Benutzerhandbuch

DevOps Amazon-Guru

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

DevOps Amazon-Guru: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Was ist Amazon DevOps Guru? ... 1
Wie funktioniert DevOps Guru? ... 1
DevOpsGuru-Workflow 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
Berichterstattung ... 8
Liste der Serviceabdeckungen ... 10
Einrichtung ... 12
Melde dich an für AWS ... 12
Melde dich an für ein AWS-Konto ... 12
Erstellen eines Benutzers mit Administratorzugriff ... 13
Ermitteln Sie den Versicherungsschutz für DevOps Guru ... 15
Identifizieren Sie das Thema Ihrer Benachrichtigungen ... 16
Ihrem Thema wurden Berechtigungen hinzugefügt ... 16
Schätzung Ihrer Kosten ... 18
Erste Schritte ... 21
Schritt 1: Richten Sie sich ein ... 21
Schritt 2: DevOps Guru aktivieren ... 21
Überwachen Sie Konten in Ihrer gesamten Organisation ... 21
Überwachen Sie Ihr Girokonto ... 23
Schritt 3: Spezifizieren Sie den Umfang Ihrer DevOps Guru-Ressourcen ... 25
Aktivierung von AWS Diensten für die DevOps Guru-Analyse ... 27
Mit Erkenntnissen arbeiten ... 28
Einblicke ansehen ... 28
Einblicke in die DevOps Guru-Konsole verstehen ... 30
Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden ... 33
Die Schweregrade von Insight verstehen ... 34

Datenbanken überwachen ... 35
Relationale Datenbanken ... 35
Überwachung von Datenbankoperationen in Amazon RDS ... 35
Überwachung von Datenbankvorgängen in Amazon Redshift ... 38
Arbeiten mit Anomalien in Guru for RDS DevOps ... 39
Nichtrelationale Datenbanken ... 60
Überwachung von Datenbankoperationen in Amazon DynamoDB ... 60
Überwachung von Datenbankoperationen in Amazon ElastiCache ... 61
Integration mit CodeGuru Profiler ... 62
Definition von Anwendungen mithilfe von AWS Ressourcen ... 63
Verwenden Sie Tags, um Ressourcen in Ihren Anwendungen zu identifizieren ... 64
Was ist ein Tag? ... 65
Definition einer Anwendung mithilfe eines Tags ... 66
Verwenden von Tags mit DevOps Guru ... 66
Hinzufügen von Tags zu Ressourcen ... 67
Verwenden Sie Stacks, um Ressourcen in Ihren DevOps Guru-Anwendungen zu identifizieren ... 68
Auswahl der zu analysierenden Stapel ... 69
Arbeitet mit EventBridge ... 71
Veranstaltungen für DevOps Guru ... 71
DevOpsGuruNeue offene Veranstaltung von Insight ... 71
Benutzerdefiniertes Beispielereignismuster für einen neuen Einblick mit hohem Schweregrad ... 73
Einstellungen werden aktualisiert ... 74
Aktualisierung Ihres Verwaltungskontos ... 74
Aktualisierung Ihres AWS Analysebereichs ... 75
Aktualisierung deiner Benachrichtigungen ... 75
Navigieren Sie zu den Benachrichtigungseinstellungen in der DevOps Guru-Konsole ... 76
Hinzufügen von Amazon SNS SNS-Benachrichtigungsthemen ... 76
Amazon SNS SNS-Benachrichtigungsthemen entfernen ... 77
Aktualisierung der Amazon SNS SNS-Benachrichtigungskonfigurationen ... 77
Ihrem Thema wurden Berechtigungen hinzugefügt ... 78
Filtere deine Benachrichtigungen ... 79
Filtern von Benachrichtigungen mit einer Amazon SNS SNS-Abonnementfilterrichtlinie ... 79
Beispiel für eine gefilterte Amazon SNS SNS-Benachrichtigung ... 80
Aktualisierung der Systems Manager Manager-Integration ... 82

Aktualisierung der Erkennung von Protokollanomalien ... 83
Die Verschlüsselung wird aktualisiert ... 83
Benachrichtigungen anzeigen ... 85
Neue Erkenntnisse ... 85
Geschlossener Einblick ... 86
Neuer Verband ... 88
Neue Empfehlung ... 89
Schweregrad wurde erhöht ... 90
Fehler bei der Ressourcenvalidierung ... 91
Analysierte Ressourcen anzeigen ... 93
Aktualisierung Ihres AWS Analysebereichs ... 93
Die Ansicht „Analysierte Ressourcen“ wird für Benutzer entfernt ... 95
Bewährte Methoden ... 97
Sicherheit ... 98
Datenschutz ... 99
Datenverschlüsselung ... 100
Wie verwendet DevOps Guru Zuschüsse in AWS KMS ... 101
Überwachen Sie Ihre Verschlüsselungsschlüssel in Guru DevOps ... 102
Einen kundenverwalteten Schlüssel erstellen ... 102
Datenschutz für Datenverkehr ... 104
Identitäts- und Zugriffsverwaltung ... 104
Zielgruppe ... 105
Authentifizierung mit Identitäten ... 106
Verwalten des Zugriffs mit Richtlinien ... 110
Richtlinienaktualisierungen ... 113
So arbeitet Amazon DevOps Guru mit IAM ... 118
Identitätsbasierte Richtlinien ... 125
Verwenden von serviceverknüpften Rollen ... 138
DevOpsReferenz zu Guru-Berechtigungen ... 144
Berechtigungen für Amazon SNS SNS-Themen ... 148
Berechtigungen für verschlüsselte Amazon SNS SNS-Themen ... 154
Fehlerbehebung ... 155
DevOpsGuru überwachen ... 160
Überwachung mit CloudWatch ... 160
DevOpsGuru-API-Aufrufe protokollieren mit AWS CloudTrail ... 163
VPC-Endpunkte (AWS PrivateLink) ... 166

Überlegungen zu DevOps Guru VPC-Endpunkten 167
Erstellen eines VPC-Schnittstellen-Endpunkts für Guru DevOps 167
Erstellen einer VPC-Endpunktrichtlinie für Guru DevOps 167
Sicherheit der Infrastruktur 168
Ausfallsicherheit 169
Kontingente und -Einschränkungen 170
Benachrichtigungen 170
AWS CloudFormation Stapel 170
DevOpsGrenzwerte für die Überwachung von Guru-Ressourcen 170
DevOpsGuru-Kontingente für die Erstellung, Bereitstellung und Verwaltung einer API 171
Dokumentverlauf 172
AWS Glossar 180
..... clxxxi

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 betrieblicher Probleme auslagern, sodass Sie schnell Empfehlungen zur Verbesserung Ihrer Anwendung umsetzen können. DevOpsGuru liefert reaktive Erkenntnisse, die Sie nutzen können, um Ihre Anwendung jetzt zu verbessern. Es bietet auch proaktive Einblicke, mit denen Sie betriebliche Probleme vermeiden können, die sich in future auf Ihre Anwendung auswirken könnten.

DevOpsGuru nutzt maschinelles Lernen, um Ihre Betriebsdaten sowie Anwendungsmetriken und Ereignisse zu analysieren und Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Sie werden benachrichtigt, wenn DevOps Guru ein betriebliches Problem oder Risiko feststellt. Für jedes Problem präsentiert DevOps Guru intelligente Empfehlungen zur Lösung aktueller und prognostizierter future betrieblicher Probleme.

Informationen zu den ersten Schritten finden Sie unter Wie fange ich mit DevOps Guru an?

Wie funktioniert DevOps Guru?

Der DevOps Guru-Workflow beginnt, wenn Sie die Abdeckung und die Benachrichtigungen konfigurieren. Nachdem Sie DevOps Guru eingerichtet haben, beginnt Guru mit der Analyse Ihrer Betriebsdaten. Wenn es ungewöhnliches Verhalten erkennt, erstellt es einen Einblick, der Empfehlungen und Listen mit Kennzahlen, Protokollgruppen und Ereignissen enthält, die sich auf das Problem beziehen. DevOpsGuru benachrichtigt dich über jeden Einblick. Wenn Sie diese Option aktiviert haben AWS Systems Manager OpsCenter, OpsItem wird eine erstellt, sodass Sie Systems Manager verwenden können OpsCenter , um die Bearbeitung Ihrer Erkenntnisse zu verfolgen und zu verwalten. Jeder Einblick enthält Empfehlungen, Metriken, Protokollgruppen und Ereignisse im Zusammenhang mit anomalem Verhalten. Verwenden Sie Informationen in Form von Erkenntnissen, die Ihnen helfen, das anomale Verhalten zu verstehen und zu beheben.

DevOpsGuru-Workflow auf hohem NiveauWeitere Informationen zu den drei allgemeinen Workflow-Schritten finden Sie unter. Weitere Informationen Detaillierter DevOps Guru-Arbeitsablauf zum detaillierteren DevOps Guru-Workflow, einschließlich seiner Interaktion mit anderen AWS Diensten, finden Sie unter.

Themen

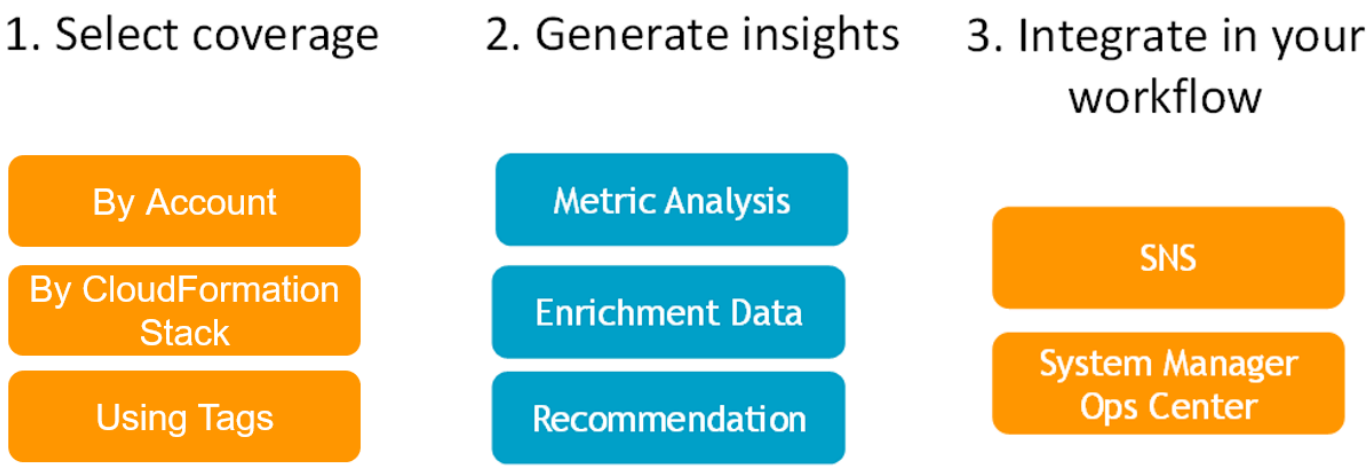
- DevOpsGuru-Workflow auf hohem Niveau
- Detaillierter DevOps Guru-Arbeitsablauf

DevOpsGuru-Workflow auf hohem Niveau

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

1. Geben Sie die Reichweite von DevOps Guru an, indem Sie dem Unternehmen mitteilen, 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 Ihre Abläufe 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 er einen Eingang erstellt AWS Systems Manager OpsCenter , OpsItem der dir hilft, deine Erkenntnisse nachzuverfolgen. Das folgende Diagramm zeigt diesen Arbeitsablauf auf hoher Ebene.



