Profiler integrieren. CodeGuru Profiler sendet Ereignisse an. EventBridge Die verwaltete Regel leitet Ereignisse weiter, die mit dem Standardereignisbus gesendet werden. Bei jedem eingehenden Ereignis von CodeGuru Profiler handelt es sich um einen proaktiven Anomaliebericht. Weitere Informationen finden Sie unter Arbeiten mit EventBridge Profiler. CodeGuru

DevOpsGuru unterstützt eingehende Ereignisse mit. EventBridge Ein Ereignis weist auf eine Änderung einer Empfehlung hin, die DevOps Guru identifiziert hat. CodeGuru Profiler sendet alle 24 Stunden ein Heartbeat-Ereignis, um die Kontinuität des Ereignisses aufzuzeigen. Ereignisse enthalten CodeGuru Profiler-Empfehlungsinformationen sowie Metadaten für Ihre Rechenressourcen. Informationen zu einem Event-Lebenszyklus finden Sie unter Amazon EventBridge Events.

Wenn Sie DevOps Guru einrichten, erstellt DevOps Guru in Ihrem Konto die EventBridge verwaltete Regel, die Ereignisse von einem anderen Service weiterleitet. Diese Regel leitet an DevOps Guru weiter. Benachrichtigungen werden gesendet, wenn es ein eingehendes Ereignis gibt.

Ein Event-Bus empfängt Ereignisse von einer Quelle wie DevOps Guru und leitet sie an Regeln weiter, die mit diesem Event-Bus verknüpft sind. Weitere Informationen zu Eventbussen finden Sie unter Eventbusse.

Informationen zu einigen Parametern finden Sie unter EventBridgeAmazon-Ereignisse.

Um CodeGuru Profiler-Einblicke in DevOps Guru zu erhalten, müssen Sie über die folgenden Voraussetzungen verfügen.

- CodeGuru Profiler muss aktiviert sein. Informationen zur Aktivierung von CodeGuru Profiler finden Sie unter Profiler einrichten CodeGuru .
- DevOpsGuru muss aktiviert sein. Informationen zur Aktivierung von DevOps Guru finden Sie unter DevOpsGuru aktivieren.
- Dieselben Ressourcen müssen in derselben Region sowohl in CodeGuru Profiler als auch in DevOps Guru überwacht werden.

Definieren von Anwendungen mithilfe von AWS Ressourcen

Amazon DevOps Guru gruppiert die Ressourcen, die sich innerhalb der Deckungsgrenze befinden, und gibt an, welche Ressourcen analysiert werden, um betriebliche Erkenntnisse zu gewinnen. Die Ressourcen sind nach Ressourcen in CloudFormation Stapeln oder nach Ressourcen mit Tags gruppiert. Du wählst die Stapel oder Tags aus, wenn du Guru DevOps einrichtest. Du kannst die Stacks oder Tags auch später aktualisieren. Wir empfehlen Ihnen, Ihre Ressourcengruppen als Anwendungen zu betrachten. Beispielsweise könnten Sie alle Ressourcen, die Sie für eine Überwachungsanwendung verwenden, in einem Stack definiert haben. Oder Sie könnten allen Ressourcen, die Sie in einer Datenbankanwendung verwenden, dasselbe Tag hinzufügen. Die Grenze, die definiert, welche Ressourcen DevOps Guru analysiert. Alle Ressourcen in der Sammlung befinden sich innerhalb dieser Grenze. Alle Ressourcen in Ihrem Konto, die nicht in Ihrer Ressourcensammlung enthalten sind, befinden sich außerhalb der Grenze und werden nicht analysiert. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

Sie können Ihre Deckungsgrenze, die die Ressourcen in Ihren Anwendungen umfasst, auf drei Arten definieren.

- Geben Sie an, dass alle AWS Ressourcen in Ihrem AWS Konto und Ihrer Region unterstützt werden. Dadurch werden Ihr Konto und Ihre Region zu Ihrer Ressourcengrenze. Mit dieser Option analysiert DevOps Guru alle unterstützten Ressourcen in deinem Konto und deiner Region. Alle Ressourcen, die sich in einem Stapel befinden, werden zu einer Anwendung zusammengefasst. Alle Ressourcen, die sich nicht in einem Stapel befinden, werden in einer eigenen Anwendung gruppiert.
- Verwenden Sie CloudFormation Stacks, um die Ressourcen in Ihren Anwendungen anzugeben. Ein Stapel enthält Ressourcen, die mit CloudFormation generiert werden. In DevOps Guru wählst du Stapel in deinem Konto aus. Die Ressourcen, die Sie in jedem Stapel, den Sie auswählen, sind in einer Anwendung gruppiert. Alle Ressourcen in den Stacks werden von DevOps Guru analysiert, um Erkenntnisse zu gewinnen.
- Verwenden Sie AWS Tags, um die Ressourcen in Ihren Anwendungen zu spezifizieren. Ein AWS Tag enthält einen Schlüssel und einen Wert. Wählen Sie in DevOps Guru einen Tag-Schlüssel und optional einen oder mehrere Werte, die mit diesem Schlüssel verknüpft sind. Sie können die Werte verwenden, um Ihre Ressourcen in Anwendungen zu gruppieren.

Weitere Informationen finden Sie unter Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps.

Themen

- Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren
- Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen

Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren

Sie können Tags verwenden, um die AWS Ressourcen zu identifizieren, die Amazon DevOps Guru analysiert, und um anhand des ausgewählten Tag-Schlüssels und der Tag-Werte festzulegen, welche Ressourcen für die Überwachung gruppiert werden. Sie können diese Konfigurationen bearbeiten, wenn Sie DevOps Guru einrichten oder wenn Sie auf der Seite „Analysierte Ressourcen“ die Option „Analysierte Ressourcen bearbeiten“ wählen. Nachdem Sie Tags ausgewählt haben, wählen Sie einen bestimmten Tag-Schlüssel, den Amazon DevOps Guru überwachen soll. Um alle Ressourcen im Konto zu analysieren und die Ressourcen anhand von Tag-Werten zu gruppieren, wählen Sie Alle Kontoressourcen aus. Um anhand von Tag-Werten die Ressourcen zu spezifizieren, die DevOps Guru analysieren soll, wähle Bestimmte Tag-Werte auswählen aus.

> **Note**
>
> Wenn „Alle Kontoressourcen“ ausgewählt ist und kein Tag-Wert existiert, werden Ressourcen ohne Tag-Schlüssel gruppiert und separat analysiert.

Sie verwenden den Schlüssel eines Tags, um die Ressourcen zu identifizieren, und verwenden dann Werte mit diesem Schlüssel, um Ressourcen in Ihren Anwendungen zu gruppieren. Beispielsweise können Sie Ihre Ressourcen mit dem Schlüssel kennzeichnen `devops-guru-applications` und diesen Schlüssel dann mit einem anderen Wert für jede Ihrer Anwendungen verwenden. Sie können das Tag-Schlüssel-Wert-Paar und `devops-guru-applications/databasedevops-guru-applications/cicd`, verwenden, `devops-guru-applications/monitoring` um drei Anwendungen in Ihrem Konto zu identifizieren. Jede Anwendung besteht aus verwandten Ressourcen, die dasselbe Tag-Schlüssel-Wert-Paar enthalten. Sie fügen Ihren

Ressourcen mithilfe des AWS Dienstes, zu dem sie gehören, Tags hinzu. Weitere Informationen finden Sie unter Hinzufügen AWS Schlagworte zu AWS Ressourcen.

Nachdem Sie den Ressourcen in Ihrer Anwendung ein Tag hinzugefügt haben, können Sie Ihre Erkenntnisse nach den Tags der Ressourcen filtern, die sie generiert haben. Weitere Informationen zum Filtern Ihrer Erkenntnisse mithilfe eines Tags finden Sie unterEinblicke von DevOps Guru anzeigen.

Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

Themen

- Was ist ein AWS Etikett?
- Definition einer DevOps Guru-Anwendung mithilfe eines Tags
- Verwenden von Stichwörtern mit DevOps Guru
- Hinzufügen AWS Schlagworte zu AWS Ressourcen

Was ist ein AWS Etikett?

Mithilfe von Stichwörtern können Sie Ihre AWS Ressourcen identifizieren und organisieren. Viele AWS Dienste unterstützen Tagging, sodass Sie Ressourcen aus verschiedenen Diensten dasselbe Tag zuweisen können, um anzuzeigen, dass die Ressourcen miteinander verwandt sind. Beispielsweise können Sie einer Amazon DynamoDB-Tabellenressource dasselbe Tag zuweisen, das Sie einer Funktion zuweisen. AWS Lambda Weitere Informationen zur Verwendung von Tags finden Sie im Whitepaper Bewährte Methoden für die Markierung.

Jedes AWS Tag besteht aus zwei Teilen.

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment`, `Project` oder `Secret`). Bei Tag-Schlüsseln wird die Groß- und Kleinschreibung beachtet.
- einem optionalen Feld, das als Tag-Wert bezeichnet wird (z. B. `111122223333`, `Production` oder ein Team-Name). Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge. Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Zusammen werden sie als Schlüssel-Wert-Paare bezeichnet.

Definition einer DevOps Guru-Anwendung mithilfe eines Tags

Um Ihre Amazon DevOps Guru-Anwendung mithilfe eines Tags zu definieren, fügen Sie dieses Tag den AWS Ressourcen in Ihrem Konto hinzu, aus denen Ihre Anwendung besteht. Ihr Tag enthält einen Schlüssel und einen Wert. Wir empfehlen, dass du jeder deiner von DevOps Guru analysierten AWS Ressourcen ein Tag hinzufügst, das denselben Schlüssel hat. Verwenden Sie einen anderen Wert im Tag, um Ressourcen in Ihren Anwendungen zu gruppieren. Sie können beispielsweise allen AWS Ressourcen innerhalb Ihrer Abdeckungsgrenze Stichwörter mit dem Schlüssel `devops-guru-analysis-boundary` zuweisen. Verwenden Sie für diesen Schlüssel unterschiedliche Werte, um Anwendungen in Ihrem Konto zu identifizieren. Sie können die Werte `containersdatabase`, und `monitoring` für drei Anwendungen verwenden. Weitere Informationen finden Sie unter Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps.

Wenn Sie AWS Tags verwenden, um anzugeben, welche Ressourcen analysiert werden sollen, können Sie Tags mit nur einem Schlüssel verwenden. Sie können den Schlüssel Ihrer Tags mit einem beliebigen Wert kombinieren. Verwenden Sie den Wert, um die Ressourcen, die Ihren Schlüssel enthalten, in Ihren betrieblichen Anwendungen zu gruppieren.

> **Important**
>
> Wenn Sie einen Schlüssel erstellen, können Sie die Groß-/Kleinschreibung im Schlüssel beliebig auswählen. Nachdem Sie einen Schlüssel erstellt haben, wird die Groß-/Kleinschreibung berücksichtigt. DevOpsGuru arbeitet beispielsweise mit einem benannten Schlüssel `devops-guru-rds` und einem benannten Schlüssel`DevOps-Guru-RDS`, und diese dienen als zwei verschiedene Schlüssel. Mögliche Schlüssel/Wert-Paare in Ihrer Anwendung könnten `Devops-Guru-production-application/RDS` oder `Devops-Guru-production-application/containers` sein.

Verwenden von Stichwörtern mit DevOps Guru

Geben Sie die AWS Tags an, die die AWS Ressourcen identifizieren, die Amazon DevOps Guru analysieren soll, oder geben Sie Tag-Werte an, die angeben, welche Ressourcen gruppiert werden. Diese Ressourcen bilden die Grenze Ihrer Ressourcenabdeckung. Sie können einen Schlüssel und null oder mehr Werte auswählen.

Um deine Schlagworte auszuwählen

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und erweitern Sie dann Einstellungen.
3. Wählen Sie unter Analysierte Ressourcen die Option Bearbeiten aus.
4. Wähle „Tags“, wenn du möchtest, dass DevOps Guru alle Ressourcen analysiert, die die von dir ausgewählten Stichwörter enthalten. Wähle einen Schlüssel und dann eine der folgenden Optionen.

   - Alle Kontoressourcen — Analysieren Sie alle AWS Ressourcen in der aktuellen Region und im aktuellen Konto. Ressourcen mit dem ausgewählten Tag-Schlüssel werden nach Tag-Werten gruppiert, falls vorhanden. Ressourcen ohne diesen Tag-Schlüssel werden gruppiert und separat analysiert.
   - Wählen Sie bestimmte Tag-Werte — Alle Ressourcen, die ein Tag mit dem von Ihnen ausgewählten Schlüssel enthalten, werden analysiert. DevOpsGuru gruppiert deine Ressourcen nach den Werten deines Tags in Anwendungen.

5. Wählen Sie Speichern.

Hinzufügen AWS Schlagworte zu AWS Ressourcen

Wenn du die AWS Tags angibst, die die AWS Ressourcen identifizieren, die DevOps Guru analysieren soll, wähle Tags aus, denen Ressourcen zugeordnet sind. Du kannst Tags zu deinen Ressourcen hinzufügen, indem du den AWS Dienst verwendest, zu dem die einzelnen Ressourcen gehören, oder den AWS Tag-Editor verwendest.

- Um Tags mithilfe des Dienstes Ihrer Ressourcen zu verwalten, verwenden Sie die Konsole oder das SDK des Dienstes AWS Command Line Interface, zu dem eine Ressource gehört. Sie können beispielsweise eine Amazon Kinesis-Stream-Ressource oder eine CloudFront Amazon-Vertriebsressource taggen. Dies sind zwei Beispiele für Dienste mit Ressourcen, die mit Tags versehen werden können. Die meisten Ressourcen, die DevOps Guru analysieren kann, unterstützen Tags. Weitere Informationen finden Sie unter Tagging your streams im Amazon Kinesis Developer Guide und Tagging a distribution im Amazon CloudFront Developer Guide. Informationen zum Hinzufügen von Tags zu anderen Arten von Ressourcen finden Sie im Benutzer- oder Entwicklerhandbuch des AWS Dienstes, zu dem sie gehören.

> **Note**
>
> Wenn Sie Amazon RDS-Ressourcen taggen, müssen Sie die Datenbank-Instance und nicht den Cluster taggen.

- Sie können den AWS Tag-Editor verwenden, um Tags nach Ressourcen in Ihrer Region und nach Ressourcen in bestimmten AWS Diensten zu verwalten. Weitere Informationen finden Sie unter Tag-Editor im Benutzerhandbuch für AWS Ressourcengruppen und Tags.

Wenn Sie einer Ressource ein Tag hinzufügen, können Sie nur den Schlüssel oder den Schlüssel und einen Wert hinzufügen. Sie können beispielsweise ein Tag mit dem Schlüssel `devops-guru-` für alle Ressourcen erstellen, die Teil Ihrer DevOps Anwendung sind. Sie können auch ein Tag mit dem Schlüssel `devops-guru-` und dem Wert `RDS` hinzufügen und dieses Schlüssel-Wert-Paar dann nur den Amazon RDS-Ressourcen in Ihrer Anwendung hinzufügen. Dies ist nützlich, wenn Sie Einblicke in der Konsole anzeigen möchten, die nur aus den Amazon RDS-Ressourcen in Ihrer Anwendung generiert wurden.

Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen

Sie können AWS CloudFormation Stacks verwenden, um anzugeben, welche AWS Ressourcen DevOps Guru analysieren soll. Ein Stapel ist eine Sammlung von AWS Ressourcen, die als eine Einheit verwaltet werden. Die Ressourcen in den Stacks, die du auswählst, bilden die Deckungsgrenze deines DevOps Gurus. Für jeden Stack, den Sie auswählen, werden die Betriebsdaten in den unterstützten Ressourcen auf anomales Verhalten hin analysiert. Diese Probleme werden dann nach verwandten Anomalien gruppiert, um Erkenntnisse zu gewinnen. Jeder Einblick enthält eine oder mehrere Empfehlungen, die Ihnen helfen, diese Probleme zu lösen. Die maximale Anzahl von Stacks, die Sie angeben können, ist 1000. Weitere Informationen finden Sie unter Arbeiten mit Stacks im AWS CloudFormation Benutzerhandbuch und. Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps

Nachdem du einen Stapel ausgewählt hast, beginnt DevOps Guru sofort mit der Analyse aller Ressourcen, die du ihm hinzufügst. Wenn du eine Ressource aus einem Stapel entfernst, wird sie nicht mehr analysiert.

Wenn du dich dafür entscheidest, dass DevOps Guru alle unterstützten Ressourcen in deinem Konto analysiert (das bedeutet, dass dein AWS Konto und deine Region die Grenze deiner DevOps Guru-Abdeckung bilden), analysiert DevOps Guru alle unterstützten Ressourcen in deinem Konto und erstellt daraus Erkenntnisse, einschließlich der Ressourcen in Stapeln. Erkenntnisse, die sich aus Anomalien in einer Ressource ergeben, die sich nicht in einem Stapel befindet, werden auf Kontoebene gruppiert. Wenn ein Insight aus Anomalien in einer Ressource gewonnen wird, die sich in einem Stack befindet, wird er auf Stack-Ebene gruppiert. Weitere Informationen finden Sie unter Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden.

Auswahl von Stacks, die Guru analysieren soll DevOps

Geben Sie die Ressourcen an, die Amazon DevOps Guru analysieren soll, indem Sie die CloudFormation Stapel auswählen, aus denen sie erstellt werden. Sie können dies mit dem AWS-Managementkonsole oder dem SDK tun.

Themen

- Stapel auswählen, die DevOps Guru analysieren soll (Konsole)
- Stapel auswählen, die DevOps Guru analysieren soll (DevOpsGuru SDK)

Stapel auswählen, die DevOps Guru analysieren soll (Konsole)

Sie können AWS CloudFormation Stapel mithilfe der Konsole hinzufügen.

Um die Stacks auszuwählen, die die zu analysierenden Ressourcen enthalten

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und wählen Sie dann Einstellungen.
3. Wählen Sie unter DevOpsGuru Analysis Coverage die Option Verwalten aus.
4. Wählen Sie CloudFormation Stapel, wenn DevOps Guru die Ressourcen analysieren soll, die sich in den von Ihnen ausgewählten Stapeln befinden, und wählen Sie dann eine der folgenden Optionen.

    - Alle Ressourcen — Alle Ressourcen, die sich in deinem Konto in Stapeln befinden, werden analysiert. Die Ressourcen in jedem Stapel sind in einer eigenen Anwendung gruppiert. Alle Ressourcen in Ihrem Konto, die sich nicht in einem Stapel befinden, werden nicht analysiert.

- Stapel auswählen — Wählen Sie die Stapel aus, die DevOps Guru analysieren soll. Die Ressourcen in jedem Stapel, den Sie auswählen, sind in einer eigenen Anwendung gruppiert. Sie können den Namen eines Stacks in Find Stacks eingeben, um schnell einen bestimmten Stack zu finden. Sie können bis zu 1.000 Stapel auswählen.

5. Wählen Sie Speichern.

Stapel auswählen, die DevOps Guru analysieren soll (DevOpsGuru SDK)

Verwenden Sie die `UpdateResourceCollection` Methode, um CloudFormation Stapel mithilfe des Amazon DevOps Guru SDK zu spezifizieren. Weitere Informationen finden Sie UpdateResourceCollectionin der Amazon DevOps Guru API-Referenz.

Zusammenarbeit mit Amazon EventBridge

Amazon DevOps Guru integriert sich in Amazon EventBridge um Sie über bestimmte Ereignisse im Zusammenhang mit Erkenntnissen und entsprechenden Insight-Updates zu informieren. Ereignisse von AWS Dienstleistungen werden erbracht an EventBridge fast in Echtzeit. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen durchgeführt werden sollen, wenn sich für ein Ereignis eine Übereinstimmung mit einer Regel ergibt. Zu den Aktionen, die automatisch initiiert werden können, gehören die folgenden Beispiele:

- Aufrufen eines AWS Lambda wirken
- Aufrufen eines Amazon Elastic Compute Cloud-Ausführungsbefehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer Step Functions-Zustandsmaschine
- Einen Amazon SNS oder einen Amazon SQS benachrichtigen

Sie können eines der folgenden vordefinierten Muster auswählen, um Ereignisse zu filtern, oder eine benutzerdefinierte Musterregel erstellen, um Aktionen in einer unterstützten Umgebung zu initiieren AWS Ressourcen.

- DevOps Guru New Insight Öffnen
- DevOps Guru New Anomaly Association
- DevOps Guru Insight-Schweregrad wurde verbessert
- DevOps Guru: Neue Empfehlung erstellt
- DevOps Guru Insight geschlossen

Veranstaltungen für DevOps Guru

Im Folgenden finden Sie Beispielereignisse von DevOps Guru. Ereignisse werden auf die bestmögliche Weise ausgegeben. Weitere Informationen zu Ereignismustern finden Sie unter Erste Schritte mit Amazon EventBridge oder Amazon EventBridge Event-Muster.

DevOps Guru New Insight: Offene Veranstaltung

Wann DevOps Guru öffnet einen neuen Einblick, er sendet das folgende Ereignis.

```
{
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
```

```
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
  },
```

Benutzerdefiniertes Beispielereignismuster für einen neuen Einblick mit hohem Schweregrad

Regeln verwenden Ereignismuster, um Ereignisse auszuwählen und sie an Ziele zu routen. Das Folgende ist ein Beispiel DevOps Guru-Event-Muster.

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

Aktualisierung der DevOps Guru-Einstellungen

Sie können die folgenden Amazon DevOps Guru-Einstellungen aktualisieren:

- Ihre DevOps Guru-Berichterstattung. Dies bestimmt, welche Ressourcen in Ihrem Konto analysiert werden.
- Ihre Benachrichtigungen. Dies bestimmt, welche Amazon Simple Notification Service-Themen verwendet werden, um Sie über wichtige DevOps Guru-Ereignisse zu informieren.
- Funktionen für bessere Einblicke. Dazu gehören die Erkennung von Protokollanomalien, Verschlüsselung und Ihre AWS Systems Manager Integrationseinstellungen. Dies bestimmt, ob DevOps Guru Protokolldaten anzeigt, ob Sie zusätzliche Sicherheitsschlüssel verwenden und ob OpsCenter für jeden neuen Einblick eine im Systems Manager erstellt OpsItem wird.

Themen

- Aktualisierung der Einstellungen Ihres Verwaltungskontos
- Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps
- Aktualisierung deiner Benachrichtigungen in DevOps Guru
- Deine DevOps Guru-Benachrichtigungen filtern
- Aktualisierung der AWS Systems Manager Integration in Guru DevOps
- Aktualisierung der Erkennung von Protokollanomalien in Guru DevOps
- Aktualisierung der Verschlüsselungseinstellungen in DevOps Guru

Aktualisierung der Einstellungen Ihres Verwaltungskontos

Du kannst DevOps Guru für Konten in deiner Organisation konfigurieren. Wenn Sie keinen delegierten Administrator registriert haben, können Sie dies tun, indem Sie Delegierten Administrator registrieren wählen. Weitere Informationen zur Registrierung eines delegierten Administrators finden Sie unter Guru aktivieren. DevOps

Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps

Sie können aktualisieren, welche AWS Ressourcen in Ihrem Konto DevOps Guru analysiert. Navigieren Sie dazu in der Konsole zur Seite Analysierte Ressourcen und wählen Sie dann Bearbeiten. Weitere Informationen finden Sie unter Analysierte Ressourcen anzeigen.

Aktualisierung deiner Benachrichtigungen in DevOps Guru

Richten Sie Amazon Simple Notification Service-Themen ein, mit denen Sie über wichtige Amazon DevOps Guru-Ereignisse informiert werden. Sie können aus einer Liste von Themennamen wählen, die bereits in Ihrem AWS Konto vorhanden sind, den Namen für ein neues Thema eingeben, das DevOps Guru in Ihrem Konto erstellt, oder den Amazon-Ressourcennamen (ARN) eines vorhandenen Themas in einem beliebigen AWS Konto in Ihrer Region eingeben. Wenn Sie den ARN eines Themas angeben, das nicht in Ihrem Konto enthalten ist, müssen Sie DevOps Guru die Erlaubnis erteilen, auf dieses Thema zuzugreifen, indem Sie dem Thema eine IAM-Richtlinie hinzufügen. Weitere Informationen finden Sie unter Berechtigungen für Amazon SNS-Themen. Sie können bis zu zwei Themen angeben.

DevOpsGuru sendet Benachrichtigungen für die folgenden Updates:

- Eine neue Einsicht wird geschaffen.
- Eine neue Anomalie wird zu einer Erkenntnis hinzugefügt.
- Der Schweregrad eines Einblicks wird von `Low` oder `Medium` auf `High` erhöht.
- Der Status einer Erkenntnis ändert sich von „Aktuell“ zu „Gelöst“.
- Es wird eine Empfehlung für einen Einblick identifiziert.

DevOpsGuru sendet auch Benachrichtigungen, wenn ein ausgewählter CloudFormation Stack- oder Tag-Schlüssel ungültig ist, wenn du versuchst, Ressourcen zu deinem DevOps Guru-Konto hinzuzufügen.

Sie können wählen, ob Sie Amazon SNS SNS-Benachrichtigungen für alle Arten von Updates zu einem Problem erhalten möchten oder ob Sie Amazon SNS SNS-Benachrichtigungen nur erhalten möchten, wenn das Problem geöffnet oder geschlossen wurde oder sich der Schweregrad geändert hat. Standardmäßig erhalten Sie Benachrichtigungen für alle Updates.

Um Ihre Benachrichtigungen zu aktualisieren, navigieren Sie zunächst zur Benachrichtigungsseite und wählen Sie dann aus, ob Sie Konfigurationen für Amazon SNS SNS-Benachrichtigungsthemen hinzufügen, entfernen oder aktualisieren möchten.

Themen

- Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole
- Hinzufügen von Amazon SNS SNS-Benachrichtigungsthemen in der DevOps Guru-Konsole
- Amazon SNS SNS-Benachrichtigungsthemen in der DevOps Guru-Konsole entfernen
- Aktualisierung der Amazon SNS SNS-Benachrichtigungskonfigurationen
- Ihrem Amazon SNS SNS-Thema hinzugefügte Berechtigungen

Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole

Um Benachrichtigungen zu aktualisieren, musst du zuerst zum Abschnitt mit den Benachrichtigungseinstellungen navigieren.

Um zum Abschnitt mit den Benachrichtigungseinstellungen zu navigieren

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.

   Die Seite Einstellungen enthält den Abschnitt Benachrichtigungen mit Informationen zu konfigurierten Amazon SNS SNS-Themen.

Hinzufügen von Amazon SNS SNS-Benachrichtigungsthemen in der DevOps Guru-Konsole

Um ein Amazon SNS SNS-Benachrichtigungsthema in der DevOps Guru-Konsole hinzuzufügen

1. the section called “Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole”.
2. Wählen Sie Add notification (Benachrichtigung hinzufügen) aus.
3. Gehen Sie wie folgt vor, um ein Amazon SNS SNS-Thema hinzuzufügen.

- Wählen Sie Neues SNS-Thema per E-Mail generieren aus. Geben Sie dann unter E-Mail-Adresse angeben die E-Mail-Adresse ein, an die Sie Benachrichtigungen erhalten möchten. Um weitere E-Mail-Adressen einzugeben, wählen Sie Neue E-Mail hinzufügen aus.
- Wählen Sie „Bestehendes SNS-Thema verwenden“. Wählen Sie dann unter Wählen Sie ein Thema in Ihrem AWS Konto aus das Thema aus, das Sie verwenden möchten.
- Wählen Sie Use an existing SNS topic ARN, um ein bestehendes Thema aus einem anderen Konto anzugeben. Geben Sie dann unter Geben Sie einen ARN für ein Thema ein den Themen-ARN ein. Der ARN ist der Amazon-Ressourcenname des Themas. Sie können ein Thema in einem anderen Konto angeben. Wenn Sie ein Thema in einem anderen Konto verwenden, müssen Sie dem Thema eine Ressourcenrichtlinie hinzufügen. Weitere Informationen finden Sie unter Berechtigungen für Amazon SNS-Themen.

4. Wählen Sie Save (Speichern) aus.

Amazon SNS SNS-Benachrichtigungsthemen in der DevOps Guru-Konsole entfernen

So entfernen Sie Amazon SNS SNS-Themen in der DevOps Guru-Konsole

1. the section called “Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole”.
2. Wählen Sie Bestehendes Thema auswählen.
3. Wählen Sie im Dropdownmenü das Thema aus, das Sie entfernen möchten.
4. Wählen Sie Remove (Entfernen) aus.
5. Wählen Sie Speichern.

Aktualisierung der Amazon SNS SNS-Benachrichtigungskonfigurationen

In DevOps Guru gibt es zwei Arten von Benachrichtigungskonfigurationen für Amazon SNS SNS-Benachrichtigungsthemen. Sie können wählen, ob Sie Benachrichtigungen mit allen Schweregraden oder nur Benachrichtigungen mit den Schweregraden Hoch und Mittel erhalten möchten. Sie können auch wählen, ob Sie Benachrichtigungen für alle Arten von Updates oder nur für einige Arten von Updates erhalten möchten.

Wenn Sie Amazon SNS SNS-Benachrichtigungen für alle Arten von Updates zu dem Problem erhalten möchten, sendet DevOps Guru Benachrichtigungen für die folgenden Updates:

- Es entsteht eine neue Einsicht.
- Eine neue Anomalie wird zu einer Erkenntnis hinzugefügt.
- Der Schweregrad eines Einblicks wird von `Low` oder `Medium` auf `High` erhöht.
- Der Status einer Erkenntnis ändert sich von „Aktuell“ zu „Gelöst“.
- Es wird eine Empfehlung für einen Einblick identifiziert.

Standardmäßig erhalten Sie nur Benachrichtigungen mit dem Schweregrad Hoch und Mittel sowie Benachrichtigungen für alle Arten von Updates.

So aktualisieren Sie die Benachrichtigungskonfigurationen für Amazon SNS SNS-Benachrichtigungsthemen

1. the section called “Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole”.
2. Wählen Sie Bestehendes Thema auswählen.
3. Wählen Sie im Dropdownmenü das Thema aus, für das Sie Aktualisierungen vornehmen möchten.
4. Wählen Sie Alle Schweregrade, um Benachrichtigungen mit den Schweregraden Hoch, Mittel und Niedrig zu erhalten, oder wählen Sie Nur Hoch und Mittel, um Benachrichtigungen mit den Schweregraden Hoch und Mittel zu erhalten.
5. Wählen Sie „Ich möchte über alle Aktualisierungen des Insights informiert werden“ oder „Benachrichtige mich, wenn ein Insight geöffnet oder geschlossen wird oder wenn sich der Schweregrad von Niedrig oder Mittel auf Hoch“ ändert.
6. Wählen Sie Speichern.