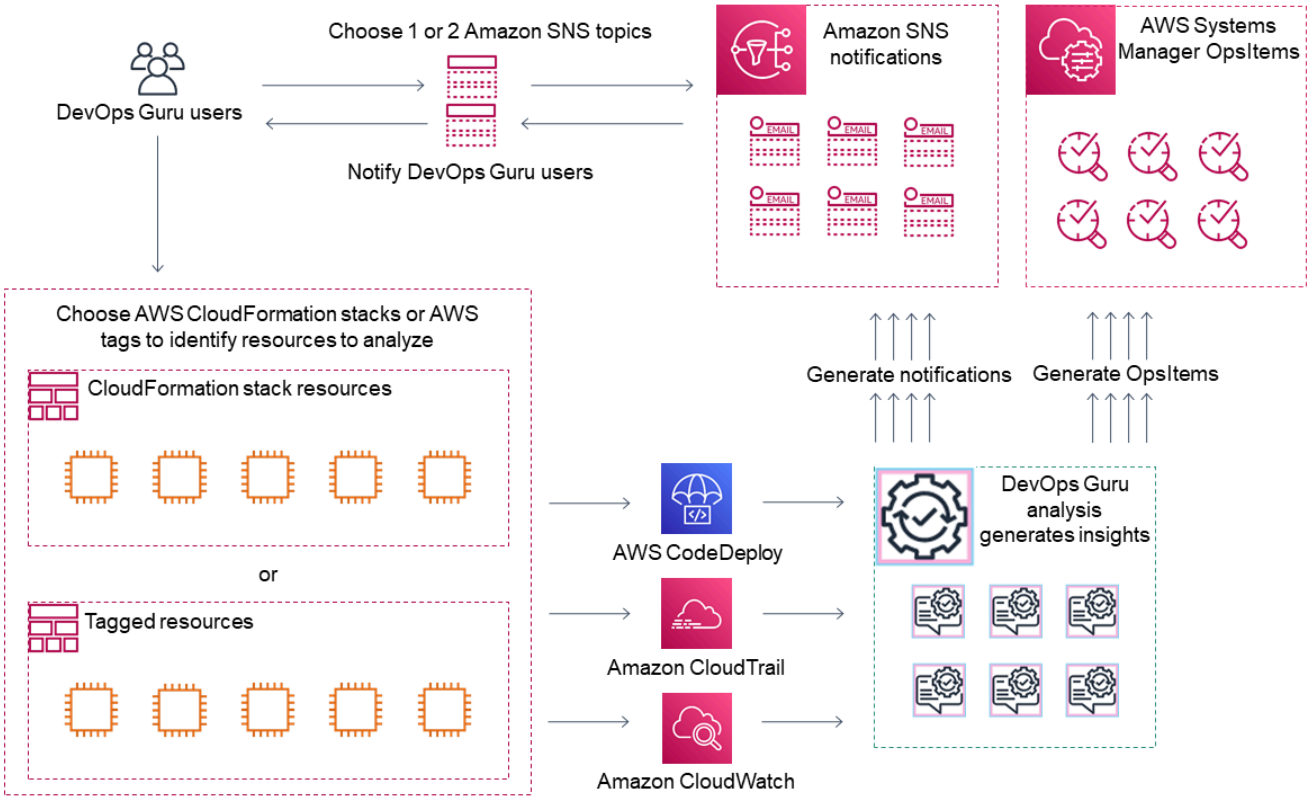
1. Im ersten Schritt wählen Sie Ihren Versicherungsschutz aus, indem Sie angeben, welche AWS Ressourcen in Ihrem AWS Konto analysiert werden. DevOpsGuru kann alle Ressourcen in einem AWS Konto abdecken oder analysieren, oder du kannst AWS CloudFormation Stapel oder AWS Tags verwenden, um eine Teilmenge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

geschäftskritischen Anwendungen, Workloads und Microservices handelt. 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. Du kannst dir die Erkenntnisse und die darin enthaltenen Empfehlungen und zugehörigen Informationen in der DevOps Guru-Konsole ansehen. 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 festgestellt 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 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 bei der Bereitstellung von Ressourcen und um Konfigurationsänderungen handeln.
   - Wenn Sie dies verwenden AWS CodeDeploy, analysiert DevOps Guru Bereitstellungsereignisse, um Erkenntnisse zu gewinnen. Ereignisse für alle Arten von CodeDeploy Bereitstellungen (lokaler Server, EC2 Amazon-Server, Lambda oder Amazon EC2) werden analysiert.
   - Wenn DevOps Guru ein bestimmtes Muster findet, generiert er eine oder mehrere Empfehlungen, um das identifizierte Problem zu mildern oder zu beheben. Die Empfehlungen werden in einem einzigen Einblick 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 zu lösen und zu verstehen.
3. Im dritten Schritt integriert DevOps Guru die Benachrichtigung über Erkenntnisse in Ihren Arbeitsablauf, um Ihnen zu helfen, Probleme zu lösen und sie schnell zu lösen.
   - In Ihrem AWS Konto generierte Erkenntnisse werden unter dem Thema Amazon Simple Notification Service (Amazon SNS) veröffentlicht, das Sie bei der DevOps Guru-Einrichtung ausgewählt haben. So wirst du 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-Einrichtung aktiviert hast, erstellt jeder Einblick eine entsprechende Information OpsItem , die 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 verschiedene AWS Dienste integrieren, darunter Amazon CloudWatch AWS CloudTrail, Amazon Simple Notification Service und AWS Systems Manager. Das folgende Diagramm zeigt einen detaillierten Workflow, der auch zeigt, wie er mit anderen AWS Diensten funktioniert.



Dieses Diagramm zeigt ein Szenario, in dem die DevOps Guru-Abdeckung durch die AWS Ressourcen bestimmt wird, die in AWS CloudFormation Stapeln oder mithilfe von AWS Tags definiert sind. Wenn keine Stapel oder Tags ausgewählt wurden, 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 SNS-Themen an, die verwendet werden, um Sie über wichtige DevOps Guru-Ereignisse zu informieren, z. B. wenn ein Insight erstellt wird. Als Nächstes können Sie AWS CloudFormation Stacks angeben, die die Ressourcen definieren, die Sie analysieren möchten. Sie können Systems Manager auch so einrichten, dass er OpsItem für jeden Einblick eine generiert, 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 ausgelöst werden, sowie mit den CloudWatch Metriken zusammenhängenden AWS CloudTrail Daten. Wenn Ihr Betrieb CodeDeploy Bereitstellungen umfasst, 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 beheben.
3. Nachdem jeder Einblick erstellt wurde, sendet DevOps Guru eine Benachrichtigung mit dem Amazon SNS SNS-Thema oder den Themen, die bei der DevOps Guru-Einrichtung angegeben wurden. Wenn du DevOps Guru aktiviert hast, einen OpsItem im Systems Manager zu generieren OpsCenter, löst jede Erkenntnis auch einen neuen Systems Manager ausOpsItem. Sie können 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 lesen DevOpsGuru-Konzepte.
2. Richten Sie Ihr AWS Konto AWS CLI, den und einen Administratorbenutzer ein, indem Sie die Schritte unter befolgenAmazon DevOps Guru einrichten.
3. Verwenden Sie DevOps Guru und folgen Sie den Anweisungen unterErste Schritte mit DevOps Guru.

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

Um Amazon DevOps Guru zu deaktivieren, sodass keine Gebühren mehr 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 Keine aus. Du musst dies für jedes AWS Konto und jede Region tun, in der DevOps Guru Ressourcen analysiert.

> **Note**
>
> Wenn du deinen Versicherungsschutz so änderst, dass keine Ressourcen mehr analysiert werden, können dir weiterhin geringfügige Gebühren anfallen, wenn du bestehende Erkenntnisse überprüfst, 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-Konzepte

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

Themen

- 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 DevOps Guru einrichten.

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 AWS 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 AWS 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 Art 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	Metriken
AWS Lambda	Erkennen Sie Latenz- oder Daueranom alien für Lambda-Funktionen, die auf verschiedene Ursachen wie Kaltstarts, erhöhte Anfragen, Downstrea m-Drosselung oder Codebereitstellung en zurückzuführen sind. Empfehlen Sie Möglichkeiten zur schnellen Problembe hebung.	Codebereitstellung : Die Amazon API Gateway Latenz wird durch einen Anstieg der Lambda-Latenz nach einer kürzlichen Lambda-Code-Bereit stellung beeinträc htigt. Downstream-Drosselung: Der Bediener reduziert e die Kapazität der Leseeinheiten für DynamoDB, was zu vermehrten Wiederhol ungsversuchen führte. Dies führt zu einer Drosselung. Kaltstart : Die Lambda-Fu nktion ist unzureich end bereitgestellt, sodass Lambda länger braucht, wenn Anfragen gestellt werden.	Dauer Drosselungen

Beispiel für einen Anwendungsfall für proaktive Einblicke:

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

Service-Name	Anwendungsfall	Metriken
	erreicht wird. Empfohlene Maßnahme: Wenn Sie den Modus für bereitgestellte 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-Kapazitätsmodus, um pro Leseanforderung zu zahlen und nur für das zu bezahlen, was tatsächlich genutzt wird. Erkennungszeit: 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

Amazon DevOps Guru einrichten

Erledigen Sie die Aufgaben in diesem Abschnitt, um Amazon DevOps Guru zum ersten Mal einzurichten. Wenn Sie bereits ein AWS Konto haben, wissen, welches AWS Konto oder welche Konten Sie analysieren möchten, und ein Amazon Simple Notification Service-Thema haben, das Sie für Insight-Benachrichtigungen verwenden können, können Sie direkt mit dem nächsten Schritt fortfahrenErste Schritte mit DevOps Guru.

Optional können Sie Quick Setup, eine Funktion von AWS Systems Manager, verwenden, um DevOps Guru einzurichten und seine Optionen schnell zu konfigurieren. Du kannst Quick Setup verwenden, um DevOps Guru für ein eigenständiges Konto oder eine Organisation einzurichten. Um mit Quick Setup in Systems Manager DevOps Guru für eine Organisation einzurichten, müssen Sie die folgenden Voraussetzungen erfüllen:

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

Informationen zur Einrichtung von DevOps Guru mithilfe von Quick Setup finden Sie unter DevOps Guru mit Quick Setup konfigurieren im AWS Systems Manager Benutzerhandbuch.

Gehen Sie wie folgt vor, um DevOps Guru ohne Quick Setup einzurichten.

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

Schritt 1 — Melde dich an für AWS

Melde dich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

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

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

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

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

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

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

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

Weiteren Benutzern Zugriff zuweisen

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

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

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

Schritt 2 — Bestimmen Sie den Versicherungsschutz für Guru DevOps

Ihre Grenzabdeckung bestimmt, welche AWS Ressourcen von Amazon DevOps Guru auf anomales Verhalten hin analysiert werden. Wir empfehlen Ihnen, Ihre Ressourcen in Ihren betrieblichen Anwendungen zu gruppieren. Alle Ressourcen innerhalb Ihrer Ressourcengrenze sollten eine oder mehrere Ihrer Anwendungen umfassen. Wenn Sie über eine betriebliche Lösung verfügen, sollte Ihre Deckungsgrenze alle Ressourcen umfassen. Wenn Sie über mehrere Anwendungen verfügen, wählen Sie die Ressourcen aus, aus denen jede Lösung besteht, und gruppieren Sie sie mithilfe von AWS CloudFormation Stacks oder AWS Tags. Alle von Ihnen angegebenen kombinierten Ressourcen, unabhängig davon, ob sie eine oder mehrere Anwendungen definieren, werden von DevOps Guru analysiert und bilden die Deckungsgrenze.

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

- Entscheiden Sie sich dafür, dass Ihre AWS Region und Ihr Konto Ihre Versorgungsgrenze definieren. Mit dieser Option analysiert DevOps Guru alle Ressourcen in deinem Konto und deiner Region. Dies ist eine gute Option, wenn Sie Ihr Konto nur für eine Anwendung verwenden.
- Verwenden Sie AWS CloudFormation Stacks, um die Ressourcen in Ihrer betrieblichen Anwendung zu definieren. AWS CloudFormation Vorlagen definieren und generieren Ihre Ressourcen für Sie. Geben Sie bei der Konfiguration von DevOps Guru die Stacks an, aus denen Ihre Anwendungsressourcen erstellt werden. Sie können Ihre Stacks jederzeit aktualisieren. Alle Ressourcen in den Stacks, die Sie auswählen, definieren Ihre Grenzabdeckung. Weitere Informationen finden Sie unter Verwenden von AWS CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- Verwenden Sie AWS Tags, um AWS Ressourcen in Ihren Anwendungen zu spezifizieren. DevOpsGuru 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 einem Tag-Wert. Sie können einen Tag-Schlüssel und mit diesem Schlüssel einen oder mehrere Werte angeben. Verwenden Sie einen Wert für alle Ressourcen in einer Ihrer Anwendungen. Wenn Sie mehrere Anwendungen haben, verwenden Sie ein Tag mit demselben Schlüssel für alle Anwendungen und gruppieren Sie die Ressourcen anhand der Werte der Tags zu Ihren Anwendungen. Alle Ressourcen mit den von Ihnen ausgewählten Tags bilden die Deckungsgrenze für DevOps Guru. Weitere Informationen

finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

Wenn Ihre Grenzabdeckung Ressourcen umfasst, die mehr als eine Anwendung ausmachen, können Sie Ihre Erkenntnisse mithilfe von Tags filtern, um sie jeweils für eine Anwendung anzuzeigen. Weitere Informationen finden Sie unter Schritt 4 unterEinblicke 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-Preise.

Schritt 3 — Identifizieren Sie Ihr Amazon SNS SNS-Benachrichtigungsthema

Sie verwenden ein oder zwei Amazon SNS SNS-Themen, um Benachrichtigungen über wichtige DevOps Guru-Ereignisse zu generieren, z. B. wenn ein Insight erstellt wird. Dadurch wird sichergestellt, dass Sie so schnell wie möglich über Probleme informiert werden, die DevOps Guru entdeckt. Halte deine Themen bereit, wenn du DevOps Guru einrichtest. Wenn Sie Guru mit der DevOps Guru-Konsole einrichten DevOps, geben Sie ein Benachrichtigungsthema mit seinem Namen oder seinem Amazon-Ressourcennamen (ARN) an. Weitere Informationen finden Sie unter DevOpsGuru aktivieren. Sie können die Amazon SNS 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 DevOps Guru über die DevOps Guru-Konsole aktivieren. Weitere Informationen finden Sie unter Thema erstellen im Amazon Simple Notification Service Developer Guide.

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.

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 AWS 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 AWS 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 AWS 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 AWS CloudFormation Benutzerhandbuch.
     3. (Optional) Wenn Sie einen AWS 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 DevOps Guru beginnen können, damit Amazon Guru die Betriebsdaten und Kennzahlen Ihrer Anwendung analysieren kann, um Erkenntnisse zu gewinnen.

Themen

- Schritt 1: Richten Sie sich ein
- Schritt 2: DevOps Guru aktivieren
- Schritt 3: Geben Sie den Umfang Ihrer DevOps Guru-Ressourcen an

Schritt 1: Richten Sie sich ein

Bevor Sie beginnen, bereiten Sie sich vor, indem Sie die unter aufgeführten Schritte durchgehenAmazon DevOps Guru einrichten.