Ihrem Amazon SNS SNS-Thema hinzugefügte Berechtigungen

Ein Amazon SNS SNS-Thema ist eine Ressource, die eine AWS Identity and Access Management (IAM-) Ressourcenrichtlinie enthält. Wenn Sie hier ein Thema angeben, fügt DevOps Guru seiner Ressourcenrichtlinie die folgenden Berechtigungen hinzu.

```
{
```

```
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

Diese Berechtigungen sind erforderlich, damit DevOps Guru Benachrichtigungen veröffentlichen kann, die ein Thema verwenden. Wenn du es vorziehst, diese Berechtigungen für das Thema nicht zu haben, kannst du sie ohne Bedenken entfernen. Das Thema funktioniert dann weiterhin so, wie es vor deiner Auswahl funktioniert hat. Wenn diese angehängten Berechtigungen jedoch entfernt werden, kann DevOps Guru das Thema nicht zum Generieren von Benachrichtigungen verwenden.

Deine DevOps Guru-Benachrichtigungen filtern

Sie können Ihre DevOps Guru-Benachrichtigungen nach the section called “Aktualisierung der Amazon SNS SNS-Benachrichtigungskonfigurationen” oder mithilfe einer Amazon SNS SNS-Abonnementfilterrichtlinie filtern.

Themen

- Filtern von Benachrichtigungen mit einer Amazon SNS SNS-Abonnementfilterrichtlinie
- Beispiel für eine gefilterte Amazon SNS SNS-Benachrichtigung für Amazon Guru DevOps

Filtern von Benachrichtigungen mit einer Amazon SNS SNS-Abonnementfilterrichtlinie

Sie können eine Abonnementfilterrichtlinie für Amazon Simple Notification Service (Amazon SNS) erstellen, um die Anzahl der Benachrichtigungen zu reduzieren, die Sie von Amazon DevOps Guru erhalten.

Verwenden Sie eine Filterrichtlinie, um die Arten von Benachrichtigungen anzugeben, die Sie erhalten. Sie können Ihre Amazon SNS SNS-Nachrichten mit den folgenden Schlüsselwörtern filtern.

- `NEW_INSIGHT`— Erhalten Sie eine Benachrichtigung, wenn ein neuer Insight erstellt wurde.
- `CLOSED_INSIGHT`— Erhalte eine Benachrichtigung, wenn ein vorhandener Insight geschlossen wird.
- `NEW_RECOMMENDATION`— Erhalte eine Benachrichtigung, wenn aus einem Insight eine neue Empfehlung erstellt wird.
- `NEW_ASSOCIATION`— Erhalten Sie eine Benachrichtigung, wenn anhand eines Insights eine neue Anomalie entdeckt wird.
- `CLOSED_ASSOCIATION`— Erhalten Sie eine Benachrichtigung, wenn eine bestehende Anomalie geschlossen wird.
- `SEVERITY_UPGRADED`— Sie erhalten eine Benachrichtigung, wenn der Schweregrad eines Insights erhöht wird

Informationen zum Erstellen einer Amazon SNS SNS-Abonnementfilterrichtlinie finden Sie unter Amazon SNS SNS-Abonnementfilterrichtlinien im Amazon Simple Notification Service Developer Guide. In Ihrer Filterrichtlinie geben Sie eines der Schlüsselwörter zusammen mit den der Richtlinie an. `MessageType` Folgendes würde beispielsweise in einem Filter erscheinen, der angibt, dass das Amazon SNS SNS-Thema nur Benachrichtigungen zustellt, wenn anhand eines Insights eine neue Anomalie erkannt wird.

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

Beispiel für eine gefilterte Amazon SNS SNS-Benachrichtigung für Amazon Guru DevOps

Im Folgenden finden Sie ein Beispiel für eine Amazon Simple Notification Service (Amazon SNS) - Benachrichtigung aus einem Amazon SNS-Thema mit einer Filterrichtlinie. Sie `MessageType` ist auf eingestelltNEW_ASSOCIATION, sodass Benachrichtigungen nur gesendet werden, wenn aufgrund von Insight eine neue Anomalie erkannt wird.

```
{
      "accountId": "123456789012",
```

```
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
```

```
        }
      }
}
```

Aktualisierung der AWS Systems Manager Integration in Guru DevOps

Sie können die Erstellung eines OpsItem für jeden neuen Einblick in aktivieren AWS Systems Manager OpsCenter. OpsCenter ist ein zentralisiertes System, in dem Sie betriebliche Arbeitsaufgaben einsehen, untersuchen und überprüfen können (OpsItems). Das Tool OpsItems For Your Insights kann Ihnen bei der Verwaltung von Aufgaben helfen, die das anomale Verhalten beheben, das zur Erstellung der einzelnen Erkenntnisse geführt hat. Weitere Informationen finden Sie unter AWS Systems Manager OpsCenterund Arbeiten mit OpsItem im AWS Systems Manager Benutzerhandbuch.

> **Note**
>
> Wenn Sie den Schlüssel oder Wert des Tag-Felds eines ändern OpsItem, kann DevOps Guru das nicht aktualisieren OpsItem. Wenn du zum Beispiel ein Tag mit einem OpsItem von `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` in etwas anderes änderst, kann DevOps Guru das nicht aktualisieren OpsItem.

Um Ihre Systems Manager-Integration zu verwalten

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie in der AWS Systems Manager Integration die Option DevOpsGuru aktivieren aus, um OpsCenter für jeden Einblick einen Eingang zu erstellen, damit für jeden neuen Einblick ein Eintrag OpsItem erstellt wird. AWS OpstItem Deaktivieren Sie diese Option, um zu verhindern, dass für jeden neuen Einblick ein neuer Insight OpsItem erstellt wird.

Die in Ihrem Konto OpsItems erstellten Inhalte werden Ihnen in Rechnung gestellt. Weitere Informationen finden Sie unter AWS Systems Manager Preise.

Aktualisierung der Erkennung von Protokollanomalien in Guru DevOps

Um Ihre Einstellungen für die Erkennung von Protokollanomalien zu verwalten

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Wählen Sie unter Erkennung von Protokollanomalien die Option Erkennung von Protokollanomalien aktivieren aus, indem Sie DevOps Guru Berechtigungen zur Anzeige von Protokolldaten gewähren, die mit einem Insight verknüpft sind. damit DevOps Guru Protokolldaten im Zusammenhang mit Erkenntnissen anzeigt.

Aktualisierung der Verschlüsselungseinstellungen in DevOps Guru

Sie können die Verschlüsselungseinstellungen aktualisieren, um AWS eigene Schlüssel oder vom AWS KMS Kunden verwaltete Schlüssel zu verwenden. Wenn Guru von einem bestehenden kundenverwalteten AWS KMS Schlüssel zu einem neuen, vom Kunden verwalteten AWS KMS Schlüssel wechselt, beginnt DevOps Guru automatisch, neu aufgenommene Metadaten mit dem neuen Schlüssel zu verschlüsseln. Die historischen Daten bleiben mit dem zuvor konfigurierten, vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt.

> **Note**
>
> Wenn du die Gewährung widerrufst oder den vorherigen AWS KMS Schlüssel deaktivierst oder löschst, kann DevOps Guru auf keine der mit diesem Schlüssel verschlüsselten Daten zugreifen, und du wirst ihn möglicherweise sehen, `AccessDeniedException` wenn du einen Lesevorgang ausführst.

Um deine Verschlüsselungseinstellungen zu verwalten

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.

3. Wählen Sie im Bereich Verschlüsselung die Option Verschlüsselung bearbeiten aus.
4. Wählen Sie den Verschlüsselungstyp aus, den Sie zum Schutz Ihrer Daten verwenden möchten. Sie können einen AWS eigenen Standardschlüssel verwenden, einen vorhandenen, vom Kunden verwalteten Schlüssel auswählen oder einen neuen vom Kunden verwalteten Schlüssel erstellen. AWS KMS
5. Wählen Sie Speichern.

Verschlüsselung ist ein wichtiger Bestandteil der DevOps Guru-Sicherheit. Weitere Informationen finden Sie unter the section called “Datenschutz”.

Benachrichtigungen anzeigen

In DevOps Guru gibt es verschiedene Arten von Benachrichtigungen.

Themen

- Neue Erkenntnisse
- Geschlossener Einblick
- Neuer Verband
- Neue Empfehlung
- Schweregrad wurde erhöht
- Fehler bei der Ressourcenvalidierung

Die Abschnitte auf dieser Seite zeigen Beispiele für jede Art von Benachrichtigung.

Neue Erkenntnisse

Benachrichtigungen über neue Erkenntnisse enthalten die folgenden Informationen:


```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

Geschlossener Einblick

Benachrichtigungen für Closed Insights enthalten die folgenden Informationen:

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
           ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

Neuer Verband

Benachrichtigungen für neue Verbände enthalten die folgenden Informationen:

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

Neue Empfehlung

Benachrichtigungen über neue Empfehlungen enthalten die folgenden Informationen:

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```


Schweregrad wurde erhöht

Benachrichtigungen für Upgrades auf den Schweregrad enthalten die folgenden Informationen:


```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

Fehler bei der Ressourcenvalidierung

Du kannst CloudFormation Stapel und AWS Tags verwenden, um die AWS Ressourcen zu filtern und zu identifizieren, die DevOps Guru analysieren soll. Wenn du einen ungültigen Stapel oder Tag auswählst, mit dem DevOps Guru Ressourcen identifizieren soll, erstellt DevOps Guru eine `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` Benachrichtigung. Dies kann passieren, wenn dem Tag oder Stacknamen, den Sie angeben, keine Ressourcen zugeordnet sind. Um das Beste aus den DevOps Guru-Filtermethoden herauszuholen, wählen Sie Stacks und Tags aus, denen Ressourcen zugeordnet sind.

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

Von DevOps Guru analysierte Ressourcen anzeigen

DevOpsGuru stellt eine Liste der Ressourcennamen und ihrer Anwendungsgrenzen bereit, die derzeit mithilfe der `ListMonitoredResources` Aktion analysiert werden. Diese Informationen werden von Amazon und anderen AWS Diensten gesammelt CloudWatch AWS CloudTrail, die die mit dem DevOps Guru-Dienst verknüpfte Rolle verwenden.

Beachten Sie, dass DevOps Guru auch dann, wenn ein Benutzer keine ausdrückliche Zugriffsberechtigung APIs für einen anderen Dienst wie AWS Lambda Amazon RDS hat, eine Liste der Ressourcen dieses Dienstes bereitstellt, solange die `ListMonitoredResources` Aktion zulässig ist.

Themen

- Aktualisierung der Berichterstattung über Ihre AWS Analysen in DevOps Guru
- Die Ansicht „Analysierte Ressourcen“ wird für Benutzer entfernt

Aktualisierung der Berichterstattung über Ihre AWS Analysen in DevOps Guru

Sie können aktualisieren, welche AWS Ressourcen in Ihrem Konto DevOps Guru analysiert. Die analysierten Ressourcen bilden die Deckungsgrenze Ihres DevOps Guru. Wenn Sie Ihre Grenze angeben, werden Ihre Ressourcen in Anwendungen gruppiert. Sie haben vier Optionen für die Grenzabdeckung.

- Entscheiden Sie sich dafür, dass DevOps Guru alle unterstützten Ressourcen in Ihrem Konto analysiert. Alle Ressourcen in Ihrem Konto, die sich in einem Stapel befinden, sind in einer Anwendung gruppiert. Wenn Sie mehrere Stapel in Ihrem Konto haben, bilden die Ressourcen in jedem Stapel eine eigene Anwendung. Wenn sich Ressourcen in Ihrem Konto nicht in einem Stapel befinden, werden sie in einer eigenen Anwendung gruppiert.
- Geben Sie Ressourcen an, indem Sie AWS CloudFormation Stacks auswählen, die diese Ressourcen definieren. Wenn Sie dies tun, analysiert DevOps Guru jede Ressource, die in den von Ihnen ausgewählten Stacks angegeben ist. Wenn eine Ressource in Ihrem Konto nicht durch einen von Ihnen ausgewählten Stapel definiert ist, wird sie nicht analysiert. Weitere Informationen finden Sie unter Arbeiten mit Stacks im CloudFormation Benutzerhandbuch und Ermitteln Sie den Versicherungsschutz für DevOps Guru.

- Geben Sie Ressourcen mithilfe von AWS Tags an. DevOpsGuru analysiert entweder alle Ressourcen in Ihrem Konto und Ihrer Region oder alle Ressourcen, die den von Ihnen ausgewählten Tag-Schlüssel enthalten. Ressourcen werden auf der Grundlage ausgewählter Tag-Werte gruppiert. Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.
- Geben Sie an, dass keine Ressourcen analysiert werden sollen, damit Ihnen keine Kosten durch die Ressourcenanalyse entstehen.

> **Note**
>
> Wenn Sie Ihren Versicherungsschutz so aktualisieren, dass keine Ressourcen mehr analysiert werden, fallen möglicherweise weiterhin geringfügige Gebühren an, wenn Sie die vorhandenen Erkenntnisse überprüfen, die DevOps Guru in der Vergangenheit generiert hat. Diese Gebühren stehen im Zusammenhang mit API-Aufrufen, die zum Abrufen und Anzeigen von Insight-Informationen verwendet werden. Weitere Informationen finden Sie unter Amazon DevOps Guru-Preise.

DevOpsGuru unterstützt alle Ressourcen, die mit unterstützten Diensten verknüpft sind. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

Um den Umfang Ihrer DevOps Guru-Analyse zu verwalten

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Erweitern Sie Analysierte Ressourcen im Navigationsbereich.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Wählen Sie eine der folgenden Deckungsoptionen.

    - Wähle Alle Kontoressourcen, wenn DevOps Guru alle unterstützten Ressourcen in deinem AWS Konto und deiner Region analysieren soll. Wenn du diese Option wählst, ist dein AWS Konto die Deckungsgrenze deiner Ressourcenanalyse. Alle Ressourcen in jedem Stapel in Ihrem Konto sind in einer eigenen Anwendung gruppiert. Alle verbleibenden Ressourcen, die sich nicht in einem Stapel befinden, werden in einer eigenen Anwendung gruppiert.
    - Wähle CloudFormation Stacks, wenn DevOps Guru die Ressourcen analysieren soll, die sich in Stacks deiner Wahl befinden, und wähle dann eine der folgenden Optionen.

- Alle Ressourcen — Alle Ressourcen, die sich in deinem Konto in Stapeln befinden, werden analysiert. Die Ressourcen in jedem Stapel sind in einer eigenen Anwendung gruppiert. Alle Ressourcen in Ihrem Konto, die sich nicht in einem Stapel befinden, werden nicht analysiert.
- Stapel auswählen — Wählen Sie die Stapel aus, die DevOps Guru analysieren soll. Die Ressourcen in jedem Stapel, den Sie auswählen, sind in einer eigenen Anwendung gruppiert. Sie können den Namen eines Stacks in Find Stacks eingeben, um schnell einen bestimmten Stack zu finden. Sie können bis zu 1.000 Stapel auswählen.

Weitere Informationen finden Sie unter Verwenden von CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

- Wähle „Tags“, wenn DevOps Guru alle Ressourcen analysieren soll, die die von dir ausgewählten Tags enthalten. Wähle einen Schlüssel und dann eine der folgenden Optionen.
  - Alle Kontoressourcen — Analysieren Sie alle AWS-Ressourcen in der aktuellen Region und im aktuellen Konto. Ressourcen mit dem ausgewählten Tag-Schlüssel werden nach Tag-Werten gruppiert, sofern vorhanden. Ressourcen ohne diesen Tag-Schlüssel werden gruppiert und separat analysiert.
  - Wählen Sie bestimmte Tag-Werte — Alle Ressourcen, die ein Tag mit dem von Ihnen ausgewählten Schlüssel enthalten, werden analysiert. DevOpsGuru gruppiert Ihre Ressourcen nach den Werten Ihres Tags in Anwendungen.

  Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren.
- Wählen Sie Keine, wenn DevOps Guru keine Ressourcen analysieren soll. Diese Option deaktiviert DevOps Guru, sodass Ihnen keine Gebühren mehr durch die Ressourcenanalyse entstehen.

5. Wählen Sie Save (Speichern) aus.

Die Ansicht „Analysierte Ressourcen“ wird für Benutzer entfernt

Selbst wenn ein Benutzer keine ausdrückliche Zugriffsberechtigung APIs für einen anderen Dienst wie Lambda oder Amazon RDS hat, stellt DevOps Guru dennoch eine Liste der Ressourcen dieses Dienstes bereit, solange die `ListMonitoredResources` Aktion zulässig ist. Um dieses Verhalten zu ändern, können Sie Ihre AWS IAM-Richtlinie aktualisieren, um diese Aktion abzulehnen.