Schritt 2: DevOps Guru aktivieren

Um Amazon DevOps Guru für die erste Verwendung zu konfigurieren, müssen Sie auswählen, wie Sie DevOps Guru einrichten möchten. Sie können entweder Anwendungen in Ihrem gesamten Unternehmen oder Anwendungen in Ihrem Girokonto überwachen.

Sie können entweder Ihre Anwendungen unternehmensweit überwachen oder DevOps Guru ausschließlich für das Girokonto aktivieren. In den folgenden Verfahren werden verschiedene Möglichkeiten beschrieben, DevOps Guru je nach Ihren Bedürfnissen einzurichten.

Überwachen Sie Konten in Ihrer gesamten Organisation

Wenn Sie Anwendungen in Ihrer gesamten Organisation überwachen möchten, melden Sie sich bei Ihrem Organisationsverwaltungskonto an. Sie können optional ein Mitgliedskonto für eine Organisation als delegierter Administrator einrichten. Sie können jeweils nur einen delegierten Administrator haben und die Administratoreinstellungen später ändern. Sowohl das Verwaltungskonto als auch das delegierte Administratorkonto, das Sie eingerichtet haben, haben Zugriff auf alle Erkenntnisse für alle Konten in Ihrer Organisation.

Sie können entweder mit der Konsole kontenübergreifenden Support für Ihr Unternehmen hinzufügen, oder Sie können dies mithilfe der AWS CLI tun.

Mit der DevOps Guru-Konsole an Bord

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

Verwenden Sie die Konsole, damit DevOps Guru aggregierte Erkenntnisse einsehen kann

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie als Setup-Typ die Option „Anwendungen in Ihren Organisationen überwachen“.
3. Wählen Sie aus, welches Konto Sie als delegierter Administrator verwenden möchten. Wählen Sie dann Delegierten Administrator registrieren aus. Dadurch erhalten Sie Zugriff auf eine konsolidierte Ansicht für jedes Konto, für das DevOps Guru aktiviert ist. Der delegierte Administrator hat eine konsolidierte Ansicht aller Erkenntnisse und Kennzahlen von DevOps Guru in Ihrem Unternehmen. Sie können andere Konten mit SSM Quick Setup oder AWS CloudFormation Stack-Sets aktivieren. Weitere Informationen zur Schnelleinrichtung findest du unter DevOps Guru mit Quick Setup konfigurieren. Weitere Informationen zur Einrichtung mit Stack-Sets finden Sie unter Arbeiten mit Stacks im AWS CloudFormation Benutzerhandbuch undSchritt 2 — Bestimmen Sie den Versicherungsschutz für Guru DevOps. undVerwenden von AWS CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

Mit der AWS CLI an Bord

Sie können die AWS CLI verwenden, um DevOps Guru die Anzeige aggregierter Erkenntnisse zu ermöglichen. 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	Beschreibung
`create-service-linked-role`	Erteilt DevOps Guru die Erlaubnis, Informati onen über Ihre Organisation zu sammeln. Fahren Sie nicht fort, wenn dieser Schritt nicht erfolgreich ist.
`enable-aws-service-access`	Integriert Ihre Organisation 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 AWS Girokonto zu überwachen, wählen Sie aus, welche AWS Ressourcen in Ihrem Konto und Ihrer Region abgedeckt oder analysiert werden, und geben Sie ein oder zwei Amazon Simple Notification Service-Themen an, die verwendet werden, um Sie zu benachrichtigen, wenn ein Insight erstellt wird. Sie können diese Einstellungen später bei Bedarf aktualisieren.

Ermöglichen Sie DevOps Guru, Anwendungen in Ihrem aktuellen AWS Konto zu überwachen

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Wählen Sie als Setup-Typ die Option Anwendungen im aktuellen AWS Konto überwachen aus.
3. Wählen Sie unter DevOpsGuru Analysis Coverage eine der folgenden Optionen aus.
   - Analysieren Sie alle AWS Ressourcen im AWS Girokonto: DevOps Guru analysiert alle AWS Ressourcen in Ihrem Konto.
   - Wählen Sie AWS-Ressourcen für die spätere Analyse aus: Sie wählen Ihre Analysegrenze später. Weitere Informationen erhalten Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru und Aktualisierung der Berichterstattung über Ihre AWS Analysen in Guru DevOps.

DevOpsGuru kann jede Ressource analysieren, die mit dem von ihm unterstützten AWS Konto verknüpft ist. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unter Amazon DevOps Guru-Preise.

4. Sie können bis zu zwei Themen hinzufügen. DevOpsGuru verwendet das Thema oder die Themen, um dich über wichtige DevOps Guru-Ereignisse zu informieren, z. B. über die Entstehung neuer Erkenntnisse. Wenn Sie jetzt kein Thema angeben, können Sie später eines hinzufügen, indem Sie im Navigationsbereich Einstellungen wählen.

   a. Wählen Sie unter Geben Sie ein Amazon SNS SNS-Thema ein Thema aus, das Sie verwenden möchten.

   b. 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 SNS-Themen.

5. Wählen Sie Enable (Aktivieren) aus.

Um Amazon DevOps Guru für die erste Nutzung zu konfigurieren, müssen Sie auswählen, welche AWS Ressourcen in Ihrem Konto und Ihrer Region abgedeckt oder analysiert werden, und ein oder zwei Amazon Simple Notification Service-Themen angeben, die verwendet werden, um Sie zu benachrichtigen, wenn ein Insight erstellt wird. Sie können diese Einstellungen später bei Bedarf aktualisieren.

Schritt 3: Geben Sie den Umfang Ihrer DevOps Guru-Ressourcen an

Wenn Sie später, als Sie DevOps Guru aktiviert haben, AWS Ressourcen angeben möchten, müssen Sie die AWS CloudFormation Stacks in Ihrem AWS Konto auswählen, aus denen die Ressourcen erstellt werden, die Sie analysieren möchten. Ein AWS CloudFormation Stapel ist eine Sammlung von AWS Ressourcen, die du als eine Einheit verwaltest. Sie können einen oder mehrere Stapel verwenden, um alle Ressourcen einzubeziehen, die für die Ausführung Ihrer betrieblichen Anwendungen erforderlich sind, und diese dann so spezifizieren, dass sie von DevOps Guru analysiert werden. Wenn Sie keine Stacks angeben, analysiert DevOps Guru alle AWS Ressourcen in Ihrem Konto. Weitere Informationen finden Sie unter Arbeiten mit Stacks im AWS CloudFormation Benutzerhandbuch undErmitteln Sie den Versicherungsschutz für DevOps Guru. und. Verwenden von AWS 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-Preise.

Geben Sie den Umfang der DevOps Guru-Ressourcen an

1. Öffnen Sie die Amazon DevOps Guru-Konsole unter https://console.aws.amazon.com/devops-guru/.
2. Erweitern Sie Einstellungen im Navigationsbereich.
3. Wählen Sie unter Analysierte Ressourcen die Option Analysierte Ressourcen 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.
   - Wählen Sie CloudFormation Stacks, wenn DevOps Guru die Ressourcen analysieren soll, die sich in Stacks Ihrer Wahl 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.

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

- 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.

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 Management Console.

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 von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

> **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 AWS 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 AWS CloudFormation Stack die Ressource erstellt hat, die die Metrik ausgegeben hat, den Namen der Ressource und ihren Typ. Nicht alle Metriken sind einem AWS 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.

Grafisch dargestellte Anomalien

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 AWS 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 for 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 for 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 aktiviertem Performance Insights bietet DevOps Guru for RDS detaillierte, datenbankspezifische Analysen von Leistungsproblemen und empfiehlt Korrekturmaßnahmen.

Themen

- Überblick über Guru for RDS DevOps
- DevOpsGuru für RDS aktivieren
- Analysieren 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 für RDS
- Schlüsselkonzepte für die Optimierung der Datenbankleistung
- Die wichtigsten Konzepte von DevOps Guru for RDS
- Wie funktioniert Guru for RDS DevOps
- Unterstützte Datenbank-Engines

Vorteile von DevOps Guru für RDS

Wenn Sie für eine Amazon RDS-Datenbank verantwortlich sind, wissen Sie möglicherweise nicht, dass ein Ereignis oder eine Regression stattfindet, die 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 Techniken und Techniken des maschinellen Lernens, 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 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 Betriebssystemmetriken mit erweiterter Überwachung 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 kann so dazu führen, dass Datenbankressourcen blockiert werden. DevOps Guru gibt Ihnen dann Empfehlungen, die Ihnen helfen, Probleme zu lösen, bevor sie zu größeren Problemen werden.

Fundierte Kenntnisse der Amazon-Ingenieure und Machine Learning

DevOpsGuru for RDS setzt auf maschinelles Lernen (ML) und erweiterte statistische Analysen, um Leistungsprobleme zu erkennen und Engpässe zu beheben. Die Datenbankingenieure von Amazon haben zur Entwicklung der Ergebnisse von DevOps Guru for RDS beigetragen, die auf viele Jahre der Verwaltung von Hunderttausenden von Datenbanken zurückzuführen sind. Durch die Nutzung dieses kollektiven Wissens kann DevOps Guru for RDS Ihnen bewährte Verfahren vermitteln.

Schlüsselkonzepte 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 Overview of Performance Insights im Amazon Aurora Aurora-Benutzerhandbuch oder Overview of Performance Insights im Amazon RDS-Benutzerhandbuch.

Themen

- Metriken
- Problemerkennung
- DB-Last
- 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 Metriken in Echtzeit für die Datenbank und das Betriebssystem (OS) bereit, auf denen 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 einige dieser Metriken und bietet Einblicke in sie. Weitere Informationen finden Sie unter Überwachen von Metriken in einem Amazon Aurora Aurora-Cluster oder Überwachen von Metriken in einer Amazon Relational Database Service Service-Instance.

Problemerkennung

DevOpsGuru for RDS verwendet Datenbank- und Betriebssystemmetriken (OS), um kritische Probleme mit der Datenbankleistung zu erkennen, unabhängig davon, ob es sich um drohende oder

anhaltende Probleme handelt. DevOpsGuru for RDS-Problemerkennung funktioniert hauptsächlich auf zwei Arten:

- Verwendung von Schwellenwerten
- Verwendung von Anomalien

Erkennung von Problemen mit Schwellenwerten

Schwellenwerte sind die Grenzwerte, anhand derer die überwachten Messwerte bewertet werden. Sie können sich einen Schwellenwert als 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 Werte für eine bestimmte Ressource als potenziell problematisch angesehen werden. DevOpsGuru for RDS generiert dann Erkenntnisse in der DevOps Guru-Konsole, wenn neue Metrikwerte über einen bestimmten Zeitraum hinweg konsistent einen bestimmten Schwellenwert überschreiten. Die Erkenntnisse enthalten Empfehlungen, um future Auswirkungen auf die Datenbankleistung zu verhindern.

DevOpsGuru for RDS könnte beispielsweise die Anzahl der temporären Tabellen, die Festplatte verwenden, über einen Zeitraum von 15 Minuten überwachen und Erkenntnisse gewinnen, wenn die Rate temporärer Tabellen, die Festplatte pro Sekunde verwenden, 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, reichen in manchen Situationen jedoch nicht aus. Stellen Sie sich einen Fall vor, in dem Metrikwerte aufgrund eines bekannten Prozesses, wie z. B. einer täglichen Berichtsaufgabe, regelmäßig zu einem potenziell problematischen Verhalten übergehen. Da mit solchen Spitzenwerten zu rechnen ist, wäre es kontraproduktiv, Erkenntnisse und Benachrichtigungen für jeden von ihnen zu erstellen, was wahrscheinlich zu einer Übermüdung der Warnmeldungen 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 können. Um dieses Problem auszuräumen, überwacht DevOps Guru for RDS bestimmte Metriken, um zu erkennen, wann das Verhalten einer Metrik äußerst ungewöhnlich oder ungewöhnlich wird. DevOpsGuru meldet diese Anomalien dann in Insights.

DevOpsGuru for RDS könnte beispielsweise Erkenntnisse gewinnen, wenn die Datenbanklast nicht nur hoch ist, sondern auch erheblich von ihrem 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-Last

Das Schlüsselkonzept für die Datenbankoptimierung ist die Metrik zur Datenbankauslastung (DB-Load). Die DB-Auslastung gibt an, wie ausgelastet Ihre Datenbank zu einem bestimmten Zeitpunkt ist. Eine Erhöhung der Datenbanklast 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 durchschnittlichen aktiven Sitzungen (AAS) gemessen. Um AAS zu berechnen, erfasst Performance Insights die Anzahl der aktiven Sitzungen pro Sekunde. 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 zu einem bestimmten Zeitpunkt 2 Sitzungen 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, erfüllen alle 100 Mitarbeiter Bestellungen gleichzeitig. 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 Laden von Datenbanken im Amazon Aurora Aurora-Benutzerhandbuch oder Laden von Datenbanken im Amazon RDS-Benutzerhandbuch.

Warteereignisse

Ein Warteereignis ist eine Art von Datenbankinstrumentierung, die Ihnen mitteilt, auf welche Ressource eine Datenbanksitzung wartet, sodass 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. Sitzungen verbrauchen beispielsweise CPU, wenn sie Arbeitsspeicher durchsuchen, eine Berechnung durchführen oder prozeduralen Code ausführen. Wenn Sitzungen keine CPU verbrauchen, warten sie möglicherweise darauf, dass eine Datendatei gelesen oder 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 für 90% der Datenbanklast verantwortlich sein. 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 ein Einkaufswagen ist möglicherweise nicht verfügbar. Oder das System, mit dem der Bestellstatus eingegeben wurde, ist möglicherweise langsam. Je länger der Mitarbeiter wartet, desto länger dauert es, bis die Bestellung ausgeführt wird. Warten ist ein natürlicher Teil des Lagerablaufs, aber wenn die Wartezeit zu lang wird, 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 Aurora-Benutzerhandbuch.