```
{
            "Sid": "DenyListMonitoredResources",
```

```
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

Bewährte Methoden in DevOps Guru

Die folgenden bewährten Methoden können Ihnen helfen, das von Amazon DevOps Guru festgestellte anomale Verhalten zu verstehen, zu diagnostizieren und zu beheben. Wenden Sie bewährte Methoden Einblicke in der DevOps Guru-Konsole verstehen an, um von Guru festgestellte Betriebsprobleme zu beheben. DevOps

- Sehen Sie sich in der Zeitleistenansicht eines Insights zunächst die hervorgehobenen Kennzahlen an. Sie sind häufig Schlüsselindikatoren für das Problem.
- Verwenden Sie Amazon CloudWatch , um Metriken anzuzeigen, die unmittelbar vor der ersten hervorgehobenen Metrik aufgetreten sind, sodass Sie feststellen können, wann und wie sich das Verhalten geändert hat. Dies kann Ihnen helfen, das Problem zu diagnostizieren und zu beheben.
- Informationen zu Amazon RDS-Ressourcen finden Sie unter Performance Insights Insights-Metriken. Indem Sie Leistungsindikatoren mit der Datenbanklast korrelieren, erhalten Sie detaillierte Informationen zu Leistungsproblemen. Weitere Informationen finden Sie unter Analysieren von Leistungsanomalien mit DevOps Guru für Amazon RDS.
- Mehrere Dimensionen derselben Metrik können oft anomal sein. Sehen Sie sich die Dimensionen in der grafischen Ansicht an, um ein tieferes Verständnis des Problems zu erhalten.
- Suchen Sie im Abschnitt „Ereignisse“ von Insight nach Bereitstellungs- oder Infrastrukturereignissen, die ungefähr zu dem Zeitpunkt eingetreten sind, zu dem die Informationen erstellt wurden. Wenn Sie wissen, welche Ereignisse eingetreten sind, als das ungewöhnliche Verhalten eines Insights eingetreten ist, können Sie das Problem besser verstehen und diagnostizieren.
- Suchen Sie in Ihrem Betriebssystem nach Tickets, die ungefähr zur gleichen Zeit aufgetreten sind, und suchen Sie nach Hinweisen.
- Um einen Einblick zu erhalten, lesen Sie die Empfehlungen und besuchen Sie die Links in den Empfehlungen. Diese enthalten häufig Schritte zur Fehlerbehebung, die Ihnen helfen können, Probleme schnell zu diagnostizieren und zu lösen.
- Ignorieren Sie gelöste Erkenntnisse nicht, es sei denn, Sie haben das Problem bereits gelöst. Schauen Sie sich einmal am Tag neue Erkenntnisse an, auch wenn sie gelöst wurden. Versuchen Sie, die Grundursache hinter so vielen Erkenntnissen wie möglich zu verstehen. Suchen Sie nach einem Muster, das auf ein systemisches Problem hindeuten könnte. Wenn ein systemisches Problem ungelöst bleibt, könnte es in future zu ernsteren Problemen führen. Die sofortige Behebung vorübergehender Probleme kann dazu beitragen, future, schwerwiegendere Vorfälle zu verhindern.

Sicherheit bei Amazon DevOps Guru

Cloud-Sicherheit bei AWS hat höchste Priorität. Als AWS Als Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die so konzipiert sind, dass sie die Anforderungen der sicherheitsrelevantesten Organisationen erfüllen.

Sicherheit ist eine gemeinsame Verantwortung zwischen AWS und du. 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 laufenden Infrastruktur AWS Dienste in der AWS Wolke. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Auditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheit im Rahmen der AWS Compliance-Programme. Um mehr über die Compliance-Programme zu erfahren, die für Amazon gelten DevOps Guru, sieh AWS-Services im Umfang nach Compliance-Programm.
- Sicherheit in der Cloud — Ihre Verantwortung wird bestimmt durch 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 anwenden können, wenn Sie DevOps Guru. Die folgenden Themen zeigen dir, wie du es konfigurierst DevOps Guru, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere AWS-Services nutzen können, die Sie bei der Überwachung und Sicherung Ihrer DevOps Guru-Ressourcen.

Topics

- Datenschutz bei Amazon DevOps Guru
- Identitäts- und Zugriffsmanagement für Amazon DevOps Guru
- Protokollierung und Überwachung DevOps Guru
- DevOps Guru- und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)
- Sicherheit der Infrastruktur in DevOps Guru
- Widerstandsfähigkeit bei Amazon DevOps Guru

Datenschutz bei Amazon DevOps Guru

Der AWS Modell der gemeinsamen Verantwortung gilt für den Datenschutz bei Amazon DevOps Guru. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle 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 DatenschutzRechtliche. Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir Ihnen, Folgendes zu schützen AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center oder AWS Identity and Access Management (ICH BIN). 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).
- Benutzen SSL/TLS um zu kommunizieren mit AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten ein mit AWS CloudTrail. Für Informationen zur Verwendung CloudTrail Spuren zum Erfassen AWS Aktivitäten, siehe Arbeiten mit CloudTrail Wanderwege in der AWS CloudTrail Benutzerleitfaden.
- Benutzen AWS Verschlüsselungslösungen sowie alle darin enthaltenen Standard-Sicherheitskontrollen 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 beim Zugriff auf FIPS 140-3-validierte kryptografische Module benötigen AWS Verwenden Sie über eine Befehlszeilenschnittstelle oder eine API 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 arbeiten DevOps Guru oder anderes AWS-Services mithilfe der Konsole, API, AWS CLI, oder 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.

Datenverschlüsselung in DevOps Guru

Verschlüsselung ist ein wichtiger Bestandteil von DevOps Guru Sicherheit. Ein Teil der Verschlüsselung, z. B. für Daten bei der Übertragung, ist standardmäßig vorgesehen, sodass Sie nichts tun müssen. Andere Verschlüsselungen, z. B. für Daten im Ruhezustand, können Sie konfigurieren, wenn Sie Ihr Projekt oder Ihren Build erstellen.

- Verschlüsselung von Daten bei der Übertragung: Die gesamte Kommunikation zwischen Kunden und DevOps Guru und dazwischen DevOps Guru und seine nachgelagerten Abhängigkeiten sind mit TLS geschützt und mit dem Signature Version 4-Signaturprozess authentifiziert. Alles DevOps Guru-Endpunkte verwenden Zertifikate, die von verwaltet werden AWS Private Certificate Authority. Weitere Informationen finden Sie unter Signaturprozess mit Signaturversion 4 und Was ist ACM PCA?.
- Verschlüsselung von Daten im Ruhezustand: Für alle AWS Ressourcen analysiert von DevOps Guru, der Amazonas CloudWatch Metriken und Daten, Ressourcen-IDs und AWS CloudTrail Ereignisse werden mit Amazon S3, Amazon DynamoDB und Amazon Kinesis gespeichert. Wenn CloudFormation Stapel werden verwendet, um die analysierten Ressourcen zu definieren, dann werden auch Stack-Daten gesammelt. DevOps Guru verwendet die Datenaufbewahrungsrichtlinien von Amazon S3, DynamoDB und Kinesis. In Kinesis gespeicherte Daten können bis zu einem Jahr aufbewahrt werden und hängen von den festgelegten Richtlinien ab. In Amazon S3 und DynamoDB gespeicherte Daten werden ein Jahr lang gespeichert.

  Gespeicherte Daten werden mithilfe der Verschlüsselungsfunktionen von Amazon S3, DynamoDB und Kinesis verschlüsselt.

  Vom Kunden verwaltete Schlüssel: DevOps Guru unterstützt die Verschlüsselung von Kundeninhalten und sensiblen Metadaten wie Protokollanomalien, die generiert wurden von CloudWatch Protokolle mit vom Kunden verwalteten Schlüsseln. Diese Funktion bietet Ihnen die Möglichkeit, eine selbstverwaltete Sicherheitsebene hinzuzufügen, mit der Sie die Compliance- und regulatorischen Anforderungen Ihres Unternehmens erfüllen können. Informationen zur Aktivierung von kundenverwalteten Schlüsseln in Ihrem DevOps Guru-Einstellungen, siehe the section called “Die Verschlüsselung wird aktualisiert”.

Da Sie die volle Kontrolle über diese Verschlüsselungsebene haben, können Sie beispielsweise folgende Aufgaben ausführen:

- Festlegung und Pflege wichtiger Richtlinien
- Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
- Aktivieren und Deaktivieren wichtiger Richtlinien
- Kryptographisches Material mit rotierendem Schlüssel
- Hinzufügen von -Tags
- Erstellen von Schlüsselaliasen
- Schlüssel für das Löschen von Schlüsseln planen

Weitere Informationen finden Sie unter Vom Kunden verwaltete Schlüssel in der AWS Key Management Service Leitfaden für Entwickler.

> **Note**
>
> DevOps Guru aktiviert automatisch die Verschlüsselung im Ruhezustand mit AWS eigene Schlüssel zum kostenlosen Schutz sensibler Metadaten. Jedoch AWS KMS Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie auf der AWS Key Management Service Preisgestaltung.

Wie DevOps Guru verwendet Zuschüsse in AWS KMS

DevOps Guru benötigt einen Zuschuss, um deinen vom Kunden verwalteten Schlüssel verwenden zu können.

Wenn du dich dafür entscheidest, die Verschlüsselung mit einem vom Kunden verwalteten Schlüssel zu aktivieren, DevOps Guru gewährt in deinem Namen einen Zuschuss, indem er eine CreateGrant Anfrage an AWS KMS. Zuschüsse in AWS KMS werden verwendet, um zu geben DevOps Guru-Zugang zu einem AWS KMS geben Sie ein Kundenkonto ein.

DevOps Guru benötigt den Zuschuss, um deinen vom Kunden verwalteten Schlüssel für die folgenden internen Abläufe verwenden zu können:

- Senden DescribeKey Anfragen an AWS KMS um zu überprüfen, ob die symmetrische, vom Kunden verwaltete KMS-Schlüssel-ID, die beim Erstellen einer Tracker- oder Geofence-Sammlung eingegeben wurde, gültig ist.
- Senden GenerateDataKey Anfragen an AWS KMS um Datenschlüssel zu generieren, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden.
- Senden Sie Entschlüsselungsanfragen an AWS KMS um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zum Verschlüsseln Ihrer Daten verwendet werden können.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn du das tust, DevOps Guru kann auf keine der Daten zugreifen, die mit dem vom Kunden verwalteten Schlüssel verschlüsselt wurden, was sich auf Abläufe auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, verschlüsselte Log-Anomalie-Informationen abzurufen, die DevOps Guru kann nicht zugreifen, dann würde die Operation einen zurückgeben AccessDeniedException Fehler.

Überwachung Ihrer Verschlüsselungsschlüssel in DevOps Guru

Wenn du einen benutzt AWS KMS vom Kunden verwalteter Schlüssel mit Ihrem DevOps Guru-Ressourcen, die du verwenden kannst AWS CloudTrail oder CloudWatch Protokolle zur Nachverfolgung von Anfragen, die DevOps Guru sendet an AWS KMS.

Erstellen eines kundenseitig verwalteten Schlüssels

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem Sie den AWS-Managementkonsole oder der AWS KMS APIs.

Informationen zum Erstellen eines symmetrischen, vom Kunden verwalteten Schlüssels finden Sie unter KMS-Schlüssel für symmetrische Verschlüsselung erstellen.

Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren kundenseitig verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Authentifizierung und Zugriffskontrolle für AWS KMS in der AWS Key Management Service Leitfaden für Entwickler.

Um Ihren vom Kunden verwalteten Schlüssel mit Ihrem zu verwenden DevOps Guru-Ressourcen, die folgenden API-Operationen müssen in der Schlüsselrichtlinie erlaubt sein:

- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf eine bestimmte AWS KMS Schlüssel, der den Zugriff auf Grant-Operationen ermöglicht DevOps Guru benötigt. Weitere Informationen zur Verwendung von Zuschüssen finden Sie in der AWS Key Management Service Leitfaden für Entwickler.

Das ermöglicht DevOps Guru, um Folgendes zu tun:

- Ruf an GenerateDataKey um einen verschlüsselten Datenschlüssel zu generieren und zu speichern, da der Datenschlüssel nicht sofort zum Verschlüsseln verwendet wird.
- Rufen Sie Decrypt auf, um den gespeicherten verschlüsselten Datenschlüssel für den Zugriff auf verschlüsselte Daten zu verwenden.
- Einen Prinzipal für die Außerbetriebnahme einrichten, damit der Service in den Status RetireGrant wechseln kann.
- Verwenden Sie kms:DescribeKey um dem Kunden die wichtigsten Daten zur Verfügung zu stellen, um dies zu ermöglichen DevOps Guru, um den Schlüssel zu validieren.

Die folgende Anweisung enthält Beispiele für Richtlinienerklärungen, die Sie hinzufügen können DevOps Guru:

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

Datenschutz für Datenverkehr

Sie können die Sicherheit Ihrer Ressourcenanalyse und der Generierung von Erkenntnissen verbessern, indem Sie Folgendes konfigurieren DevOps Guru, um einen Schnittstellen-VPC-Endpunkt zu verwenden. Dafür benötigen Sie kein Internet-Gateway, kein NAT-Gerät und kein virtuelles privates Gateway. Es ist auch nicht erforderlich, es zu konfigurieren PrivateLink, obwohl es empfohlen wird. Weitere Informationen finden Sie unter DevOps Guru- und Schnittstellen-VPC-Endpunkte (AWS PrivateLink). Für weitere Informationen über PrivateLink und VPC-Endpunkte finden Sie unter AWS PrivateLink und Zugriff auf AWS-Services über PrivateLink.

Identitäts- und Zugriffsmanagement für Amazon DevOps Guru

AWS Identity and Access Management (IAM) ist ein AWS-Service das hilft einem Administrator, den Zugriff auf sicher zu kontrollieren AWS Ressourcen. IAM-Administratoren kontrollieren, wer sein kann authentifiziert (angemeldet) und autorisiert (über Berechtigungen verfügen) zur Nutzung DevOps Guru-Ressourcen. IAM ist ein AWS-Service die Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- DevOps Guru aktualisiert für AWS verwaltete Richtlinien und dienstbezogene Rolle
- Wie Amazon DevOps Guru arbeitet mit IAM
- Identity-based Richtlinien für Amazon DevOps Guru
- Verwenden von dienstverknüpften Rollen für DevOps Guru
- Amazonas DevOps Referenz zu Guru-Berechtigungen
- Berechtigungen für Amazon SNS-Themen
- Berechtigungen für AWS KMS— verschlüsselte Amazon SNS-Themen
- Fehlerbehebung bei Amazon DevOps Guru-Identität und Zugang

Zielgruppe

Wie benutzt du AWS Identity and Access Management (IAM) unterscheidet sich je nach Ihrer Rolle:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Amazon DevOps Guru-Identität und Zugang).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe Wie Amazon DevOps Guru arbeitet mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinien für Amazon DevOps Guru).

Authentifizierung mit Identitäten

Bei der Authentifizierung melden Sie sich an AWS mit Ihren Identitätsdaten. Sie müssen authentifiziert sein als Root-Benutzer des AWS-Kontos, ein IAM-Benutzer oder indem Sie eine IAM-Rolle übernehmen.

Sie können sich als Verbundidentität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single-Sign-On-Authentifizierung

oder Google/Facebook Anmeldeinformationen. Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

Für den programmatischen Zugriff AWS bietet 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 eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität namens AWS-Konto Root-Benutzer das hat vollen Zugriff auf alle AWS-Services und Ressourcen. 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, menschliche Benutzer dazu zu verpflichten, einen Verbund mit einem Identitätsanbieter für den Zugriff zu verwenden AWS-Services Verwendung temporärer Anmeldeinformationen.

EIN föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Web Identity Provider oder Directory Service das zugreift AWS-Services unter Verwendung von Anmeldeinformationen aus einer Identitätsquelle. 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 unter Erfordern Sie, dass menschliche Benutzer einen Verbund mit einem Identitätsanbieter für den Zugriff verwenden AWS Verwendung temporärer Anmeldeinformationen in der IAM-Benutzerhandbuch.

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 wechseln (Konsole) oder indem Sie einen anrufen AWS CLI oder AWS API-Betrieb. 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 in AWS indem Sie Richtlinien erstellen und sie anhängen AWS Identitäten oder Ressourcen. Eine Richtlinie definiert Berechtigungen, wenn sie einer Identität oder Ressource zugeordnet sind. AWS wertet diese Richtlinien aus, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien sind gespeichert in AWS als JSON-Dokumente. 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.

Identity-based Politik

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. 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.

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

Resource-based Politik

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. 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.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können nicht verwenden AWS verwaltete Richtlinien von IAM in einer ressourcenbasierten Richtlinie.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximale Anzahl von Berechtigungen festgelegt werden kann, 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.
- Service-Kontrollrichtlinien (SCPs) – SCPs legen die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in AWS Organizations fest. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Ressourcen-Kontrollrichtlinien (RCPs) – RCPs definieren die maximale Anzahl an Berechtigungen, die Ressourcen in Ihren Konten zur Verfügung stehen. Weitere Informationen finden Sie unter Ressourcen-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- 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 mehrere Arten von Richtlinien für eine Anfrage gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Um zu erfahren, wie AWS bestimmt, ob eine Anfrage

zulässig ist, wenn mehrere Richtlinientypen betroffen sind, siehe Logik der Bewertung von Richtlinien in der IAM-Benutzerhandbuch.

DevOps Guru aktualisiert für AWS verwaltete Richtlinien und dienstbezogene Rolle

Sehen Sie sich Details zu Updates an AWS verwaltete Richtlinien und dienstbezogene Rolle für DevOps Guru, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Für automatische Benachrichtigungen über Änderungen an dieser Seite abonnieren Sie den RSS-Feed auf der DevOps Guru Amazon DevOps Guru-Dokumentenhistorie.

Änderungen	Beschreibung	Date
AmazonDevOpsGuruConsoleFullAccess – Aktualisierung auf eine bestehende Richtlinie.	Das `AmazonDevOpsGuruFullAccess` Die verwaltete Richtlinie unterstützt jetzt Amazon SNS-Abonnements.	9. August 2023
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` Die verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf Amazon SNS-Abonnementlisten.	9. August 2023
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die service-verknüpfte Rolle unterstützt jetzt den Zugriff auf API Gateway GET-Aktionen auf REST-APIs.	11. Januar 2023
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die serviceverknüpfte Rolle unterstützt jetzt mehrere Amazon Simple	19. Oktober 2022

Änderungen	Beschreibung	Date
	Storage Service- und Service Quota-Aktionen.	
AmazonDevOpsGuruFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die von `AmazonDevOpsGuruFullAccess` verwaltete Richtlinie unterstützt jetzt den Zugriff auf CloudWatch `FilterLogEvents` Aktion.	30. August 2022
AmazonDevOpsGuruConsoleFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruConsoleFullAccess` Die verwaltete Richtlinie unterstützt jetzt den Zugriff auf CloudWatch `FilterLogEvents` Aktion.	30. August 2022
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` Die verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf CloudWatch `FilterLogEvents` Aktion.	30. August 2022
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die service-verknüpfte Rolle unterstützt jetzt CloudWatch protokolliert Aktionen `FilterLogEvents` , `DescribeLogGroups` , und `DescribeLogStreams` .	12. Juli 2022

Änderungen	Beschreibung	Date
Identity-based Richtlinien für DevOps Guru — Neue verwaltete Richtlinie.	• Das `AmazonDevOpsGuruConsoleFullAccess` Richtlinie wurde hinzugefügt.	16. Dezember 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die serviceverknüpfte Rolle unterstützt jetzt Performance Insights `DescribeMetricsKeys` und Amazon RDS `DescribeDBInstances` Aktionen.	1. Dezember 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` Die verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf Amazon RDS `DescribeDBInstances` Aktionen.	1. Dezember 2021
AmazonDevOpsGuruFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruFullAccess` Die verwaltete Richtlinie unterstützt jetzt den Zugriff auf Amazon RDS `DescribeDBInstances` Aktionen.	1. Dezember 2021

Änderungen	Beschreibung	Date
Identity-based Richtlinien für Amazon DevOps Guru — Neue Richtlinie hinzugefügt.	— Das `AWSServiceRoleForDevOpsGuru` Die serviceverknüpfte Rolle unterstützt jetzt den Zugriff auf Amazon RDS `DescribeDBInstances` und Performance Insights `GetResourceMetrics` Aktionen. Die `AmazonDevOpsGuruOrganizationsAccess` Die verwaltete Richtlinie bietet Zugriff auf DevOps Guru innerhalb einer Organisation.	16. November 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Der `AWSServiceRoleForDevOpsGuru` Die serviceverknüpfte Rolle unterstützt jetzt AWS-Organisationen.	4. November 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die service-verknüpfte Rolle enthält jetzt neue Bedingungen für `ssm:CreateOpsItem` und `ssm:AddTagsToResource` Aktionen.	11. Oktober 2021

Änderungen	Beschreibung	Date
Service-linked Rollenberechtigungen für DevOps Guru – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die service-verknüpfte Rolle enthält jetzt neue Bedingungen für `ssm:CreateOpsItem` und `ssm:AddTagsToResource` Aktionen.	14. Juni 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` Die verwaltete Richtlinie ermöglicht jetzt den schreibgeschützten Zugriff auf AWS Identity and Access Management `GetRole` und der DevOps Guru `DescribeFeedback` Aktionen.	14. Juni 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` Die verwaltete Richtlinie ermöglicht jetzt den schreibgeschützten Zugriff auf DevOps Guru `GetCostEstimation` und `StartCostEstimation` Aktionen.	27. April 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Die Rolle ermöglicht jetzt den Zugriff auf AWS Systems Manager `AddTagsToResource` und Amazon EC2 Auto Scaling `DescribeAutoScalingGroups` Aktionen.	27. April 2021

Änderungen	Beschreibung	Date
DevOps Guru fing an, Änderungen zu verfolgen	DevOps Guru begann, Änderungen für seine zu verfolgen AWS verwaltete Richtlinien.	10. Dezember 2020

Wie Amazon DevOps Guru arbeitet mit IAM

Bevor Sie IAM verwenden, um den Zugriff zu verwalten DevOps Guru, lerne, mit welchen IAM-Funktionen du verwenden kannst DevOps Guru.

IAM-Funktionen, die Sie mit Amazon verwenden können DevOps Guru

IAM-Feature	DevOps Guru-Unterstützung
Identity-based Politik	Ja
Resource-based Politik	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Service-linked Rollen	Ja

Um einen allgemeinen Überblick darüber zu erhalten, wie DevOps Guru und andere AWS Dienste funktionieren mit den meisten IAM-Funktionen, siehe AWS Dienste, die mit IAM funktionieren in der IAM-Benutzerhandbuch.

Identity-based Richtlinien für DevOps Guru

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. 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.

Identity-based Richtlinienbeispiele für DevOps Guru

Um Beispiele zu sehen von DevOps Identitätsbasierte Guru-Richtlinien, siehe Identity-based Richtlinien für Amazon DevOps Guru.

Resource-based Richtlinien innerhalb DevOps Guru

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. 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. Principals können Konten, Benutzer, Rollen, Verbundbenutzer oder 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.

Politische Maßnahmen für DevOps Guru

Unterstützt Richtlinienaktionen: Ja

Administratoren können verwenden AWS JSON-Richtlinien, um festzulegen, wer Zugriff auf was 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 gewähren.

Um eine Liste von zu sehen DevOps Guru-Aktionen, siehe Von Amazon definierte Aktionen DevOps Guru in der Referenz zur Serviceautorisierung.

Politische Maßnahmen in DevOps Guru benutzt vor der Aktion das folgende Präfix:

```
aws
```

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

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

Um Beispiele zu sehen für DevOps Identitätsbasierte Guru-Richtlinien, siehe Identity-based Richtlinien für Amazon DevOps Guru.

Politische Ressourcen für DevOps Guru

Unterstützt Richtlinienressourcen: Ja

Administratoren können verwenden AWS JSON-Richtlinien, um festzulegen, wer Zugriff auf was 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": "*"
```

Um eine Liste von zu sehen DevOps Guru-Ressourcentypen und ihre ARNs, siehe Von Amazon definierte Ressourcen DevOps Guru in der Referenz zur Serviceautorisierung. Informationen zu den Aktionen, mit denen Sie den ARN der einzelnen Ressourcen angeben können, finden Sie unter Von Amazon definierte Aktionen DevOps Guru.

Um Beispiele zu sehen von DevOps Identitätsbasierte Guru-Richtlinien, siehe Identity-based Richtlinien für Amazon DevOps Guru.

Schlüssel zu den Bedingungen der Richtlinie für DevOps Guru

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können verwenden AWS JSON-Richtlinien, um festzulegen, wer Zugriff auf was 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. Um alles zu sehen AWS globale Bedingungsschlüssel finden Sie unter AWS globale Bedingungskontextschlüssel in der IAM-Benutzerhandbuch.

Um eine Liste von zu sehen DevOps Guru-Zustandstasten, siehe Bedingungsschlüssel für Amazon DevOps Guru in der Referenz zur Serviceautorisierung. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon definierte Aktionen DevOps Guru.

Um Beispiele zu sehen von DevOps Identitätsbasierte Guru-Richtlinien, siehe Identity-based Richtlinien für Amazon DevOps Guru.

Zugriffskontrolllisten (ACLs) in DevOps Guru

Unterstützt ACLs: Nein

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

Attribute-based Zugangskontrolle (ABAC) mit DevOps Guru

Unterstützt ABAC (Tags in Richtlinien): Nein

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können IAM-Entitäten Tags anhängen und AWS Ressourcen und entwerfen Sie dann ABAC-Richtlinien, um Operationen zu ermöglichen, wenn das Tag des Principals 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 Sie temporäre Anmeldeinformationen mit DevOps Guru

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen bieten 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.

Cross-service Hauptberechtigungen für DevOps Guru

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Rechte des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung AWS-Service um Anfragen an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für DevOps Guru

Unterstützt Servicerollen: Nein

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**
>
> Das Ändern der Berechtigungen für eine Servicerolle könnte zu Problemen führen DevOps Guru-Funktionalität. Bearbeiten Sie Servicerollen nur, wenn DevOps Der Guru gibt dazu eine Anleitung.

Service-linked Rollen für DevOps Guru

Unterstützt serviceverknüpfte Rollen: Ja

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

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Dienst, der einen enthält `Yes` in der Service-linked Rolle Spalte. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Identity-based Richtlinien für Amazon DevOps Guru

Standardmäßig haben Benutzer und Rollen keine Berechtigung zum Erstellen oder Ändern DevOps Guru-Ressourcen. 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.

Für Details zu Aktionen und Ressourcentypen, definiert von DevOps Guru, einschließlich des Formats der ARNs für jeden der Ressourcentypen, siehe Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DevOps Guru in der Referenz zur Serviceautorisierung.

Themen

- Best Practices für Richtlinien
- Mit dem DevOps Guru-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Von AWS verwaltete (vordefinierte) Richtlinien für DevOps Guru

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand etwas erstellen, darauf zugreifen oder löschen kann DevOps Guru-Ressourcen in deinem Konto. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn du identitätsbasierte Richtlinien erstellst oder bearbeitest, befolge diese Richtlinien und Empfehlungen:

- Beginnen Sie mit AWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit geringsten Rechten — Um mit der Vergabe von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, verwenden Sie AWS verwaltete Richtlinien die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen, die Berechtigungen weiter zu reduzieren, indem Sie Folgendes definieren AWS vom Kunden verwaltete Richtlinien, 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 im Rahmen einer bestimmten Aktion genutzt werden AWS-Service, wie CloudFormation. 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.
- Mehrstufige Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem AWS-Konto, schalten Sie MFA für zusätzliche Sicherheit ein. 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.

Mit dem DevOps Guru-Konsole

Um auf den Amazonas zuzugreifen DevOps Guru-Konsole, Sie müssen über ein Minimum an Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den DevOps Guru-Ressourcen in deinem 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 Anrufe tätigen, keine Mindestberechtigungen für die Konsole gewähren AWS CLI oder der AWS API. 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 weiterhin die verwenden können DevOps Guru-Konsole, befestige auch die DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` oder `AmazonDevOpsGuruFullAccess` AWS verwaltete Richtlinie gegenüber den Unternehmen. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

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 beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Von AWS verwaltete (vordefinierte) Richtlinien für DevOps Guru

AWS adressiert viele gängige Anwendungsfälle, indem es eigenständige IAM-Richtlinien bereitstellt, die von erstellt und verwaltet werden AWS. Diese AWS-verwaltete Richtlinien gewähren die erforderlichen Berechtigungen für häufige Anwendungsfälle, sodass Sie nicht erst untersuchen müssen, welche Berechtigungen benötigt werden. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien im IAM Benutzerhandbuch.

Um sie zu erstellen und zu verwalten DevOps Guru-Servicerollen, du musst auch die beifügen AWS-verwaltete Richtlinie mit dem Namen `IAMFullAccess`.

Sie können auch Ihre eigenen benutzerdefinierten IAM-Richtlinien erstellen, um Berechtigungen für zu gewähren DevOps Guru-Aktionen und Ressourcen. Die benutzerdefinierten Richtlinien können Sie dann den -Benutzern oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

Folgendes AWS-verwaltete Richtlinien, die Sie Benutzern in Ihrem Konto zuordnen können, sind spezifisch für DevOps Guru.

Themen

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess` — Bietet vollen Zugriff auf DevOps Guru, einschließlich der Berechtigungen zum Erstellen von Amazon SNS-Themen, greifen auf Amazon zu CloudWatch Metriken und Zugriff AWS CloudFormation Stapel. Wenden Sie dies nur auf Benutzer mit Administratorrechten an, über die Sie die volle Kontrolle gewähren möchten DevOps Guru.

Der `AmazonDevOpsGuruFullAccess` Die Richtlinie enthält die folgende Aussage.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
```

```
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
```

```
                "logs:FilterLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DevOps-Guru-Analysis": "true"
                }
            }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess` — Bietet vollen Zugriff auf DevOps Guru, einschließlich der Berechtigungen zum Erstellen von Amazon SNS-Themen, greifen auf Amazon zu CloudWatch Metriken und Zugriff AWS CloudFormation Stapel. Diese Richtlinie verfügt über zusätzliche Performance-Insights-Berechtigungen, sodass Sie detaillierte Analysen zu anomalen Amazon RDS Aurora-DB-Instances in der Konsole einsehen können. Wenden Sie dies nur auf Benutzer mit Administratorrechten an, über die Sie die volle Kontrolle gewähren möchten DevOps Guru.

Der `AmazonDevOpsGuruConsoleFullAccess` Die Richtlinie enthält die folgende Aussage.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
```

```
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess` — Gewährt schreibgeschützten Zugriff auf DevOps Guru und verwandte Ressourcen in anderen AWS Dienstleistungen. Wenden Sie diese Richtlinie auf Benutzer an, denen Sie die Möglichkeit gewähren möchten, Einblicke einzusehen, aber keine Aktualisierungen an DevOps Gurus Analyseabdeckungsgrenze, Amazon SNS-Themen oder Systems Manager OpsCenter Integration.

Die `AmazonDevOpsGuruReadOnlyAccess` Die Richtlinie enthält die folgende Aussage.

JSON

```
{
"Version":"2012-10-17",
"Statement": [
    {
        "Sid": "DevOpsGuruReadOnlyAccess",
        "Effect": "Allow",
        "Action": [
            "devops-guru:DescribeAccountHealth",
            "devops-guru:DescribeAccountOverview",
            "devops-guru:DescribeAnomaly",
            "devops-guru:DescribeEventSourcesConfig",
            "devops-guru:DescribeFeedback",
            "devops-guru:DescribeInsight",
            "devops-guru:DescribeResourceCollectionHealth",
            "devops-guru:DescribeServiceIntegration",
            "devops-guru:GetCostEstimation",
            "devops-guru:GetResourceCollection",
            "devops-guru:ListAnomaliesForInsight",
            "devops-guru:ListEvents",
            "devops-guru:ListInsights",
            "devops-guru:ListAnomalousLogGroups",
            "devops-guru:ListMonitoredResources",
            "devops-guru:ListNotificationChannels",
            "devops-guru:ListRecommendations",
            "devops-guru:SearchInsights",
            "devops-guru:StartCostEstimation"
        ],
        "Resource": "*"
    },
```

```
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:FilterLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DevOps-Guru-Analysis": "true"
                }
            }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess` — Ermöglicht Administratoren von Organisationen den Zugriff auf DevOps Guru-Ansicht mit mehreren Konten innerhalb einer Organisation. Wenden Sie diese Richtlinie auf die Benutzer Ihrer Organisation auf Administratorebene an, denen Sie vollen Zugriff gewähren möchten DevOps Guru innerhalb einer Organisation. Du kannst diese Richtlinie auf das Verwaltungskonto deiner Organisation und auf das Konto eines delegierten Administrators anwenden für DevOps Guru. Du kannst dich bewerben `AmazonDevOpsGuruReadOnlyAccess` oder `AmazonDevOpsGuruFullAccess` zusätzlich zu dieser Richtlinie, um nur lesbaren oder vollständigen Zugriff auf DevOps Guru.