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

Die wichtigsten Konzepte von 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 erkannt wurden und die unerwartet oder ungewöhnlich sind.

Eine Erkenntnis hat einen Schweregrad von hoch, mittel oder niedrig. Der Schweregrad der Erkenntnisse wird durch die schwerwiegendste Anomalie bestimmt, die zur Erstellung der Erkenntnisse beigetragen hat. Wenn die Erkenntnis AWS-ECS_ MemoryUtilization _and_others beispielsweise eine Anomalie mit niedrigem Schweregrad und eine weitere mit hohem Schweregrad umfasst, ist der Gesamtschweregrad der Erkenntnis hoch.

Wenn bei Amazon RDS-DB-Instances Performance Insights 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 Grundlage für Datenbankmetrikwerte. DevOpsGuru for RDS vergleicht dann die aktuellen Metrikwerte mit der historischen Basislinie.

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 Kennzahlen, damit Sie Probleme beheben können, bevor sie zu größeren Problemen werden.

Jede Seite mit proaktiven Erkenntnissen enthält Details zu einer Anomalie.

Reaktive Einblicke

Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Sie enthält Anomalien mit Empfehlungen, zugehörigen Kennzahlen und Ereignissen, damit Sie die Probleme sofort 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. Beispielsweise könnte der Insight AWS-ECS_ MemoryUtilization _and_others mehrere metrische Anomalien aufweisen, von denen eine die Datenbanklast (DB-Last) für die Ressource AWS/RDS ist.

Innerhalb eines Insights kann die Anomalie 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 auf der Seite mit den Anomaliedetails in der Guru-Konsole im Abschnitt „Verwandte Metriken“ angezeigt. DevOps 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 Warteschlange für die CPU-Ausführung oder die CPU-Auslastung liegen über dem Normalwert.
- Niedriger Datenbankspeicher — Prozesse verfügen nicht über genügend Arbeitsspeicher.
- Anstieg der Datenbankverbindungen — Die Anzahl der Datenbankverbindungen liegt über dem Normalwert.

Empfehlungen

Für jede Einsicht gibt es mindestens einen Vorschlag für eine Aktion. Die folgenden Beispiele sind Empfehlungen, die DevOps Guru für RDS generiert hat:

- Optimieren Sie SQL, IDs `list_of_IDs` um die CPU-Auslastung zu reduzieren, oder aktualisieren Sie den Instance-Typ, um die CPU-Kapazität zu erhöhen.
- Überprüfen Sie den damit verbundenen Anstieg der aktuellen Datenbankverbindungen. Erwägen Sie, die Einstellungen des Anwendungspools zu optimieren, um eine häufige dynamische Zuweisung neuer Datenbankverbindungen zu vermeiden.
- Suchen Sie nach SQL-Anweisungen, die zu viele Speicheroperationen ausführen, wie z. B. Sortierung im Speicher oder große Verknüpfungen.
- Untersuchen Sie die hohe I/O-Auslastung für das folgende 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 zu sehen, was die Ursache für den Anstieg der Datenbank-Arbeitslast ist.

- Erwägen Sie die Aktivierung des MySQL-Leistungsschemas.
- 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 „Inaktiv in Transaktion“ befand.

Wie funktioniert Guru for RDS DevOps

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

Themen

- Datenerfassung und Analyse
- Veröffentlichung von 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 Leistungskennzahl ist`DBLoad`. DevOpsGuru for RDS verwendet Performance Insights 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 Aurora-Benutzerhandbuch oder Überwachen der DB-Auslastung mit Performance Insights auf Amazon RDS im Amazon RDS-Benutzerhandbuch.

DevOpsGuru for RDS verwendet maschinelles Lernen und fortschrittliche 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 von Anomalien

Ein Problem mit der Datenbankleistung, z. B. eine hohe Datenbanklast, kann die Servicequalität für Ihre Datenbank beeinträchtigen. Wenn DevOps Guru ein Problem in einer RDS-Datenbank entdeckt, veröffentlicht Guru einen Einblick im Dashboard. Die Erkenntnis enthält eine Anomalie für die Ressource AWS/RDS.

Wenn Performance Insights für Ihre Instances aktiviert ist, beinhaltet die Anomalie eine detaillierte Analyse des Problems. DevOps Guru for RDS empfiehlt Ihnen außerdem, eine Untersuchung oder bestimmte Korrekturmaßnahmen durchzuführen. 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 idle-in-transaction.

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 Aurora-Benutzerhandbuch.

Amazon Aurora mit PostgreSQL-Kompatibilität

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

Kompatibilität mit Amazon RDS for PostgreSQL

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

DevOpsGuru meldet Anomalien und führt grundlegende Analysen für andere Datenbank-Engines durch. 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 finden 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 Sichtbarkeit AWS CloudTrail 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 von Zugriffsrichtlinien für DevOps Guru for RDS
- Amazon RDS-DB-Instances zu Ihrer DevOps Guru-Abdeckung hinzufügen

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 Sie Einblicke nach Ressourcentyp anzeigen, weist Sie 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 unten auf der Seite im Abschnitt Empfehlungen die Option Amazon RDS Performance Insights aktivieren aus.

Einstellungen

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

Weitere Informationen finden Sie unter Performance Insights ein- und ausschalten im Amazon Aurora Aurora-Benutzerhandbuch oder Performance Insights ein- und ausschalten im Amazon RDS-Benutzerhandbuch.

Konfiguration von Zugriffsrichtlinien für DevOps Guru for RDS

Damit ein Benutzer auf DevOps Guru for RDS zugreifen kann, muss er über Berechtigungen gemäß 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 von Zugriffsrichtlinien für Performance Insights im Amazon Aurora Aurora-Benutzerhandbuch oder Konfiguration von Zugriffsrichtlinien für Performance Insights im Amazon RDS-Benutzerhandbuch.

Amazon RDS-DB-Instances zu Ihrer DevOps Guru-Abdeckung hinzufügen

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

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

- Aktiviere DevOps Guru auf Kontoebene. Dies 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 AWS CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- Kennzeichnen 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 Erkenntnisse zu sehen, die mit Ihrer Anwendung erstellt wurden. Um nur Erkenntnisse zu sehen, die von den Amazon RDS-Ressourcen in Ihrer Anwendung generiert wurden, fügen Sie einen Wert hinzu, z. B. `Devops-guru-rds` zu Ihren Amazon RDS-Ressourcen-Tags. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.

  > **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”.

Analysieren von Anomalien in Amazon RDS

Wenn DevOps Guru for RDS eine Performance-Anomalie im Dashboard veröffentlicht, führen Sie in der Regel die folgenden Schritte aus:

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

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

   Weitere Informationen erhalten Sie unter Anzeige reaktiver Anomalien und Proaktive Anomalien anzeigen.
3. Beantworten Sie DevOps Guru für RDS-Empfehlungen.

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

   Weitere Informationen finden Sie unter Überwachen von Metriken in einem Amazon Aurora Aurora-DB-Cluster im Amazon Aurora Aurora-Benutzerhandbuch und Überwachen 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 kannst du einen Einblick aus der Liste auswählen, um eine detaillierte Seite mit Kennzahlen, Empfehlungen und weiteren Informationen zu diesem Einblick anzuzeigen.

Um sich 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.
3. Wählen Sie die Registerkarte Reaktiv, um reaktive Einblicke anzuzeigen, oder wählen Sie Proactive, um proaktive Einblicke anzuzeigen.

4. Wählen Sie den Namen eines Einblicks und priorisieren Sie ihn nach Status und Schweregrad.

   Die Seite mit detaillierten Erkenntnissen wird angezeigt.

Anzeige reaktiver Anomalien

In einem Einblick können Sie sich Anomalien für Amazon RDS-Ressourcen ansehen. Auf einer Seite mit reaktiven Erkenntnissen können Sie im Abschnitt Aggregierte Metriken eine Liste von Anomalien mit entsprechenden Zeitplänen einsehen. Es gibt auch Abschnitte, in denen Informationen zu Protokollgruppen und Ereignissen im Zusammenhang mit den Anomalien angezeigt werden. Für kausale Anomalien in einem reaktiven Einblick gibt es jeweils eine entsprechende Seite mit Einzelheiten zu der Anomalie.

Anzeige der detaillierten Analyse einer reaktiven RDS-Anomalie

In dieser Phase können Sie die Anomalie genauer untersuchen, um detaillierte Analysen und Empfehlungen für Ihre Amazon RDS-DB-Instances zu erhalten.

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

Um zur Seite mit den Details zur Anomalie vorzudringen

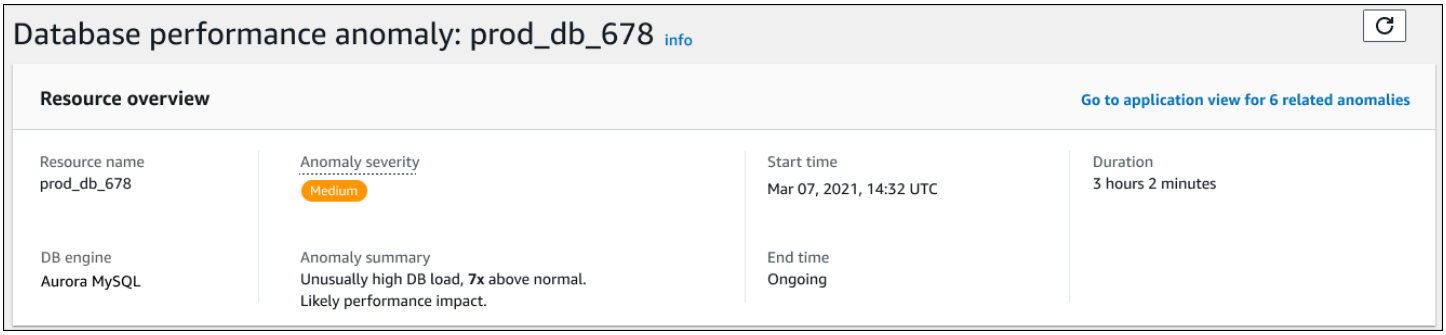
1. Suchen Sie auf der Insight-Seite nach einer aggregierten Metrik mit dem Ressourcentyp AWS/RDS.
2. Wählen Sie die Option Details anzeigen aus.

   Die Seite mit den Details zur Anomalie wird angezeigt. Der Titel beginnt mit Database Performance Anomaly und gibt der Ressource den Namen Show. 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 der Komponenten der Detailseite.

Überblick über die Ressourcen

Der obere Bereich der Detailseite ist Ressourcenübersicht. In diesem Abschnitt werden die Leistungsanomalien zusammengefasst, die bei Ihrer Amazon RDS-DB-Instance aufgetreten sind.

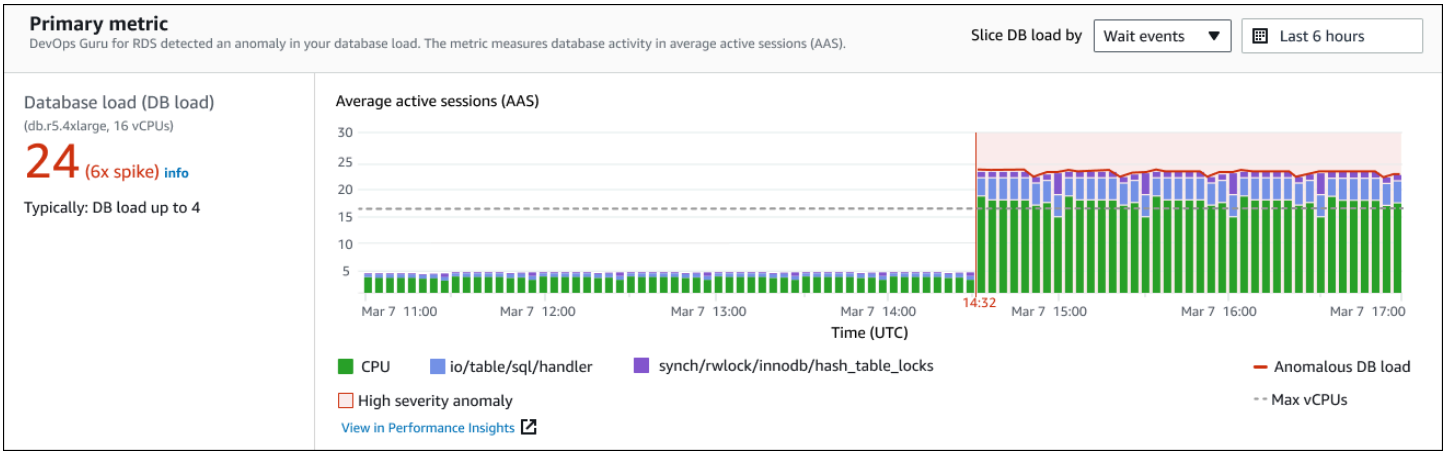


Dieser Abschnitt enthält die folgenden Felder:

- Ressourcenname — Der Name der DB-Instance, bei der die Anomalie auftritt. In diesem Beispiel hat die Ressource den Namen prod_db_678.
- DB-Engine — Der Name der DB-Instance, bei der die Anomalie aufgetreten ist. 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 Datenbanklast“.
- Startzeit und Endzeit — Die Zeit, 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 besteht die Anomalie weiterhin und tritt seit 3 Stunden und 2 Minuten auf.