Der `AmazonDevOpsGuruOrganizationsAccess` Die Richtlinie enthält die folgende Aussage.

Verwenden von dienstverknüpften Rollen für DevOps Guru

Amazon DevOps Guru benutzt AWS Identity and Access Management (ICH BIN) dienstgebundene Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger IAM-Rollentyp, der direkt mit verknüpft ist DevOps Guru. Service-linked Rollen sind vordefiniert durch DevOps Guru und füge alle Berechtigungen hinzu, die der Dienst benötigt, um anzurufen AWS CloudTrail, Amazon CloudWatch, AWS CodeDeploy, AWS X-Ray, und AWS-Organisationen in Ihrem Namen.

Eine serviceverknüpfte Rolle macht die Einrichtung DevOps Guru ist einfacher, weil Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. DevOps Guru definiert die Berechtigungen seiner dienstverknüpften Rollen, und sofern nicht anders definiert, nur DevOps Guru kann seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauensrichtlinie

und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen juristischen Stelle von IAM zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Das schützt deine DevOps Guru-Ressourcen, weil Sie nicht versehentlich die Erlaubnis zum Zugriff auf die Ressourcen entfernen können.

Service-linked Rollenberechtigungen für DevOps Guru

DevOps Guru verwendet die mit dem Dienst verknüpfte Rolle namens `AWSServiceRoleForDevOpsGuru`. Das ist ein AWS verwaltete Richtlinie mit bereichsspezifischen Berechtigungen, die DevOps Guru muss in deinem Konto laufen.

Die serviceverknüpfte Rolle `AWSServiceRoleForDevOpsGuru` vertraut darauf, dass der folgende Service die Rolle annimmt:

- `devops-guru.amazonaws.com`

Die Richtlinie über Rollenberechtigungen, `AmazonDevOpsGuruServiceRolePolicy` erlaubt DevOps Guru, um die folgenden Aktionen an den angegebenen Ressourcen durchzuführen.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:DescribeAnomalyDetectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListDashboards",
    "cloudwatch:GetDashboard",
    "cloudformation:GetTemplate",
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
    "cloudformation:DescribeStacks",
```

```
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
```

```
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAddTagsToOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:AddTagsToResource"
   ],
   "Resource": "arn:aws:ssm:*:*:opsitem/*"
  },
  {
   "Sid": "AllowAccessOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:GetOpsItem",
    "ssm:UpdateOpsItem"
```

```
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
     }
    }
   },
   {
    "Sid": "AllowCreateManagedRule",
    "Effect": "Allow",
    "Action": "events:PutRule",
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowAccessManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:ListTargetsByRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
   },
   {
    "Sid": "AllowOtherOperationsOnManagedRule",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
    "Condition": {
     "StringEquals": {
      "events:ManagedBy": "devops-guru.amazonaws.com"
     }
    }
   },
   {
    "Sid": "AllowTagBasedFilterLogEvents",
    "Effect": "Allow",
    "Action": [
```

```
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

Erstellen einer dienstverknüpften Rolle für DevOps Guru

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn du einen Einblick in die AWS-Managementkonsole, der AWS CLI, oder der AWS API, DevOps Guru erstellt die dienstbezogene Rolle für dich.

> **Important**
>
> Diese dienstbezogene Rolle kann in deinem Konto erscheinen, wenn du eine Aktion in einem anderen Dienst abgeschlossen hast, der die von dieser Rolle unterstützten Funktionen nutzt; sie kann beispielsweise erscheinen, wenn du sie hinzugefügt hast DevOps Guru zu einem Repositorium von AWS CodeCommit.

Bearbeitung einer dienstverknüpften Rolle für DevOps Guru

DevOps Guru erlaubt dir nicht, das zu bearbeiten `AWSServiceRoleForDevOpsGuru` Rolle, die mit einem Dienst verknüpft ist. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann

der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeitung einer Service-Linked Rolle in der IAM-Benutzerhandbuch.

Löschen einer dienstverknüpften Rolle für DevOps Guru

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Allerdings musst du die Verbindung zu allen Repositorys trennen, bevor du sie manuell löschen kannst.

> **Note**
>
> Wenn der DevOps Guru Service verwendet die Rolle, wenn Sie versuchen, die Ressourcen zu löschen. Das Löschen schlägt möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI, oder die AWS API zum Löschen der `AWSServiceRoleForDevOpsGuru` Mit einem Dienst verknüpfte Rolle. Weitere Informationen finden Sie unter Löschen einer Service-Linked Rolle in der IAM-Benutzerhandbuch.

Amazonas DevOps Referenz zu Guru-Berechtigungen

Sie können verwenden AWS-weite Zustandstasten in Ihrem DevOps Guru-Richtlinien zum Ausdrücken von Bedingungen. Eine Liste finden Sie unter Referenz zu IAM-JSON-Richtlinienelementen in der IAM-Benutzerhandbuch.

Sie geben die Aktionen im Feld `Action` der Richtlinie an. Um eine Aktion anzugeben, verwenden Sie das Präfix `devops-guru:` gefolgt vom Namen der API-Operation (z. B. `devops-guru:SearchInsights` und `devops-guru:ListAnomalies`). Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Komma (z. B. `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

Verwendung von Platzhalterzeichen

Sie geben einen Amazon-Ressourcennamen (ARN) mit oder ohne Platzhalterzeichen (*) als Ressourcenwert in der Richtlinie an `Resource` Feld. Sie können das Platzhalterzeichen verwenden, um mehrere Aktionen oder Ressourcen anzugeben. Zum Beispiel `devops-guru:*` spezifiziert alle DevOps Guru-Aktionen und `devops-guru:List*` spezifiziert alle DevOps Guru-Aktionen, die mit dem Wort beginnen `List`. Das folgende Beispiel bezieht sich auf alle Erkenntnisse mit einem universally unique identifier (UUID), der beginnt mit `12345`.

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

Bei der Einrichtung können Sie die folgende Tabelle als Referenz verwenden Authentifizierung mit Identitäten und Richtlinien für Schreibberechtigungen, die Sie an eine IAM-Identität anhängen können (identitätsbasierte Richtlinien).

DevOps Guru-API-Operationen und erforderliche Berechtigungen für Aktionen

`AddNotificationChannel`

Aktion: `devops-guru:AddNotificationChannel`

Erforderlich, um einen Benachrichtigungskanal hinzuzufügen von DevOps Guru. Ein Benachrichtigungskanal wird verwendet, um Sie zu benachrichtigen, wenn DevOps Guru generiert einen Einblick, der Informationen darüber enthält, wie Sie Ihre Abläufe verbessern können.

Ressource: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Erforderlich, um einen Benachrichtigungskanal von zu entfernen DevOps Guru. Ein Benachrichtigungskanal wird verwendet, um Sie zu benachrichtigen, wenn DevOps Guru generiert einen Einblick, der Informationen darüber enthält, wie Sie Ihre Abläufe verbessern können.

Ressource: *

`ListNotificationChannels`

Aktion: `devops-guru:ListNotificationChannels`

Erforderlich, um eine Liste der Benachrichtigungskanäle zurückzugeben, die für konfiguriert wurden DevOps Guru. Jeder Benachrichtigungskanal wird verwendet, um Sie zu benachrichtigen,

wenn DevOps Guru generiert einen Einblick, der Informationen darüber enthält, wie Sie Ihre Abläufe verbessern können. Der einzige unterstützte Benachrichtigungstyp ist Amazon Simple Notification Service.

Ressource: *

`UpdateResourceCollectionFilter`

Aktion: `devops-guru:UpdateResourceCollectionFilter`

Erforderlich, um die Liste von zu aktualisieren CloudFormation Stapel, mit denen angegeben wird, welche AWS Die Ressourcen in Ihrem Konto werden analysiert von DevOps Guru. Die Analyse generiert Erkenntnisse, die Empfehlungen, Betriebskennzahlen und Betriebsereignisse beinhalten, die Sie zur Verbesserung Ihrer Betriebsleistung nutzen können. Bei dieser Methode werden auch die IAM-Rollen erstellt, die Sie verwenden müssen CodeGuru OpsAdvisor.

Ressource: *

`GetResourceCollectionFilter`

Aktion: `devops-guru:GetResourceCollectionFilter`

Erforderlich, um die Liste von zurückzugeben AWS CloudFormation Stapel, die verwendet werden, um anzugeben, welche AWS Die Ressourcen in Ihrem Konto werden analysiert von DevOps Guru. Die Analyse generiert Erkenntnisse, die Empfehlungen, Betriebskennzahlen und Betriebsereignisse enthalten, die Sie zur Verbesserung Ihrer Betriebsleistung nutzen können.

Ressource: *

`ListInsights`

Aktion: `devops-guru:ListInsights`

Erforderlich, um eine Liste der Erkenntnisse in Ihrem AWS Konto. Sie können anhand ihrer Startzeit und ihres Status angeben, welche Erkenntnisse zurückgegeben werden (`ongoing` oder `any`) und geben Sie (ein`reactive` oder `predictive`).

Ressource: *

`DescribeInsight`

Aktion: `devops-guru:DescribeInsight`

Erforderlich, um Details zu einem Einblick zurückzugeben, den Sie anhand seiner ID angeben.

Ressource: *

`SearchInsights`

Aktion: `devops-guru:SearchInsights`

Erforderlich, um eine Liste von Erkenntnissen in Ihrem AWS Konto. Sie können anhand der Startzeit, der Filter und des Typs angeben, welche Erkenntnisse zurückgegeben werden (`reactive` oder `predictive`).

Ressource: *

`ListAnomalies`

Aktion: `devops-guru:ListAnomalies`

Erforderlich, um eine Liste der Anomalien zurückzugeben, die zu einem Insight gehören, den Sie anhand seiner ID angeben.

Ressource: *

`DescribeAnomaly`

Aktion: `devops-guru:DescribeAnomaly`

Erforderlich, um Details zu einer Anomalie zurückzugeben, die Sie anhand ihrer ID angeben.

Ressource: *

`ListEvents`

Aktion: `devops-guru:ListEvents`

Erforderlich, um eine Liste der von den Ressourcen ausgehenden Ereignisse zurückzugeben, die von ausgewertet werden DevOps Guru. Sie können Filter verwenden, um anzugeben, welche Ereignisse zurückgegeben werden.

Ressource: *

`ListRecommendations`

Aktion: `devops-guru:ListRecommendations`

Erforderlich, um eine Liste der Empfehlungen eines bestimmten Insights zurückzugeben. Jede Empfehlung enthält eine Liste von Metriken und eine Liste von Ereignissen, die sich auf die Empfehlungen beziehen.

Ressource: *

`DescribeAccountHealth`

Aktion: `devops-guru:DescribeAccountHealth`

Erforderlich, um die Anzahl der offenen reaktiven Erkenntnisse, die Anzahl der offenen prädiktiven Erkenntnisse und die Anzahl der analysierten Metriken in Ihrem AWS Konto. Verwenden Sie diese Zahlen, um den Zustand der Operationen in Ihrem AWS Konto.

Ressource: *

`DescribeAccountOverview`

Aktion: `devops-guru:DescribeAccountOverview`

Erforderlich, um Folgendes zurückzugeben, das während eines Zeitraums passiert ist: die Anzahl der offenen reaktiven Erkenntnisse, die erstellt wurden, die Anzahl der offenen prädiktiven Erkenntnisse, die erstellt wurden, und die mittlere Wiederherstellungszeit (MTTR) für alle reaktiven Erkenntnisse, die geschlossen wurden.

Ressource: *

`DescribeResourceCollectionHealthOverview`

Aktion: `devops-guru:DescribeResourceCollectionHealthOverview`

Erforderlich, um die Anzahl offener prädiktiver Erkenntnisse, offener reaktiver Erkenntnisse und die mittlere Wiederherstellungszeit (MTTR) für alle Erkenntnisse für jeden einzelnen Einblick zurückzugeben CloudFormation Stapel, angegeben in DevOps Guru.

Ressource: *

`DescribeIntegratedService`

Aktion: `devops-guru:DescribeIntegratedService`

Erforderlich, um den Integrationsstatus von Diensten zurückzugeben, in die integriert werden können DevOps Guru. Der eine Dienst, der integriert werden kann DevOps Guru ist AWS Systems Manager, das verwendet werden kann, um eine zu erstellen OpsItem für jeden generierten Einblick.

Ressource: *

`UpdateIntegratedServiceConfig`

Aktion: `devops-guru:UpdateIntegratedServiceConfig`

Erforderlich, um die Integration mit einem Dienst zu aktivieren oder zu deaktivieren, der integriert werden kann DevOps Guru. Der eine Dienst, der integriert werden kann DevOps Guru ist Systems Manager, der verwendet werden kann, um einen zu erstellen OpsItem für jeden generierten Einblick.

Ressource: *

Berechtigungen für Amazon SNS-Themen

Verwenden Sie die Informationen in diesem Thema nur, wenn Sie Amazon konfigurieren möchten DevOps Guru versendet Benachrichtigungen zu Amazon SNS-Themen, die einem anderen gehören AWS Konto.

Für DevOps Guru: Um Benachrichtigungen zu einem Amazon SNS-Thema zu senden, das einem anderen Konto gehört, müssen Sie dem Amazon SNS-Thema eine Richtlinie beifügen, die Folgendes gewährt: DevOps Guru hat die Erlaubnis, Benachrichtigungen an ihn zu senden. Wenn du konfigurierst DevOps Guru, um Benachrichtigungen zu Amazon SNS-Themen zu senden, die demselben Konto gehören, für das Sie es verwenden DevOps Guru, dann DevOps Guru fügt den Themen eine Richtlinie für dich hinzu.

Nachdem Sie eine Richtlinie zur Konfiguration von Berechtigungen für ein Amazon SNS-Thema in einem anderen Konto angehängt haben, können Sie das Amazon SNS-Thema in hinzufügen DevOps Guru. Sie können Ihre Amazon SNS-Richtlinie auch mit einem Benachrichtigungskanal aktualisieren, um sie sicherer zu machen.

> **Note**
>
> DevOps Guru unterstützt derzeit nur den kontoübergreifenden Zugriff in derselben Region.

Themen

- Berechtigungen für ein Amazon SNS-Thema in einem anderen Konto konfigurieren
- Hinzufügen eines Amazon SNS-Themas von einem anderen Konto

- Aktualisierung Ihrer Amazon SNS-Richtlinie mit einem Benachrichtigungskanal (empfohlen)

Berechtigungen für ein Amazon SNS-Thema in einem anderen Konto konfigurieren

Hinzufügen von Berechtigungen als IAM-Rolle

Um ein Amazon SNS-Thema von einem anderen Konto aus zu verwenden, nachdem Sie sich mit einer IAM-Rolle angemeldet haben, müssen Sie dem Amazon SNS-Thema, das Sie verwenden möchten, eine Richtlinie anhängen. Um eine Richtlinie aus einem anderen Konto an ein Amazon SNS-Thema anzuhängen, während Sie eine IAM-Rolle verwenden, benötigen Sie im Rahmen Ihrer IAM-Rolle die folgenden Berechtigungen für diese Kontoressource:

- sns:CreateTopic
- sns:GetTopicAttributes
- sns:SetTopicAttributes
- sns:Publish

Hängen Sie die folgende Richtlinie an das Amazon SNS-Thema an, das Sie verwenden möchten. Für die `Resource` Schlüssel, *`topic-owner-account-id`* ist die Konto-ID des Themen-Inhabers, *`topic-sender-account-id`* ist die Konto-ID des Benutzers, der das Konto eingerichtet hat DevOps Guru, und *`devops-guru-role`* ist die IAM-Rolle des einzelnen beteiligten Benutzers. Sie müssen die entsprechenden Werte durch ersetzen *`region-id`* (zum Beispiel `us-west-2`) und *`my-topic-name`*.

Hinzufügen von Berechtigungen als IAM-Benutzer

Um als IAM-Benutzer ein Amazon SNS-Thema von einem anderen Konto aus zu verwenden, fügen Sie dem Amazon SNS-Thema, das Sie verwenden möchten, die folgende Richtlinie hinzu. Für den `Resource` Schlüssel, *`topic-owner-account-id`* ist die Konto-ID des Themen-Inhabers, *`topic-sender-account-id`* ist die Konto-ID des Benutzers, der das Konto eingerichtet hat DevOps Guru, und *`devops-guru-user-name`* ist der einzelne beteiligte IAM-Benutzer. Sie müssen die entsprechenden Werte durch ersetzen *`region-id`* (zum Beispiel `us-west-2`) und *`my-topic-name`*.

> **Note**
>
> Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und

Zugriffsschlüssel haben. Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Hinzufügen eines Amazon SNS-Themas von einem anderen Konto

Nachdem Sie die Berechtigungen für ein Amazon SNS-Thema in einem anderen Konto konfiguriert haben, können Sie dieses Amazon SNS-Thema zu Ihrem hinzufügen DevOps Guru-Benachrichtigungseinstellungen. Sie können das Amazon SNS-Thema mit dem hinzufügen AWS CLI oder der DevOps Guru-Konsole.

- Wenn Sie die Konsole verwenden, müssen Sie die Option auswählen Verwenden Sie einen SNS-Thema-ARN, um ein vorhandenes Thema anzugeben um ein Thema aus einem anderen Konto zu verwenden.
- Wenn du den verwendest AWS CLI Betrieb Benachrichtigungskanal hinzufügen, müssen Sie das angeben `TopicArn` innerhalb der `NotificationChannelConfig` Objekt.

Fügen Sie mithilfe der Konsole ein Amazon SNS-Thema von einem anderen Konto hinzu

1. Öffnen Sie Amazon DevOps Guru-Konsole bei https://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und wählen Sie dann Einstellungen.
3. Gehe zum Benachrichtigungen Abschnitt und wähle Bearbeiten.
4. Wählen SNS-Thema hinzufügen.
5. Wählen Verwenden Sie einen SNS-Thema-ARN, um ein vorhandenes Thema anzugeben.
6. Geben Sie den ARN des Amazon SNS-Themas ein, das Sie verwenden möchten. Sie sollten die Berechtigungen für dieses Thema bereits konfiguriert haben, indem Sie ihm eine Richtlinie angehängt haben.
7. (Optional) Wählen Sie Konfiguration der Benachrichtigung um die Einstellungen für die Häufigkeit von Benachrichtigungen zu bearbeiten.
8. Wählen Sie Speichern.

Nachdem Sie das Amazon SNS-Thema zu Ihren Benachrichtigungseinstellungen hinzugefügt haben, DevOps Guru verwendet dieses Thema, um dich über wichtige Ereignisse zu informieren, z. B. wenn eine neue Erkenntnis entsteht.

Aktualisierung Ihrer Amazon SNS-Richtlinie mit einem Benachrichtigungskanal (empfohlen)

Nachdem Sie ein Thema hinzugefügt haben, empfehlen wir Ihnen, Ihre Richtlinie sicherer zu machen, indem Sie nur Berechtigungen für DevOps Guru-Benachrichtigungskanal, der dein Thema enthält.

Aktualisieren Sie Ihre Amazon SNS-Themenrichtlinie mit einem Benachrichtigungskanal (empfohlen)

1. Führen Sie das aus `list-notification-channels` DevOps Guru AWS CLI Befehl in deinem Konto, von dem aus du Benachrichtigungen senden möchtest.

   ```
   aws devops-guru list-notification-channels
   ```

2. In der `list-notification-channels` Notieren Sie sich in Ihrer Antwort die Kanal-ID, die den ARN Ihres Amazon SNS-Themas enthält. Die Kanal-ID ist eine GUID.

   In der folgenden Antwort beispielsweise die Kanal-ID für das Thema mit dem ARN `arn:aws:sns:region-id:111122223333:topic-name` ist *e89be5f7-989d-4c4c-b1fe-e7145037e531*

   ```
   {
     "Channels": [
       {
         "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
         "Config": {
         "Sns": {
             "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
           },
         "Filters": {
             "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
             "Severities": ["HIGH", "MEDIUM"]
           }
         }
       }
     ]
   }
   ```

3. Gehen Sie zu der Richtlinie, die Sie in einem anderen Konto erstellt haben, und verwenden Sie dabei die Inhaber-ID des Themas in the section called “Berechtigungen für ein Amazon SNS-Thema in einem anderen Konto konfigurieren”. In der `Condition` Fügen Sie in der Erklärung der Richtlinie die Zeile hinzu, die Folgendes angibt `SourceArn`. Der ARN enthält Ihre Regions-

ID (z. B. `us-east-1`), das AWS Kontonummer des Absenders des Themas und die Kanal-ID, die Sie sich notiert haben.

Du hast es aktualisiert `Condition` Aussage sieht wie folgt aus.

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

Wenn `AddNotificationChannel` Ihr SNS-Thema nicht hinzufügen kann, überprüfen Sie, ob Ihre IAM-Richtlinie über die folgenden Berechtigungen verfügt.

Berechtigungen für AWS KMS— verschlüsselte Amazon SNS-Themen

Das von Ihnen angegebene Amazon SNS-Thema ist möglicherweise verschlüsselt durch AWS Key Management Service. Zulassen DevOps Guru, um mit verschlüsselten Themen zu arbeiten, musst du zuerst eine erstellen AWS KMS key und fügen Sie dann die folgende Anweisung zur Richtlinie des KMS-Schlüssels hinzu. Weitere Informationen finden Sie unter Verschlüsseln von Nachrichten, die auf Amazon SNS veröffentlicht wurden, mit AWS KMS, Wichtige Identifikatoren (KeyId) in der AWS KMS Benutzerleitfaden, und Verschlüsselung der Daten in der Amazon Simple Notification Service — Entwicklerhandbuch.

> **Note**
>
> DevOps Guru unterstützt derzeit verschlüsselte Themen zur Verwendung in einem einzigen Konto. Die Verwendung eines verschlüsselten Themas für mehrere Konten wird derzeit nicht unterstützt.

Fehlerbehebung bei Amazon DevOps Guru-Identität und Zugang

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit DevOps Guru und IAM.

Themen

- Ich bin nicht berechtigt, eine Aktion auszuführen in DevOps Guru
- Ich möchte Benutzern programmatischen Zugriff gewähren
- Ich bin nicht berechtigt, iam: auszuführenPassRole
- Ich möchte Leute außerhalb von mir zulassen AWS Konto für den Zugriff auf mein DevOps Guru-Ressourcen

Ich bin nicht berechtigt, eine Aktion auszuführen in DevOps Guru

Wenn der AWS-Managementkonsole wenn Ihnen mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einem fiktiven Objekt anzuzeigen *`my-example-widget`* Ressource, hat aber nicht das Fiktive `aws:`*`GetWidget`* Genehmigungen.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `aws:`*`GetWidget`* zugreifen zu können.

Ich möchte Benutzern programmatischen Zugriff gewähren

Benutzer benötigen programmatischen Zugriff, wenn sie interagieren möchten AWS außerhalb von AWS-Managementkonsole. Die Art und Weise, wie der programmatische Zugriff gewährt wird, hängt von der Art des Benutzers 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 die Anmeldeinformationen der Konsole als temporäre	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten.

Welcher Benutzer benötigt programmgesteuerten Zugriff?	Bis	Von
	Anmeldeinformationen, um programmatische Anfragen an die zu signieren AWS CLI, AWS SDKs oder AWS APIs.	• Für die AWS CLI, siehe Einloggen für AWS lokale Entwicklung in der AWS Command Line Interface Benutzerleitfaden. • Für AWS SDKs finden Sie unter Einloggen für AWS lokale Entwicklung in der AWS Referenzhandbuch für SDKs und Tools.
Mitarbeiteridentität (Benutzer, die in IAM Identity Center verwaltet werden)	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die zu signieren AWS CLI, AWS SDKs oder AWS APIs.	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Für die AWS CLI, siehe Konfiguration der AWS CLI zu verwenden AWS IAM Identity Center in der AWS Command Line Interface Benutzerleitfaden. • Für AWS SDKs, Tools und AWS APIs, siehe IAM Identity Center-Authentifizierung in der AWS Referenzhandbuch für SDKs und Tools.
IAM	Verwenden Sie temporäre Anmeldeinformationen, um programmatische Anfragen an die zu signieren AWS CLI, AWS SDKs oder AWS APIs.	Folgen Sie den Anweisungen in Verwenden Sie temporäre Anmeldeinformationen mit AWS Ressourcen in der IAM-Benutzerhandbuch.

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

Ich bin nicht berechtigt, iam: auszuführenPassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, das auszuführen `iam:PassRole` Aktion, Ihre Richtlinien müssen aktualisiert werden, damit Sie eine Rolle übergeben können DevOps Guru.

Etwas AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Dienst zu übergeben, anstatt eine neue Dienstrolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer den Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion auszuführen in DevOps Guru. 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 Leute außerhalb von mir zulassen AWS Konto für den Zugriff auf mein DevOps Guru-Ressourcen

Du kannst eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb deiner Organisation auf deine Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Um zu erfahren, ob DevOps Guru unterstützt diese Funktionen, siehe Wie Amazon DevOps Guru arbeitet mit IAM.
- Um zu erfahren, wie Sie überall Zugriff auf Ihre Ressourcen gewähren AWS-Konten die Sie besitzen, finden Sie Bereitstellung des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto das Sie besitzen in der IAM-Benutzerhandbuch.
- Um zu erfahren, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, siehe Bereitstellung des Zugangs zu AWS-Konten im Besitz von Dritten in der IAM-Benutzerhandbuch.
- 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.

Protokollierung und Überwachung DevOps Guru

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von DevOps Guru und Ihre anderen AWS-Lösungen. AWS bietet die folgenden Überwachungstools zum Beobachten DevOps Guru, melde, wenn etwas nicht stimmt, und ergreife gegebenenfalls automatische Maßnahmen:

- Amazon CloudWatch überwacht deine AWS Ressourcen und die Anwendungen, auf denen Sie laufen AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Zum Beispiel kannst du haben CloudWatch verfolgen Sie die CPU-Auslastung oder andere Messwerte Ihrer Amazon EC2-Instances und starten Sie bei Bedarf automatisch neue Instances. Weitere Informationen finden Sie auf der Amazon CloudWatch Benutzerleitfaden.
- AWS CloudTrail erfasst API-Aufrufe und damit verbundene Ereignisse, die von oder in Ihrem Namen getätigt wurden AWS Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.

Themen

- Überwachung DevOps Guru bei Amazon CloudWatch
- Amazon protokollieren DevOps Guru-API-Aufrufe mit AWS CloudTrail

Überwachung DevOps Guru bei Amazon CloudWatch

Sie können überwachen DevOps Guru benutzt CloudWatch, das Rohdaten sammelt und sie zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie auf der Amazon CloudWatch Benutzerleitfaden.

Für DevOps Guru, du kannst Kennzahlen verfolgen, um Erkenntnisse zu gewinnen, und Kennzahlen für deine DevOps Guru-Nutzung. Vielleicht möchten Sie nach einer großen Anzahl von erstellten Dateien Ausschau halten `Insights` um Ihnen bei der Feststellung zu helfen, ob Ihre betrieblichen Lösungen ein ungewöhnliches Verhalten aufweisen. Oder vielleicht möchten Sie sich Ihre ansehen DevOps Verwendung von Guru, um Ihre Kosten im Auge zu behalten.

Das DevOps Der Guru-Service meldet die folgenden Metriken im `AWS/DevOps-Guru` Namespace.

Themen

- Kennzahlen für Einblicke
- DevOps Metriken zur Guru-Nutzung

Kennzahlen für Einblicke

Sie können verwenden CloudWatch um eine Metrik zu verfolgen, die Ihnen zeigt, wie viele Erkenntnisse in Ihrem AWS Konto. Sie können angeben `Type` Dimension, die verfolgt werden soll `proactive` oder `reactive` Einblicke. Geben Sie keine Dimension an, wenn Sie alle Erkenntnisse verfolgen möchten.

Metriken

Metrik	Description
`Insight`	Die Anzahl der Erkenntnisse, die in einem erstellt wurden AWS Konto. Gültige Abmessungen: `Type` Gültige Statistiken: Anzahl der Stichproben, Summe Einheiten: Anzahl

Die folgende Dimension wird unterstützt für DevOps Guru `Insight` metrisch.

Dimensions (Abmessungen)

Dimension	Description
`Type`	Das ist die Art der Einsicht. Geben Sie keine Dimension für den an `Insights` Metrik, wenn Sie alle Erkenntnisse verfolgen möchten. Gültige Werte sind: `proactive` , `reactive`.

DevOps Metriken zur Guru-Nutzung

Du kannst verwenden CloudWatch um deinen Amazon zu verfolgen DevOps Guru-Nutzung.

Metriken

Metrik	Description
`CallCount`	Die Anzahl der Anrufe, die von einem der folgenden Unternehmen getätigt wurden DevOps Guru-Methoden. • `ListInsights` • `ListAnomaliesForInsight` • `ListRecommendations` • `ListEvents` • `SearchInsights` • `DescribeInsight` • `DescribeAnomaly` Gültige Abmessungen: `Service`, `Class`, `Type`, `Resource` Gültige Statistiken: Anzahl der Stichproben, Summe

Metrik	Description
	Einheiten: Anzahl

Die folgenden Dimensionen werden unterstützt für DevOps Metriken zur Guru-Nutzung.

Dimensions (Abmessungen)

Dimension	Description
`Service`	Dies ist der Name des AWS-Service, der die Ressource enthält. Zum Beispiel für DevOps Guru, dieser Wert ist `DevOps-Guru` .
`Class`	Dies ist die Klasse der Ressource, die verfolgt wird. DevOps Guru verwendet diese Dimension mit dem Wert `None`.
`Type`	Dies ist der Typ der Ressource, die verfolgt wird. DevOps Guru verwendet diese Dimension mit dem Wert `API`.
`Resource`	Das ist der Name des DevOps Guru-Operation. Gültige Werte sind: `ListInsights` , `ListAnomaliesForInsight` , `ListRecommendations` , `ListEvents` , `SearchInsights` , `DescribeInsight` , `DescribeAnomaly` .

Amazon protokollieren DevOps Guru-API-Aufrufe mit AWS CloudTrail

Amazonas DevOps Guru ist integriert in AWS CloudTrail, ein Dienst, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst in DevOps Guru. CloudTrail erfasst API-Aufrufe für DevOps Guru als Ereignisse. Zu den aufgezeichneten Anrufen gehören Anrufe von DevOps Guru-Konsole und Codeanrufe an die DevOps Guru-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von aktivieren CloudTrail Ereignisse an einen Amazon S3-Bucket, einschließlich Ereignisse für DevOps Guru. Wenn du keinen Trail konfigurierst, kannst du trotzdem die neuesten Ereignisse in der CloudTrail Konsole in Verlauf der Veranstaltung. Verwendung der gesammelten Informationen von CloudTrail, können Sie die Anfrage ermitteln, die gestellt wurde an DevOps Guru, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Um mehr zu erfahren über CloudTrail, siehe AWS CloudTrail Benutzerleitfaden.