Primäre Metrik

Im Abschnitt Primäre Kennzahl wird die zufällige Anomalie zusammengefasst, bei der es sich um die Anomalie auf oberster Ebene innerhalb des Insights handelt. Sie können sich die kausale Anomalie als das allgemeine Problem Ihrer DB-Instance vorstellen.



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 auf Amazon veröffentlicht CloudWatch.
- db.r5.4xlarge — Die DB-Instance-Klasse. Die Anzahl von vCPUs, die in diesem Beispiel 16 ist, entspricht der gepunkteten Linie im Diagramm der durchschnittlichen aktiven Sitzungen (AAS).
- 24 (6-fache Spitze) — Die Datenbanklast, gemessen in den durchschnittlichen aktiven Sitzungen (AAS) während des im Insight angegebenen Zeitintervalls. Somit waren zu einem beliebigen Zeitpunkt während des Zeitraums der Anomalie durchschnittlich 24 Sitzungen in der Datenbank aktiv. Die Datenbanklast beträgt das Sechsfache der normalen Datenbanklast für diese Instance.
- Typischerweise: DB-Auslastung 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.

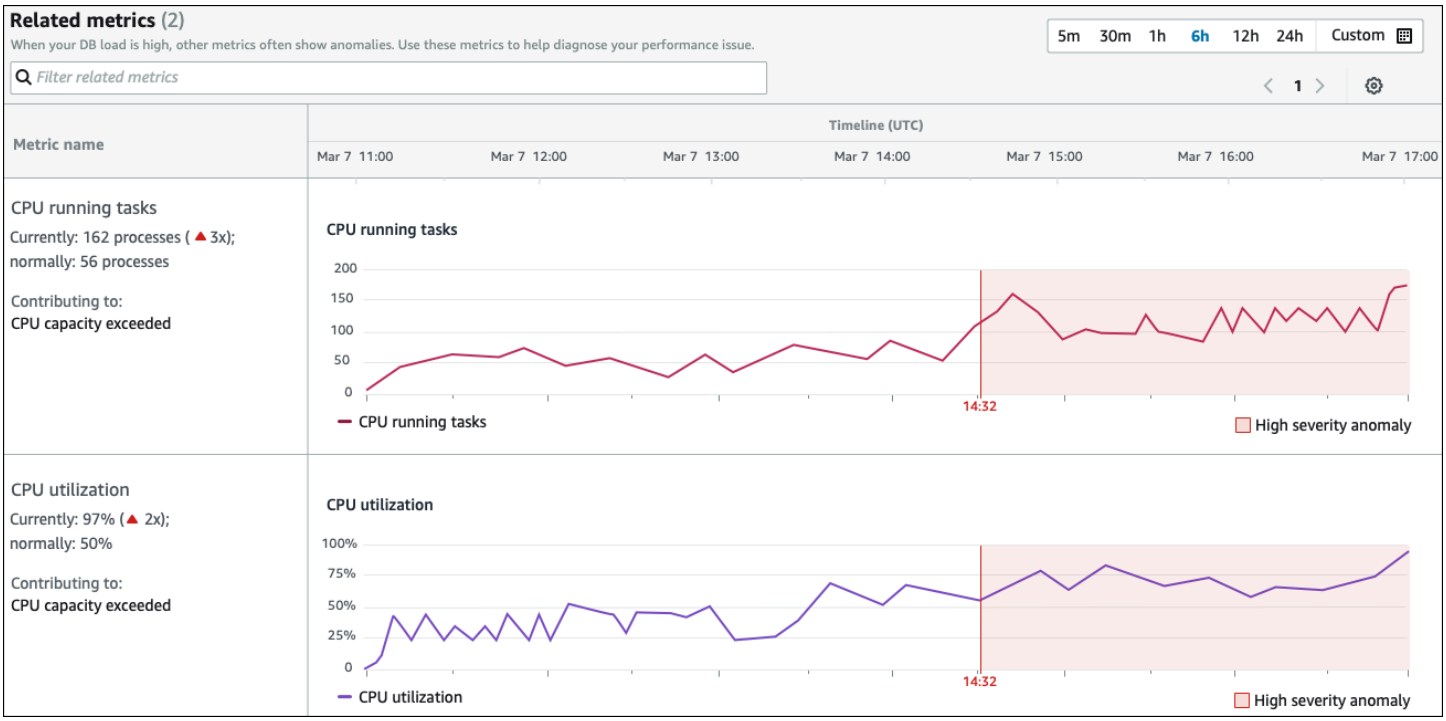
Standardmäßig ist das Lastdiagramm nach Warteereignissen unterteilt. Das bedeutet, dass für jeden Balken im Diagramm der größte farbige Bereich das Warteereignis darstellt, das am meisten zur Gesamtlast der Datenbank beiträgt. Das Diagramm zeigt den Zeitpunkt (in Rot), zu dem das Problem begann. Konzentrieren Sie sich auf die Warteereignisse, die den meisten Platz in der Leiste beanspruchen:

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

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

Verwandte Metriken

Im Abschnitt Verwandte Kennzahlen 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 mit verwandten Metriken hat zwei Spalten: Name der Metriken und Zeitleiste (UTC). Jede Zeile in der Tabelle entspricht einer bestimmten Metrik.

Die erste Spalte jeder Zeile enthält die folgenden Informationen:

- ***Name***— Der Name der Metrik. In der ersten Zeile wird die Metrik als CPU-laufende Aufgaben identifiziert.
- Aktuell — Der aktuelle Wert der Metrik. In der ersten Zeile ist der aktuelle Wert 162 Prozesse (3x).

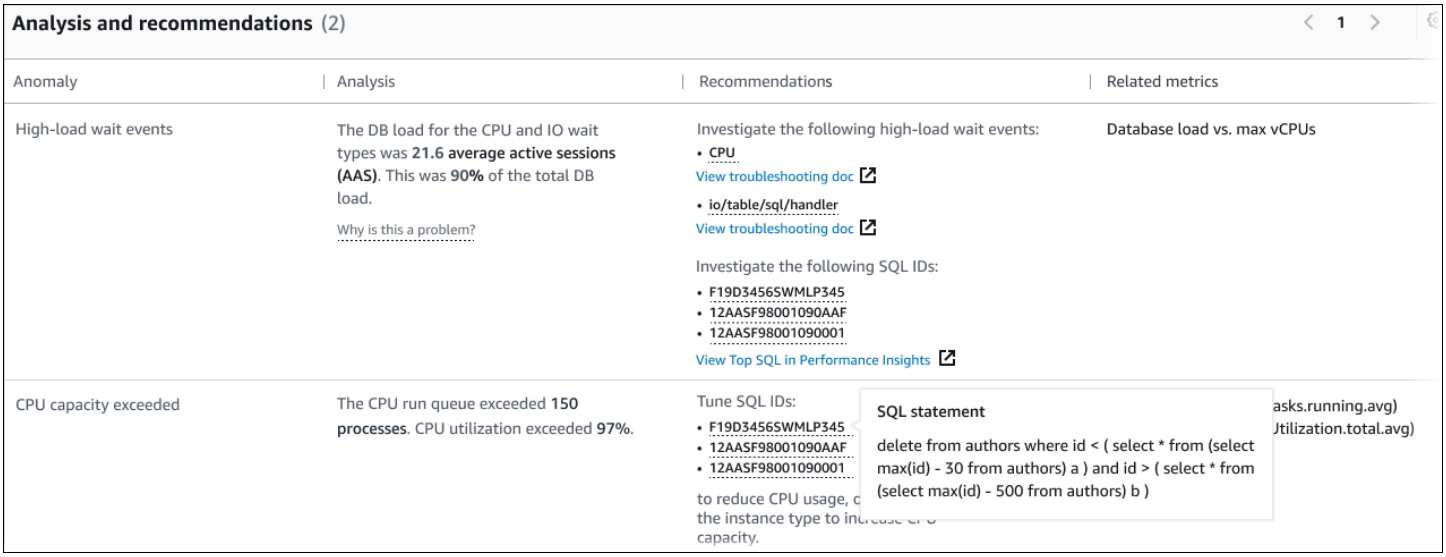
- Normalerweise — Die Basislinie dieser Metrik für diese Datenbank, wenn sie normal funktioniert. DevOpsGuru for RDS berechnet den Ausgangswert als den 95. Perzentilwert im Verlauf einer Woche. Die erste Zeile gibt an, dass 56 Prozesse normalerweise auf der CPU ausgeführt werden.
- Beitrag zu — Das mit dieser Metrik verbundene Ergebnis. In der ersten Zeile wird die Metrik „CPU running tasks“ mit der Anomalie „CPU-Kapazitätsüberschreitung“ verknüpft.

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

Analyse und Empfehlungen

Während die kausale Anomalie das Gesamtproblem beschreibt, beschreibt eine kontextuelle Anomalie ein bestimmtes Ergebnis, das untersucht werden muss. Jedes Ergebnis entspricht einer Reihe verwandter Kennzahlen.

Im folgenden Beispiel eines Abschnitts mit Analysen und Empfehlungen wurden zwei Ergebnisse für die Anomalie mit hoher Datenbanklast festgestellt.



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 bei hoher Auslastung und bei der zweiten um eine Überschreitung der CPU-Kapazität.
- Analyse — Eine detaillierte Erklärung der Anomalie.

Bei der ersten Anomalie tragen drei Wartearten 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% ausgelastet war. Somit war die CPU fast ununterbrochen ausgelastet, während durchschnittlich 150 Sitzungen darauf warteten, auf der CPU ausgeführt zu werden.

- Empfehlungen — Die vorgeschlagene Benutzerreaktion auf die Anomalie.

  Bei der ersten Anomalie empfiehlt DevOps Guru for RDS, dass Sie die Warteereignisse `cpu` untersuchen und. `io/table/sql/handler` Informationen dazu, wie Sie Ihre Datenbankleistung auf der Grundlage dieser Ereignisse optimieren können, finden Sie unter cpu und io/table/sql/handlerim Amazon Aurora 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 liefern. Weitere Informationen zu diesen Metriken finden Sie unter Metrik-Referenz für Amazon Aurora im Amazon Aurora Aurora-Benutzerhandbuch oder Metrik-Referenz für Amazon RDS im Amazon RDS-Benutzerhandbuch.

  Bei der ersten Anomalie empfiehlt DevOps Guru for RDS, die Datenbanklast 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.

Proaktive Anomalien anzeigen

In Insights können Sie Anomalien für Amazon RDS-Ressourcen anzeigen. Jeder proaktive Einblick enthält Details zu einer proaktiven Anomalie. Auf einer Seite mit proaktiven Erkenntnissen können Sie sich einen Überblick über die Erkenntnisse, detaillierte Kennzahlen zur Anomalie und Empfehlungen zur Vermeidung future Probleme ansehen. Eine proaktive Anomalie finden Sie auf der Seite mit proaktiven Erkenntnissen.

Überblick über Einblicke

Der Abschnitt Überblick über Insight enthält Einzelheiten darüber, warum der Insight erstellt wurde. Darin werden der Schweregrad des Insights sowie eine Beschreibung der Anomalie und ein Zeitrahmen für das Auftreten der Anomalie angezeigt. Außerdem wird die Anzahl der betroffenen Dienste und Anwendungen aufgeführt, die von Guru erkannt wurden. DevOps

Metriken

Der Abschnitt „Metriken“ enthält Grafiken der Anomalie. Jedes Diagramm zeigt einen Schwellenwert, der durch das Ausgangsverhalten der Ressource bestimmt wird, sowie Daten der Metrik, die seit 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 Aktionen, die Sie ergreifen können, sind in der Spalte Empfohlene benutzerdefinierte Änderung aufgeführt. Die Gründe für die Empfehlungen finden Sie im Abschnitt Warum empfiehlt DevOps Guru das? Kolumne. Weitere Informationen darüber, wie Sie auf Empfehlungen reagieren können, 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 ist ein Problem zu erwarten, das harmlos ist. Wenn Sie beispielsweise eine Testdatenbank einer extremen DB-Auslastung aussetzen, meldet DevOps Guru for RDS die Belastung als Leistungsanomalie. Sie müssen diese Anomalie jedoch nicht beheben, da sie 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 Tabelle mit Empfehlungen werden in einer Spalte die empfohlenen Maßnahmen aufgeführt. Für reaktive Einblicke ist dies die Spalte Was wir empfehlen auf einer Detailseite mit reaktiven

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

DevOpsGuru for RDS bietet eine Liste mit Empfehlungen, die mehrere potenzielle Problemszenarien abdecken. Stellen Sie nach Durchsicht dieser Liste fest, welche Empfehlung für Ihre aktuelle Situation relevanter ist, und ziehen Sie in Betracht, 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 Aktionen aus.

   DevOpsGuru for RDS empfiehlt, dass Sie einen der folgenden Schritte ausführen:

   - Führen Sie eine bestimmte Korrekturmaßnahme durch.

     DevOpsGuru for RDS könnte Ihnen beispielsweise empfehlen, die CPU-Kapazität zu aktualisieren, die Einstellungen für den Anwendungspool 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 Wartungsereignisse untersuchen. Eine Empfehlung könnte beispielsweise darin bestehen, das Wartungsereignis zu untersuchen`io/table/sql/handler`. Suchen Sie nach dem aufgelisteten Warteereignis 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. Führen Sie dann die empfohlenen Maßnahmen 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. AWS 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	Metriken
Erkennt, wenn ein großer Prozentsatz von AccountProvisionedReadCapacityUtilization und AccountProvisionedWriteCapacityUtilization aufgrund einer großen Anzahl	Amazon DynamoDB Die Kapazität des Tabellenverbrauchs für Lese- oder Schreibanforderungen erreicht die Grenzwerte auf Tabellenebene.	AccountProvisionedReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization

Amazon DynamoDB Anwendungsfall	Beispiele	Metriken
von Lese- und Schreiban forderungen verwendet wird.		
Erkennt Fehler bei der bedingten Prüfung in Amazon DynamoDB Anfragen, die darauf zurückzuführen sind, dass ein bereitgestellter Bedingungsausdruck nicht den Erwartungen in der Datenbank entspricht.	Fehler bei der bedingten Prüfung werden durch fehlerhafte Daten in Ihrer Tabelle, durch einen strikten Bedingungsausdruck oder durch Rennbedingungen verursacht.	ConditionalCheckFailedReque sts

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 CPUUtiliz ation

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 AWS 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 AWS CloudFormation Stacks, um die Ressourcen in Ihren Anwendungen anzugeben. Ein Stapel enthält Ressourcen, die mit AWS 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 von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen
- Verwenden von AWS CloudFormation Stacks zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen

Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen

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

> **Note**
>
> Wenn „Alle Kontoressourcen“ ausgewählt ist und kein Tag-Wert vorhanden ist, werden Ressourcen ohne den 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. Sie können beispielsweise Ihre Ressourcen mit dem Schlüssel `devops-guru-applications` kennzeichnen und diesen Schlüssel dann mit einem anderen Wert für jede Ihrer Anwendungen verwenden. Sie können das Tag-Schlüssel-Wert-Paar`devops-guru-applications/database`, und verwenden`devops-guru-applications/cicd`, `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 Tags

hinzu, indem Sie den AWS Dienst verwenden, zu dem sie gehören. Weitere Informationen finden Sie unter Hinzufügen von AWS Tags 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 Tag?
- Definition einer DevOps Guru-Anwendung mithilfe eines Tags
- Verwenden von Tags mit DevOps Guru
- Hinzufügen von AWS Tags zu AWS Ressourcen

Was ist ein AWS Tag?

Mithilfe von Tags 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 verknüpft sind. Sie können beispielsweise einer Amazon DynamoDB-Tabellenressource dasselbe Tag zuweisen, das Sie einer AWS Lambda Funktion zuweisen. 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 zu den AWS Ressourcen in Ihrem Konto hinzu, aus denen Ihre Anwendung besteht. Ihr Tag enthält einen Schlüssel und einen Wert. Wir empfehlen dir, jeder deiner von DevOps Guru analysierten AWS Ressourcen, die denselben Schlüssel haben, ein Tag hinzuzufügen. Verwenden Sie einen anderen Wert im Tag, um Ressourcen in Ihren Anwendungen zu gruppieren. Sie können beispielsweise allen AWS Ressourcen innerhalb Ihrer Versorgungsgrenze Tags mit dem Schlüssel `devops-guru-analysis-boundary` zuweisen. Verwenden Sie verschiedene Werte mit diesem Schlüssel, 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 verknüpfen. 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 Schlüssel mit dem Namen `devops-guru-rds` und einem Schlüssel mit dem Namen`DevOps-Guru-RDS`, die als zwei verschiedene Schlüssel fungieren. Mögliche Schlüssel/Wert-Paare in Ihrer Anwendung könnten `Devops-Guru-production-application/RDS` oder `Devops-Guru-production-application/containers` sein.

Verwenden von Tags 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 sollen. Diese Ressourcen bilden die Grenze Ihrer Ressourcenabdeckung. Sie können einen Schlüssel und null oder mehrere Werte wählen.

Um deine Tags 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. Wählen Sie „Tags“, wenn DevOps Guru alle Ressourcen analysieren soll, die die von Ihnen 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.
5. Wählen Sie Save (Speichern) aus.

Hinzufügen von AWS Tags zu AWS Ressourcen

Wenn Sie die AWS Tags angeben, die die AWS Ressourcen identifizieren, die DevOps Guru analysieren soll, wählen Sie Tags aus, denen Ressourcen zugeordnet sind. Sie können Ihren Ressourcen Tags hinzufügen, indem Sie den AWS Dienst verwenden, zu dem die jeweilige Ressource gehört, oder den AWS Tag-Editor verwenden.

- 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-Distributionsressource taggen. Dies sind zwei Beispiele für Dienste mit Ressourcen, die markiert 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 Ressourcentypen finden Sie im Benutzer- oder Entwicklerhandbuch für den AWS Service, 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 dann dieses Schlüssel-Wert-Paar nur den Amazon RDS-Ressourcen in Ihrer Anwendung hinzufügen. Dies ist nützlich, wenn Sie Erkenntnisse in der Konsole anzeigen möchten, die nur aus den Amazon RDS-Ressourcen in Ihrer Anwendung generiert wurden.

Verwenden von AWS 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 AWS CloudFormation Stapel auswählen, aus denen sie erstellt werden. Sie können dies mit dem AWS Management Console 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 Save (Speichern) aus.

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

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

Mit Amazon arbeiten EventBridge

Amazon DevOps Guru ist in Amazon integriert EventBridge , um Sie über bestimmte Ereignisse im Zusammenhang mit Erkenntnissen und entsprechenden Erkenntnisaktualisierungen zu informieren. Ereignisse aus AWS Diensten werden nahezu EventBridge in Echtzeit übermittelt. 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:

- Eine AWS Lambda Funktion aufrufen
- Aufrufen eines Amazon Elastic Compute Cloud-Ausführungsbefehls
- Weiterleiten des Ereignisses an Amazon Kinesis Data Streams
- Aktivierung einer Step Functions Functions-Zustandsmaschine
- Ein Amazon SNS oder ein Amazon SQS benachrichtigen

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

- DevOps Guru New Insight Öffnen
- DevOps Guru New Anomaly Association
- DevOps Guru Insight Severity wurde aktualisiert
- DevOps Neue Empfehlung für Guru 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 EventBridge Amazon-Ereignismustern.

DevOpsGuruNeue offene Veranstaltung von Insight

Wenn DevOps Guru einen neuen Einblick öffnet, sendet er 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. Im Folgenden finden Sie ein Beispiel für ein DevOps Guru-Ereignismuster.

```
{
  "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 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 AWS 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 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 Save (Speichern) aus.

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 Save (Speichern) aus.

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 Save (Speichern) aus.

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 AWS 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 AWS CloudFormation Benutzerhandbuch undErmitteln 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 von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- 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 AWS 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 von Tags zur Identifizierung von Ressourcen in Ihren DevOps Guru-Anwendungen.
- 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 AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon DevOps Guru gelten, finden Sie unter AWS-Services in Umfang nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, 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 dir zu verstehen, wie du das Modell der geteilten Verantwortung bei der Nutzung von DevOps Guru anwenden kannst. In den folgenden Themen erfahren Sie, wie Sie DevOps Guru so konfigurieren, dass es Ihre Sicherheits- und Compliance-Ziele erreicht. Sie lernen auch, wie Sie andere AWS-Services nutzen können, die Ihnen helfen, Ihre DevOps Guru-Ressourcen zu überwachen und zu sichern.

Themen

- Datenschutz bei Amazon DevOps Guru
- Identity and Access Management für Amazon DevOps Guru
- Guru für Protokollierung und Überwachung DevOps
- DevOpsGuru- und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink
- Sicherheit der Infrastruktur in Guru DevOps
- Resilienz bei Amazon DevOps Guru

Datenschutz bei Amazon DevOps Guru

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

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

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit DevOps Guru oder anderen zusammenarbeiten und dabei die Konsole, die API oder AWS-Services verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung in DevOps Guru

Verschlüsselung ist ein wichtiger Bestandteil der DevOps Guru-Sicherheit. Einige Verschlüsselungen, z. B. für Daten während der Übertragung, sind standardmäßig verfügbar und erfordern nichts von Ihnen. Andere Verschlüsselungen, z. B. für Daten im Ruhezustand, können Sie bei der Erstellung Ihres Projekts oder Builds konfigurieren.

- Verschlüsselung von Daten während der Übertragung: Die gesamte Kommunikation zwischen Kunden und DevOps Guru sowie zwischen DevOps Guru und seinen nachgelagerten Abhängigkeiten wird mit TLS geschützt und mithilfe des Signature Version 4-Signaturprozesses authentifiziert. Alle 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 ruhender Daten: Für alle von DevOps Guru analysierten AWS Ressourcen werden die CloudWatch Amazon-Metriken und -Daten IDs, Ressourcen und AWS CloudTrail Ereignisse mit Amazon S3, Amazon DynamoDB und Amazon Kinesis gespeichert. Wenn AWS CloudFormation Stapel zur Definition der analysierten Ressourcen verwendet werden, werden auch Stack-Daten gesammelt. DevOpsGuru 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 für ein Jahr gespeichert.

  Gespeicherte Daten werden mit den data-at-rest 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 aus Protokollen mit vom CloudWatch Kunden verwalteten Schlüsseln generiert wurden. Diese Funktion bietet Ihnen die Möglichkeit, eine selbstverwaltete Sicherheitsebene hinzuzufügen, um die Compliance- und behördlichen Anforderungen Ihres Unternehmens zu erfüllen. Informationen zur Aktivierung von kundenverwalteten Schlüsseln in Ihren DevOps Guru-Einstellungen finden Sie unterthe 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 im AWS Key Management Service Entwicklerhandbuch unter Vom Kunden verwaltete Schlüssel.

> **Note**
>
> DevOpsGuru aktiviert automatisch die Verschlüsselung im Ruhezustand mithilfe AWS eigener Schlüssel, um vertrauliche Metadaten kostenlos zu schützen. Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen jedoch AWS KMS Gebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service Preisgestaltung.

Wie verwendet DevOps Guru Zuschüsse in AWS KMS

DevOpsGuru benötigt einen Zuschuss, um deinen vom Kunden verwalteten Schlüssel nutzen zu können.

Wenn du dich dafür entscheidest, die Verschlüsselung mit einem vom Kunden verwalteten Schlüssel zu aktivieren, erstellt DevOps Guru in deinem Namen einen Zuschuss, indem er eine CreateGrant Anfrage an sendet AWS KMS. Zuschüsse AWS KMS werden verwendet, um DevOps Guru Zugriff auf einen AWS KMS Schlüssel in einem Kundenkonto zu gewähren.

DevOpsGuru benötigt den Zuschuss, um deinen vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwenden zu können:

- Senden Sie DescribeKey Anfragen, um AWS KMS zu überprüfen, ob die symmetrische, vom Kunden verwaltete KMS-Schlüssel-ID, die Sie bei der Erstellung einer Tracker- oder Geofence-Sammlung eingegeben haben, gültig ist.
- Senden Sie GenerateDataKey Anfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie Entschlüsselungsanfragen an AWS KMS , um die verschlüsselten Datenschlüssel zu entschlüsseln, sodass sie zur Verschlüsselung 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 Sie dies tun, kann DevOps Guru auf keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind. Wenn Sie beispielsweise versuchen, verschlüsselte Informationen zu Protokollanomalien abzurufen, auf die DevOps Guru nicht zugreifen kann, würde der Vorgang einen AccessDeniedException Fehler zurückgeben.

Überwachen Sie Ihre Verschlüsselungsschlüssel in Guru DevOps

Wenn du einen vom AWS KMS Kunden verwalteten Schlüssel mit deinen DevOps Guru-Ressourcen verwendest, kannst du AWS CloudTrail oder CloudWatch Logs verwenden, um Anfragen nachzuverfolgen, an die DevOps Guru sendet AWS KMS.

Einen kundenverwalteten Schlüssel erstellen

Sie können einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem Sie das AWS Management Console oder das AWS KMS APIs verwenden.

Informationen zum Erstellen eines symmetrischen, vom Kunden verwalteten Schlüssels finden Sie unter KMS-Schlüssel mit symmetrischer 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 vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie AWS KMS im AWS Key Management Service Entwicklerhandbuch unter Authentifizierung und Zugriffskontrolle für.

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

- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Kontrollzugriff auf einen bestimmten AWS KMS Schlüssel, der den Zugriff auf die von DevOps Guru benötigten Zuschussoperationen ermöglicht. Weitere Informationen zur Verwendung von Zuschüssen finden Sie im AWS Key Management Service Entwicklerhandbuch.

Dadurch kann DevOps Guru Folgendes tun:

- Rufen Sie GenerateDataKey auf, um einen verschlüsselten Datenschlüssel zu generieren und ihn 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.
- Richten Sie einen Principal ein, der in den Ruhestand geht, damit der Dienst dies tun kann. RetireGrant
- Wird verwendet kms:DescribeKey , um dem Kunden verwaltete Schlüsseldetails zur Verfügung zu stellen, damit DevOps Guru den Schlüssel validieren kann.

Die folgende Erklärung enthält Beispiele für Grundsatzerklärungen, die Sie für DevOps Guru hinzufügen können:

```
"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 DevOps Guru so konfigurieren, dass er einen VPC-Schnittstellen-Endpunkt verwendet. Dafür benötigen Sie kein Internet-Gateway, kein NAT-Gerät und kein virtuelles privates Gateway. Eine Konfiguration ist ebenfalls nicht erforderlich PrivateLink, wird jedoch empfohlen. Weitere Informationen finden Sie unter DevOpsGuru- und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink. Weitere Informationen zu PrivateLink VPC-Endpunkten finden Sie unter AWS PrivateLinkund Zugreifen auf AWS-Services über. PrivateLink

Identity and Access Management für Amazon DevOps Guru

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Guru-Ressourcen zu

verwenden DevOps. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- DevOpsGuru-Updates zu AWS verwalteten Richtlinien und serviceverknüpften Rollen
- So arbeitet Amazon DevOps Guru mit IAM
- Identitätsbasierte Richtlinien für Amazon Guru DevOps
- Verwenden von dienstbezogenen Rollen für Guru DevOps
- Referenz zu Amazon DevOps Guru-Berechtigungen
- Berechtigungen für Amazon SNS SNS-Themen
- Berechtigungen für AWS KMS—verschlüsselte Amazon SNS SNS-Themen
- Fehlerbehebung bei Identität und Zugriff auf Amazon DevOps Guru

Zielgruppe

Wie du AWS Identity and Access Management (IAM) verwendest, hängt von der Arbeit ab, die du in DevOps Guru machst.