DevOps Guru-Informationen in CloudTrail

CloudTrail ist auf deinem aktiviert AWS Konto, wenn Sie das Konto erstellen. Wenn Aktivität stattfindet in DevOps Guru, diese Aktivität wird in einem aufgezeichnet CloudTrail Veranstaltung zusammen mit anderen AWS Serviceveranstaltungen in Verlauf der Ereignisse. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS Konto. Weitere Informationen finden Sie unter Ereignisse anzeigen mit CloudTrail Verlauf der Ereignisse.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich Veranstaltungen für DevOps Guru, erstelle eine Spur. EIN Wanderweg aktiviert CloudTrail um Protokolldateien an einen Amazon S3-Bucket zu liefern. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS partitioniert und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere konfigurieren AWS Dienste zur weiteren Analyse und Bearbeitung der in CloudTrail protokolliert. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail Protokolldateien aus mehreren Regionen und Empfangen CloudTrail Protokolldateien von mehreren Konten

DevOps Guru unterstützt das Protokollieren all seiner Aktionen als Ereignisse in CloudTrail Protokolldateien. Weitere Informationen finden Sie unter Aktionen in der DevOps Guru API-Referenz.

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 Root- oder -Benutzeranmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen gestellt wurde AWS Service.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Verstehen DevOps Guru-Logdateieinträge

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt eine CloudTrail Protokolleintrag, der das demonstriert `UpdateResourceCollection` Aktion.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
```

```
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


DevOps Guru- und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können VPC-Endpunkte verwenden, wenn Sie Amazon anrufen DevOps Guru-APIs. Wenn Sie VPC-Endpunkte verwenden, sind Ihre API-Aufrufe sicherer, da sie in Ihrer VPC enthalten sind und nicht auf das Internet zugreifen. Weitere Informationen finden Sie unter Aktionen in der Amazonas DevOps Guru API-Referenz.

Sie stellen eine private Verbindung zwischen Ihrer VPC her und DevOps Guru, indem du einen erstellst Schnittstelle VPC-Endpunkt. Schnittstellen-Endpunkte werden unterstützt von AWS PrivateLink, eine Technologie, die es Ihnen ermöglicht, privat darauf zuzugreifen DevOps Guru-APIs ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct Connect-Verbindung. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit ihnen zu kommunizieren DevOps Guru-APIs. Verkehr zwischen Ihrer VPC und DevOps Guru verlässt das Amazon-Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter Schnittstelle: VPC-Endpunkte (AWS) PrivateLink) in der Amazon VPC-Benutzerhandbuch.

Überlegungen für DevOps Guru VPC-Endpunkte

Bevor Sie einen Schnittstellen-VPC-Endpunkt einrichten für DevOps Guru, stell sicher, dass du rezensierst Eigenschaften und Einschränkungen von Schnittstellen-Endpunkten in der Amazon VPC-Benutzerhandbuch.

DevOps Guru unterstützt das Aufrufen all seiner API-Aktionen von deiner VPC aus.

Erstellen eines Schnittstellen-VPC-Endpunkts für DevOps Guru

Sie können einen VPC-Endpunkt für den erstellen DevOps Guru-Service, der entweder die Amazon VPC-Konsole oder die AWS Command Line Interface (AWS CLI). Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für DevOps Guru verwendet den folgenden Dienstnamen:

- com.amazonaws.*region*.devops-guru

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen stellen an DevOps Guru verwendet zum Beispiel seinen Standard-DNS-Namen für die Region `devops-guru.us-east-1.amazonaws.com`.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für DevOps Guru

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf steuert DevOps Guru. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die 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 DevOps Guru-Aktionen

Das Folgende ist ein Beispiel für eine Endpunktrichtlinie für DevOps Guru. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie Zugriff auf die aufgelisteten DevOps Guru-Aktionen für alle Schulleiter auf allen Ressourcen.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

Sicherheit der Infrastruktur in DevOps Guru

Als verwalteter Dienst, Amazon DevOps Guru ist geschützt durch AWS globale Netzwerksicherheit. Für Informationen über AWS Sicherheitsdienste und wie AWS schützt die Infrastruktur, siehe AWS Cloud-Sicherheit. Um Ihre zu entwerfen AWS Umgebung, in der die bewährten Methoden für die Infrastruktursicherheit verwendet werden, finden Sie unter Schutz der Infrastruktur in Säule „Sicherheit“ AWS Gut durchdachtes Framework.

Du benutzt AWS veröffentlichte API-Aufrufe für den Zugriff DevOps Guru durch das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungssammlungen 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.

Widerstandsfähigkeit bei Amazon DevOps Guru

Das AWS Die globale Infrastruktur basiert auf AWS Regionen und Verfügbarkeitszonen. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. DevOps Guru arbeitet in mehreren Availability Zones und speichert Artefaktdaten und Metadaten in Amazon S3 und Amazon DynamoDB. Ihre verschlüsselten Daten werden redundant in mehreren Einrichtungen und auf mehreren Geräten in jeder Einrichtung gespeichert, wodurch sie hochverfügbar und äußerst langlebig sind.

Für weitere Informationen über AWS Regionen und Verfügbarkeitszonen finden Sie unter AWS Weltweite Infrastruktur.

Kontingente und Limits für Amazon DevOps Guru

In der folgenden Tabelle ist das aktuelle Kontingent in Amazon DevOps Guru aufgeführt. Dieses Kontingent gilt für jede unterstützte AWS Region für jedes AWS Konto.

Benachrichtigungen

Maximale Anzahl Amazon-Simple-Notification-Service-Themen, die Sie gleichzeitig festlegen können	2

CloudFormation Stapel

Maximale Anzahl von AWS CloudFormation Stacks, die Sie angeben können	1000

DevOpsGrenzwerte für die Überwachung von Guru-Ressourcen

Beschreibung der Ressource	Limit	Kann erhöht werden
Standardlimit für die Überwachung von Amazon Simple Queue Service (Amazon SQS) -Wartesch langen	100*	Ja**

*Für neue DevOps Guru-Konten, die am oder nach dem 29. Juni 2023 erstellt wurden, und für bestehende Konten, die am selben Tag aktiv waren und weniger als 100 Amazon SQS SQS-Warteschlangen haben.

**Um eine Änderung dieses Limits zu beantragen, kontaktieren Sie uns unter /contact-us. Support https://aws.amazon.com Sie können ein Amazon SQS SQS-Warteschlangenüberwachungslimit von 100, 500, 1.000, 5.000 oder 10.000 anfordern.

DevOpsGuru-Kontingente für die Erstellung, Bereitstellung und Verwaltung einer API

Die folgenden festen Kontingente gelten für das Erstellen, Bereitstellen und Verwalten einer API in DevOps Guru mithilfe der AWS CLI API Gateway Gateway-Konsole oder der API Gateway Gateway-REST-API und ihrer SDKs.

Eine Liste aller DevOps Guru finden Sie APIs unter Amazon DevOps Guru Actions.

Standardkontingent	Kann erhöht werden	
20 Anfragen alle 1 Sekunde pro Konto	Ja	

Amazon DevOps Guru-Dokumentenhistorie

In der folgenden Tabelle wird die Dokumentation für diese Version von beschrieben DevOps Guru.

- API-Version: aktuelle
- Neuestes Update der Dokumentation: 9. August 2023

Änderung	Beschreibung	Datum
Leitfaden für die Umstellung auf Amazon CloudWatch und Amazon DevOps Agent	Eine Anleitung für den Übergang von Amazon wurde hinzugefügt DevOps Guru zu Amazon CloudWatch und Amazon DevOps Agent vor Amazon DevOps Guru erreicht am 30. September 2027 das Ende der Unterstüt zung. Weitere Informationen finden Sie unter Übergang von Amazon DevOps Guru zu Amazon CloudWatch und Amazon DevOps Agent.	8. Oktober 2026
Mitteilung zum Ende des Supports	Hinweis zum Ende des Supports: Am 30. September 2027, AWS wird die Unterstüt zung für Amazon beenden DevOps Guru. Nach dem 30. September 2027 können Sie nicht mehr auf Amazon zugreifen DevOps Guru-Kons ole oder Amazon DevOps Guru-Ressourcen. Weitere Informationen finden Sie	29. September 2026

	unter Amazon DevOps Guru beendet den Support.	
Aktualisierung der verwalteten Richtlinien	Amazon SNS-Abonnements und der Zugriff auf Abonnementlisten wurden dem hinzugefügt `AmazonDevOpsGuruConsoleFullAccess` Richtlinie. Der Zugriff auf die Abonnementliste wurde ebenfalls zur `AmazonDevOpsGuruReadOnlyAccess` Richtlinie. Weitere Informationen finden Sie unter Identity-based Richtlinien für Amazon DevOps Guru.	9. August 2023
Vom Kunden verwaltete Verschlüsselungsschlüssel	DevOps Guru unterstützt jetzt die Verschlüsselung mit vom Kunden verwalteten Schlüsseln mit AWS KMS. Weitere Informationen finden Sie unter Datenschutz in DevOps Guru.	5. Juli 2023
DevOps Guru für RDS unterstützt RDS PostgreSQL	DevOps Guru for RDS kann Leistungsengpässe und andere Erkenntnisse in PostgreSQL-Datenbanken erkennen. Weitere Informationen finden Sie unter Vorteile von DevOps Guru für RDS.	30. März 2023

DevOps Guru for RDS unterstützt proaktive Einblicke	DevOps Guru for RDS veröffentlicht proaktive Einblicke mit Empfehlungen, die Ihnen helfen, Probleme in Ihren Aurora-Datenbanken zu beheben, bevor sie zu größeren Problemen werden. Weitere Informationen finden Sie unter Arbeiten mit Anomalien in DevOps Guru für RDS.	28. Februar 2023
Seite mit analysierten Ressourcen	Eine neue Seite in der DevOps Die Guru-Konsole listet Ressourcen in Ihrem Konto auf, die analysiert werden von DevOps Guru. Weitere Informationen finden Sie unter Ressourcen anzeigen, analysiert von DevOps Guru.	20. Oktober 2022
Neue Konfigurationseinstellungen für Benachrichtigungen	Sie können jetzt wählen, ob Sie alle Benachrichtigungen oder nur Benachrichtigungen für bestimmte Schweregrade und Ereignisse erhalten möchten. Weitere Informationen finden Sie unter Aktualisierung der Amazon Amazon SNS-Benachrichtigungskonfigurationen.	30. September 2022

Zusätzlich zu den verwaltet en Richtlinien die Analyse von Anomalien protokollieren	AWS verwaltete Richtlinien für DevOps Guru wurde in der IAM-Konsole aktualisi ert, um den Zugriff auf das zu unterstützen CloudWatch Aktion `FilterLogEvents` . Weitere Informationen finden Sie unter DevOps Guru aktualisiert für AWS verwaltet e Richtlinien und dienstbez ogene Rolle.	30. August 2022
Analyse der Protokollanomalie hinzugefügt	Detaillierte Informationen zu Protokollgruppen, die sich auf Erkenntnisse beziehen, finden Sie im DevOps Guru-Konsole. Es steht auch eine erweiterte, dienstbezogene Rolle zur Beschreibung zur Verfügung CloudWatc h Protokolle und Streams. Weitere Informationen finden Sie unter Grundlegendes zu den Erkenntnissen in DevOps Guru-Konsole und DevOps Guru aktualisiert für AWS verwaltete Richtlinien und dienstbezogene Rolle.	12. Juli 2022

CodeGuru Profiler-Integration	DevOps Guru lässt sich jetzt in Amazon integrieren CodeGuru Profiler mit einem EventBridge verwaltete Regel. Jedes eingehende Ereignis von CodeGuru Profiler ist ein proaktiver Anomaliebericht. Weitere Informationen finden Sie unter Integrieren mit CodeGuru Profiler.	7. März 2022
Service-linked Aktualisierungen von Rollen und verwalteten Richtlinien	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderungen ermöglichen DevOps Guru unterstützt die erweiterte Integration mit Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unter Verwenden von dienstverknüpften Rollen und AWS verwaltete (vordefinierte) Richtlinien für DevOps Guru.	21. Dezember 2021
Neue verwaltete Richtlinie hinzugefügt	Die `AmazonDevOpsGuruConsoleFullAccess` Richtlinie wurde hinzugefügt. Weitere Informationen finden Sie unter Identity-based Richtlinien für Amazon DevOps Guru.	6. Dezember 2021

Unterstützung bei der Definition Ihrer Anwendung mit AWS Tags	Sie können jetzt verwenden AWS Tags, um die gewünschten Ressourcen zu identifizieren DevOps Guru zum Analysieren, Identifizieren der Ressourcen in Ihren Anwendungen und Filtern von Erkenntnissen in der Konsole. Weitere Informationen finden Sie unter Verwenden Sie Tags, um Ressourcen in Ihren Anwendungen zu identifizieren.	1. Dezember 2021
Service-linked Aktualisierungen von Rollen und verwalteten Richtlinien	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderungen ermöglichen DevOps Guru unterstützt die erweiterte Integration mit Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unter Verwenden von dienstverknüpften Rollen und AWS verwaltete (vordefinierte) Richtlinien für DevOps Guru.	1. Dezember 2021

Amazon RDS-Unterstützung	DevOps Guru bietet jetzt umfassende Analysen und Einblicke für Amazon Relational Database Service (Amazon RDS) -Ressourcen in Ihrer Anwendung. Weitere Informationen finden Sie unter Arbeiten mit Anomalien in DevOps Guru für Amazon RDS.	1. Dezember 2021
Amazonas EventBridge Integration	DevOps Guru integriert sich jetzt in EventBridge um Sie über bestimmte Ereignisse im Zusammenhang mit Ihrem zu informieren DevOps Einblicke in Gurus. Weitere Informationen finden Sie unter Arbeiten mit EventBridge.	18. November 2021
AWS verwaltete Richtlinie hinzugefügt	Neu AWS verwaltete Richtlinie hinzugefügt. Die `AmazonDevOpsGuruOrganizationsAccess` Die Richtlinie bietet Zugang zu DevOps Guru innerhalb einer Organisation. Weitere Informationen finden Sie unter identitätsbasierte Richtlinien.	16. November 2021

Service-linked Aktualisierung der Rollenrichtlinie	Erweiterte Richtlinie in der IAM-Konsole verfügbar. Die Änderung ermöglicht DevOps Guru zur Unterstützung der Multi-Account-Ansicht. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen.	4. November 2021
Kontoübergreifende Unterstützung	Sie können jetzt Einblicke und Kennzahlen für mehrere Konten in Ihrer Organisation einsehen. Weitere Informationen finden Sie unter Was ist Amazon DevOps Guru.	4. November 2021
Veröffentlichung zur allgemeinen Verfügbarkeit	Amazon DevOps Guru ist jetzt allgemein verfügbar (GA).	4. Mai 2021
Neues Thema	Sie können jetzt einen monatlichen Kostenvoranschlag erstellen für DevOps Guru, um deine Ressourcen zu analysieren. Weitere Informationen finden Sie unter Schätzen Sie Ihren Amazon-Wert DevOps Guru kostet.	27. April 2021
Unterstützung für VPC-Endpunkte	Sie können jetzt VPC-Endpunkte verwenden, um die Sicherheit Ihrer Ressourcenanalyse und der Generierung von Erkenntnissen zu verbessern. Weitere Informationen finden Sie unter DevOps Guru- und Schnittstellen-VPC-Endpunkte (AWS PrivateLink).	15. April 2021

Neues Thema	Ein neues Thema zur Überwachung DevOps Guru bei Amazon CloudWatch wurde hinzugefügt. Weitere Informationen finden Sie unter Überwachung DevOps Guru bei Amazon CloudWatch.	11. Dezember 2020
Vorschauversion	Dies ist die Vorabversion der Amazon DevOps Guru-Benutzerhandbuch.	1. Dezember 2020

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.