Dienstbenutzer — Wenn Sie den DevOps Guru-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Je mehr DevOps Guru-Funktionen du für deine Arbeit verwendest, desto mehr Berechtigungen benötigst du möglicherweise. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in DevOps Guru nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei Identität und Zugriff auf Amazon DevOps Guru.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die DevOps Guru-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf DevOps Guru. Es ist Ihre Aufgabe, zu bestimmen, auf welche DevOps Guru-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die

Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit DevOps Guru nutzen kann, finden Sie unterSo arbeitet Amazon DevOps Guru mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Guru schreiben können. DevOps Beispiele für identitätsbasierte DevOps Guru-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Identitätsbasierte Richtlinien für Amazon Guru DevOps

Authentifizierung mit Identitäten

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

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

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

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

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

AWS-Konto Root-Benutzer

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

Verbundidentität

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

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

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

IAM-Benutzer und -Gruppen

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

Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

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

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

IAM-Rollen

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

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein

Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

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

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

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

Identitätsbasierte Richtlinien

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

Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

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

Ressourcenbasierte Richtlinien

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

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

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und

der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

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

DevOpsGuru-Updates zu AWS verwalteten Richtlinien und serviceverknüpften Rollen

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien und der dienstbezogenen Rolle für DevOps Guru, seit dieser Dienst begonnen hat, diese Änderungen nachzuverfolgen. Abonnieren Sie den RSS-Feed auf DevOps GuruAmazon DevOps Guru-Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonDevOpsGuruConsoleFullAccess – Aktualisierung auf eine bestehende Richtlinie.	Die `AmazonDevOpsGuruFullAccess` verwaltete Richtlinie unterstützt jetzt Amazon SNS SNS-Abonnements.	9. August 2023
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf Amazon SNS SNS-Abonnementlisten.	9. August 2023
AmazonDevOpsGuruServiceRolePolicy – Aktualisi	Die `AWSServiceRoleForDevOpsGuru` dienstver	11. Januar 2023

Änderung	Beschreibung	Datum
erung auf eine bestehende Richtlinie.	knüpfte Rolle unterstützt jetzt den Zugriff auf API Gateway Gateway-GET-Aktionen auf REST APIs.	
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte Rolle unterstützt jetzt mehrere Amazon Simple Storage Service- und Service Quotas Quota-Aktionen.	19. Oktober 2022
AmazonDevOpsGuruFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die von `AmazonDevOpsGuruFullAccess` verwaltete Richtlinie unterstützt jetzt den Zugriff auf die CloudWatch `FilterLogEvents` Aktion.	30. August 2022
AmazonDevOpsGuruConsoleFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruConsoleFullAccess` verwaltete Richtlinie unterstützt jetzt den Zugriff auf die CloudWatch `FilterLogEvents` Aktion.	30. August 2022
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf die CloudWatch `FilterLogEvents` Aktion.	30. August 2022

Änderung	Beschreibung	Datum
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die mit dem `AWSServiceRoleForDevOpsGuru` Dienst verknüpfte Rolle unterstützt jetzt die CloudWatch Protokoll aktionen`FilterLogEvents`, und`DescribeLogGroups`. `DescribeLogStreams`	12. Juli 2022
Identitätsbasierte Richtlinien für DevOps Guru — Neue verwaltete Richtlinie.	Die `AmazonDevOpsGuruConsoleFullAccess` Richtlinie wurde hinzugefügt.	16. Dezember 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte Rolle unterstützt jetzt Performance Insights `DescribeMetricsKeys` - und Amazon `DescribeDBInstances` RDS-Aktionen.	1. Dezember 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` verwaltete Richtlinie unterstützt jetzt den schreibgeschützten Zugriff auf Amazon `DescribeDBInstances` RDS-Aktionen.	1. Dezember 2021

Änderung	Beschreibung	Datum
AmazonDevOpsGuruFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruFullAccess` verwaltete Richtlinie unterstützt jetzt den Zugriff auf Amazon `DescribeDBInstances` RDS-Aktionen.	1. Dezember 2021
Identitätsbasierte Richtlinien für Amazon Guru DevOps— Neue Richtlinie hinzugefügt.	Die `AWSServiceRoleForDevOpsGuru` servicevorknüpfte Rolle unterstützt jetzt den Zugriff auf Amazon RDS `DescribeDBInstances` - und Performance Insights `GetResourceMetrics` Insights-Aktionen. Die `AmazonDevOpsGuruOrganizationsAccess` verwaltete Richtlinie ermöglicht den Zugriff auf DevOps Guru innerhalb einer Organisation.	16. November 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` servicevorknüpfte Rolle unterstützt jetzt AWS Organizations.	4. November 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` servicevorknüpfte Rolle enthält jetzt neue Bedingungen für die Aktionen `ssm:CreateOpsItem` und`ssm:AddTagsToResource` .	11. Oktober 2021

Änderung	Beschreibung	Datum
Mit dem Dienst verknüpfte Rollenberechtigungen für Guru DevOps – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` dienstbezogene Rolle enthält jetzt neue Bedingungen für die Aktionen `ssm:CreateOpsItem` und `ssm:AddTagsToResource` .	14. Juni 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` verwaltete Richtlinie ermöglicht jetzt schreibgeschützten Zugriff auf die Aktionen AWS Identity and Access Management `GetRole` und Guru. DevOps `DescribeFeedback`	14. Juni 2021
AmazonDevOpsGuruReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruReadOnlyAccess` verwaltete Richtlinie ermöglicht jetzt schreibgeschützten Zugriff auf den Guru und die DevOps Aktionen. `GetCostEstimation` `StartCostEstimation`	27. April 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` Rolle ermöglicht jetzt den Zugriff auf die `DescribeAutoScalingGroups` Aktionen AWS Systems Manager `AddTagsToResource` und Amazon EC2 Auto Scaling.	27. April 2021

Änderung	Beschreibung	Datum
DevOpsGuru begann, Änderungen zu verfolgen	DevOpsGuru begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	10. Dezember 2020

So arbeitet Amazon DevOps Guru mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf DevOps Guru zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Guru verfügbar sind. DevOps

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

IAM-Feature	DevOpsGuru-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

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

Identitätsbasierte Richtlinien für Guru DevOps

Unterstützt Richtlinien auf Identitätsbasis: Ja

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

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

Beispiele für identitätsbasierte Richtlinien für Guru DevOps

Beispiele für identitätsbasierte Richtlinien von DevOps Guru finden Sie unter. Identitätsbasierte Richtlinien für Amazon Guru DevOps

Ressourcenbasierte Richtlinien innerhalb von Guru DevOps

Unterstützt ressourcenbasierte Richtlinien: Nein

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

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

Politische Maßnahmen für Guru DevOps

Unterstützt Richtlinienaktionen: Ja

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

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

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

Eine Liste der DevOps Guru-Aktionen finden Sie unter Von Amazon DevOps Guru definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in DevOps Guru verwenden 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"
           ]
```

Beispiele für identitätsbasierte Richtlinien von DevOps Guru finden Sie unter. Identitätsbasierte Richtlinien für Amazon Guru DevOps

Politische Ressourcen für Guru DevOps

Unterstützt Richtlinienressourcen: Ja

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

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

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

Eine Liste der DevOps Guru-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon DevOps Guru definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon DevOps Guru definierte Aktionen.

Beispiele für identitätsbasierte DevOps Guru-Richtlinien finden Sie unter. Identitätsbasierte Richtlinien für Amazon Guru DevOps

Bedingungsschlüssel für Richtlinien für Guru DevOps

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

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

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

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

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

Eine Liste der DevOps Guru-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon DevOps Guru in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon DevOps Guru definierte Aktionen.

Beispiele für identitätsbasierte DevOps Guru-Richtlinien finden Sie unter. Identitätsbasierte Richtlinien für Amazon Guru DevOps

Zugriffskontrolllisten (ACLs) in Guru DevOps

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle (ABAC) mit Guru DevOps

Unterstützt ABAC (Tags in Richtlinien): Nein

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

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

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

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

Weitere Informationen zu ABAC finden Sie unter 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.

Temporäre Anmeldeinformationen mit DevOps Guru verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Manche funktionieren AWS-Services nicht, wenn du dich mit temporären Zugangsdaten anmeldest. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden

und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

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

Serviceübergreifende Prinzipalberechtigungen für Guru DevOps

Unterstützt Forward Access Sessions (FAS): Ja

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

Servicerollen für Guru DevOps

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 die DevOps Guru-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn DevOps Guru Sie dazu anleitet.

Dienstbezogene Rollen für Guru DevOps

Unterstützt dienstbezogene Rollen: Ja

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

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

Identitätsbasierte Richtlinien für Amazon Guru DevOps

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

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

Einzelheiten zu den von DevOps Guru definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon DevOps Guru in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Guru-Konsole DevOps
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Von AWS verwaltete (vordefinierte) Richtlinien für DevOps Guru

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand DevOps Guru-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen

AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren

Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

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

Verwenden der Guru-Konsole DevOps

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

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

Um sicherzustellen, dass Benutzer und Rollen die DevOps Guru-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die DevOps Guru-Richtlinie `AmazonDevOpsGuruReadOnlyAccess` oder die `AmazonDevOpsGuruFullAccess` AWS verwaltete Richtlinie hinzu. 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 die Erlaubnis, diese Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS durchzuführen.

```
{
    "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 durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet AWS werden. Diese AWS verwalteten Richtlinien gewähren die erforderlichen Berechtigungen für allgemeine Anwendungsfälle, sodass Sie nicht erst untersuchen müssen, welche Berechtigungen benötigt werden. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien im IAM Benutzerhandbuch.

Um DevOps Guru-Dienstrollen zu erstellen und zu verwalten, müssen Sie auch die AWS-verwaltete Richtlinie mit dem Namen anhängen. `IAMFullAccess`

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

Die folgenden AWS verwalteten Richtlinien, die du Benutzern in deinem Konto zuordnen kannst, gelten nur für Guru. DevOps

Themen

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

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

Die `AmazonDevOpsGuruFullAccess` Richtlinie enthält die folgende Erklärung.

```
{
    "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 SNS-Themen, zum Zugriff auf CloudWatch Amazon-Metriken und zum Zugreifen auf AWS CloudFormation Stacks. Diese Richtlinie verfügt über zusätzliche Berechtigungen für Leistungseinblicke, sodass Sie detaillierte Analysen zu anomalen Amazon RDS Aurora-DB-Instances in der Konsole einsehen können. Wenden Sie dies nur auf Benutzer auf Administratorebene an, denen Sie die volle Kontrolle über Guru gewähren möchten. DevOps

Die `AmazonDevOpsGuruConsoleFullAccess` Richtlinie enthält die folgende Erklärung.

```
{
    "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 nur Lesezugriff auf DevOps Guru und verwandte Ressourcen in anderen AWS Diensten. Wenden Sie diese Richtlinie auf Benutzer an, denen Sie die Möglichkeit gewähren möchten, Einblicke einzusehen, aber keine Aktualisierungen an DevOps Gurus Analyseabdeckungsgrenzen, Amazon SNS SNS-Themen oder der Systems Manager OpsCenter Manager-Integration vorzunehmen.

Die `AmazonDevOpsGuruReadOnlyAccess` Richtlinie enthält die folgende Erklärung.

```
    {
    "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`— Bietet Organisationsadministratoren Zugriff auf die DevOps Guru-Ansicht für mehrere Konten innerhalb einer Organisation. Wenden Sie diese Richtlinie auf die Benutzer Ihrer Organisation auf Administratorebene an, denen Sie innerhalb einer Organisation vollen Zugriff auf DevOps Guru gewähren möchten. Sie können diese Richtlinie auf das Verwaltungskonto und das delegierte Administratorkonto Ihrer Organisation für Guru anwenden. DevOps Sie können diese Richtlinie `AmazonDevOpsGuruReadOnlyAccess` oder `AmazonDevOpsGuruFullAccess` zusätzlich zu dieser Richtlinie anwenden, um nur Lesezugriff oder vollen Zugriff auf Guru zu gewähren. DevOps

Die `AmazonDevOpsGuruOrganizationsAccess` Richtlinie enthält die folgende Erklärung.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDevOpsGuruOrganizationsAccess",
```

```
    "Effect": "Allow",
    "Action": [
     "devops-guru:DescribeOrganizationHealth",
     "devops-guru:DescribeOrganizationResourceCollectionHealth",
     "devops-guru:DescribeOrganizationOverview",
     "devops-guru:ListOrganizationInsights",
     "devops-guru:SearchOrganizationInsights"
    ],
    "Resource": "*"
   },
   {
    "Sid": "OrganizationsDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAWSServiceAccessForOrganization",
     "organizations:ListAccounts",
     "organizations:ListChildren",
     "organizations:ListOrganizationalUnitsForParent",
     "organizations:ListRoots"
    ],
    "Resource": "arn:aws:organizations::*:"
   },
   {
    "Sid": "OrganizationsAdminDataAccess",
    "Effect": "Allow",
    "Action": [
     "organizations:DeregisterDelegatedAdministrator",
     "organizations:RegisterDelegatedAdministrator",
     "organizations:ListDelegatedAdministrators",
     "organizations:EnableAWSServiceAccess",
     "organizations:DisableAWSServiceAccess"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "devops-guru.amazonaws.com"
      ]
     }
    }
   }
  ]
```

```
}
```

Verwenden von dienstbezogenen Rollen für Guru DevOps

Amazon DevOps Guru verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Guru verknüpft ist. DevOps Servicebezogene Rollen sind von DevOps Guru vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um Amazon- AWS CloudTrail, CloudWatch AWS CodeDeploy AWS X-Ray, und AWS Organizations in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von DevOps Guru, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. DevOpsGuru definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur DevOps Guru 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. Dadurch werden deine DevOps Guru-Ressourcen geschützt, da du die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen kannst.

Mit dem Dienst verknüpfte Rollenberechtigungen für Guru DevOps

DevOpsGuru verwendet die angegebene dienstbezogene Rolle. `AWSServiceRoleForDevOpsGuru` Dies ist eine AWS verwaltete Richtlinie mit eingeschränkten Berechtigungen, die DevOps Guru für die Ausführung in Ihrem Konto benötigt.

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

- `devops-guru.amazonaws.com`

Die Richtlinie für Rollenberechtigungen `AmazonDevOpsGuruServiceRolePolicy` ermöglicht es DevOps Guru, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen.

```
{
 "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"
    ]
   }
  ]
}
```

Eine dienstbezogene Rolle für DevOps Guru erstellen

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

> **Important**
>
> Diese dienstbezogene Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Dienst abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen verwendet. Sie kann beispielsweise erscheinen, wenn Sie DevOps Guru zu einem Repository von hinzugefügt haben. AWS CodeCommit

Eine dienstbezogene Rolle für Guru bearbeiten DevOps

DevOpsGuru erlaubt dir nicht, die `AWSServiceRoleForDevOpsGuru` dienstbezogene Rolle zu bearbeiten. 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 Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für Guru DevOps

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. Sie müssen jedoch die Verbindung zu allen Repositorys trennen, bevor Sie sie manuell löschen können.

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

So löschen Sie die serviceverknüpfte Rolle mit IAM

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

Referenz zu Amazon DevOps Guru-Berechtigungen

Sie können in Ihren DevOps Guru-Richtlinien allgemeine Bedingungsschlüssel verwenden AWS, um Bedingungen auszudrücken. Eine Liste finden Sie unter IAM JSON Policy Elements Reference im 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" ]`).

Verwenden von Platzhalterzeichen

Sie geben einen Amazon-Ressourcennamen (ARN) mit oder ohne Platzhalterzeichen (*) als Ressourcenwert im `Resource` Feld der Richtlinie an. Sie können das Platzhalterzeichen verwenden, um mehrere Aktionen oder Ressourcen anzugeben. `devops-guru:*`Gibt beispielsweise alle DevOps Guru-Aktionen an und `devops-guru:List*` gibt alle DevOps Guru-Aktionen an, die mit dem Wort `List` beginnen. Das folgende Beispiel bezieht sich auf alle Erkenntnisse mit einer Universally Unique Identifier (UUID), die mit beginnt. `12345`

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

Sie können die folgende Tabelle als Referenz verwenden, wenn Sie Berechtigungsrichtlinien einrichten Authentifizierung mit Identitäten und schreiben, die Sie einer IAM-Identität zuordnen können (identitätsbasierte Richtlinien).

DevOpsGuru-API-Operationen und erforderliche Berechtigungen für Aktionen

`AddNotificationChannel`

Aktion: `devops-guru:AddNotificationChannel`

Erforderlich, um einen Benachrichtigungskanal von DevOps Guru hinzuzufügen. Ein Benachrichtigungskanal wird verwendet, um dich zu benachrichtigen, wenn DevOps Guru Erkenntnisse generiert, die Informationen darüber enthalten, wie du deine Abläufe verbessern kannst.

Ressource: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Erforderlich, um einen Benachrichtigungskanal von DevOps Guru zu entfernen. Ein Benachrichtigungskanal wird verwendet, um dich zu benachrichtigen, wenn DevOps Guru Erkenntnisse generiert, die Informationen darüber enthalten, wie du deine Abläufe verbessern kannst.

Ressource: *

`ListNotificationChannels`

Aktion: `devops-guru:ListNotificationChannels`

Erforderlich, um eine Liste der für DevOps Guru konfigurierten Benachrichtigungskanäle zurückzugeben. Jeder Benachrichtigungskanal wird verwendet, um Sie zu benachrichtigen, wenn DevOps Guru Erkenntnisse generiert, die Informationen darüber enthalten, 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 der AWS CloudFormation Stacks zu aktualisieren, mit denen angegeben wird, welche AWS Ressourcen in Ihrem Konto von DevOps Guru analysiert werden. Die Analyse generiert Erkenntnisse, die Empfehlungen, Betriebskennzahlen und betriebliche Ereignisse beinhalten, mit denen Sie die Leistung Ihrer Betriebsabläufe verbessern können. Mit dieser Methode werden auch die IAM-Rollen erstellt, die Sie verwenden CodeGuru OpsAdvisor müssen.

Ressource: *

`GetResourceCollectionFilter`

Aktion: `devops-guru:GetResourceCollectionFilter`

Erforderlich, um die Liste der AWS CloudFormation Stacks zurückzugeben, anhand derer angegeben wird, welche AWS Ressourcen in Ihrem Konto von DevOps Guru analysiert werden. Die Analyse generiert Erkenntnisse, die Empfehlungen, Betriebskennzahlen und betriebliche Ereignisse beinhalten, mit denen Sie die Leistung Ihrer Betriebsabläufe verbessern können.

Ressource: *

`ListInsights`

Aktion: `devops-guru:ListInsights`

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

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 mit Erkenntnissen in Ihrem AWS Konto zurückzugeben. Sie können anhand der Startzeit, der Filter und des Typs (`reactive`oder`predictive`) angeben, welche Erkenntnisse zurückgegeben werden.

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 Ereignisse zurückzugeben, die von den Ressourcen ausgelöst wurden und von DevOps Guru ausgewertet werden. Sie können Filter verwenden, um anzugeben, welche Ereignisse zurückgegeben werden.

Ressource: *

`ListRecommendations`

Aktion: `devops-guru:ListRecommendations`

Erforderlich, um eine Liste mit Empfehlungen eines bestimmten Insights zurückzugeben. Jede Empfehlung enthält eine Liste von Kennzahlen 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 zurückzugeben. Verwenden Sie diese Zahlen, um den Zustand der Abläufe in Ihrem AWS Konto zu beurteilen.

Ressource: *

`DescribeAccountOverview`

Aktion: `devops-guru:DescribeAccountOverview`

Erforderlich, um Folgendes zurückzugeben, was in einem bestimmten Zeitraum passiert ist: die Anzahl der erstellten offenen reaktiven Erkenntnisse, die erstellt wurden, die Anzahl der erstellten offenen prädiktiven Erkenntnisse und die mittlere Wiederherstellungszeit (MTTR) für alle reaktiven Erkenntnisse, die geschlossen wurden.

Ressource: *

`DescribeResourceCollectionHealthOverview`

Aktion: `devops-guru:DescribeResourceCollectionHealthOverview`

Erforderlich, um die Anzahl der offenen prädiktiven Erkenntnisse, der offenen reaktiven Erkenntnisse und der mittleren Wiederherstellungszeit (MTTR) für alle Erkenntnisse für jeden in Guru angegebenen Stack zurückzugeben. AWS CloudFormation DevOps

Ressource: *

`DescribeIntegratedService`

Aktion: `devops-guru:DescribeIntegratedService`

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

Ressource: *

`UpdateIntegratedServiceConfig`

Aktion: `devops-guru:UpdateIntegratedServiceConfig`

Erforderlich, um die Integration mit einem Dienst zu aktivieren oder zu deaktivieren, der in DevOps Guru integriert werden kann. Der einzige Dienst, der in DevOps Guru integriert werden kann, ist Systems Manager, mit dem OpsItem für jeden generierten Einblick ein erstellt werden kann.

Ressource: *

Berechtigungen für Amazon SNS SNS-Themen

Verwenden Sie die Informationen in diesem Thema nur, wenn Sie Amazon DevOps Guru so konfigurieren möchten, dass Benachrichtigungen an Amazon SNS SNS-Themen gesendet werden, die einem anderen AWS Konto gehören.

Damit DevOps Guru Benachrichtigungen an ein Amazon SNS SNS-Thema senden kann, das einem anderen Konto gehört, müssen Sie dem Amazon SNS SNS-Thema eine Richtlinie beifügen, die DevOps Guru die Erlaubnis erteilt, Benachrichtigungen an dieses Konto zu senden. Wenn Sie DevOps Guru so konfigurieren, dass Benachrichtigungen an Amazon SNS SNS-Themen gesendet

werden, die demselben Konto gehören, das Sie für DevOps Guru verwenden, fügt DevOps Guru den Themen eine Richtlinie für Sie hinzu.

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

> **Note**
>
> DevOpsGuru unterstützt derzeit nur kontoübergreifenden Zugriff in derselben Region.

Themen

- Berechtigungen für ein Amazon SNS SNS-Thema in einem anderen Konto konfigurieren
- Hinzufügen eines Amazon SNS SNS-Themas von einem anderen Konto
- Aktualisierung Ihrer Amazon SNS SNS-Richtlinie mit einem Benachrichtigungskanal (empfohlen)

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

Berechtigungen als IAM-Rolle hinzufügen

Um ein Amazon SNS SNS-Thema von einem anderen Konto aus zu verwenden, nachdem Sie sich mit einer IAM-Rolle angemeldet haben, müssen Sie eine Richtlinie an das Amazon SNS SNS-Thema anhängen, das Sie verwenden möchten. Um eine Richtlinie von einem anderen Konto an ein Amazon SNS SNS-Thema anzuhängen und gleichzeitig eine IAM-Rolle zu 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 SNS-Thema an, das Sie verwenden möchten. Bei dem `Resource` Schlüssel *`topic-owner-account-id`* handelt es sich um die Konto-ID des Eigentümers des Themas, *`topic-sender-account-id`* um die Konto-ID des Benutzers,

der DevOps Guru eingerichtet hat, und *devops-guru-role* um die IAM-Rolle des jeweiligen Benutzers. Sie müssen *region-id* (z. B.`us-west-2`) und *my-topic-name* durch entsprechende Werte ersetzen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:role/devops-guru-role"]
            }
        }
    ]
}
```

Berechtigungen als IAM-Benutzer hinzufügen

Um ein Amazon SNS SNS-Thema von einem anderen Konto als IAM-Benutzer zu verwenden, fügen Sie dem Amazon SNS SNS-Thema, das Sie verwenden möchten, die folgende Richtlinie bei. Bei dem `Resource` Schlüssel *topic-owner-account-id* handelt es sich um die Konto-ID des Eigentümers des Themas, *topic-sender-account-id* um die Konto-ID des Benutzers, der DevOps Guru eingerichtet hat, und *devops-guru-user-name* um den betreffenden individuellen IAM-Benutzer. Sie müssen *region-id* (z. B.`us-west-2`) und *my-topic-name* durch entsprechende Werte ersetzen.

> **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 Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EnableDevOpsGuruServicePrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "Service": "region-id.devops-guru.amazonaws.com"
            },
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "topic-sender-account-id"
                }
            }
        },
        {
            "Sid": "EnableAccountPrincipal",
            "Action": "sns:Publish",
            "Effect": "Allow",
            "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
            "Principal": {
                "AWS": ["arn:aws:iam::topic-sender-account-id:user/devops-guru-user-
name"]
            }
        }
    ]
}
```

Hinzufügen eines Amazon SNS SNS-Themas von einem anderen Konto

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

- Wenn Sie die Konsole verwenden, müssen Sie die Option SNS-Themen-ARN verwenden auswählen, um ein vorhandenes Thema anzugeben, um ein Thema aus einem anderen Konto verwenden zu können.
- Wenn Sie die AWS CLI Operation verwenden add-notification-channel, müssen Sie die `TopicArn` innerhalb des `NotificationChannelConfig` Objekts angeben.

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

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. Gehen Sie zum Abschnitt Benachrichtigungen und wählen Sie Bearbeiten.
4. Wählen Sie „SNS-Thema hinzufügen“.
5. Wählen Sie SNS-Themen-ARN verwenden, um ein vorhandenes Thema anzugeben.
6. Geben Sie den ARN des Amazon SNS SNS-Themas ein, das Sie verwenden möchten. Sie sollten bereits Berechtigungen für dieses Thema konfiguriert haben, indem Sie dem Thema eine Richtlinie beifügen.
7. (Optional) Wählen Sie „Benachrichtigungskonfiguration“, um die Einstellungen für die Benachrichtigungshäufigkeit zu bearbeiten.
8. Wählen Sie Speichern.

Nachdem Sie das Amazon SNS SNS-Thema zu Ihren Benachrichtigungseinstellungen hinzugefügt haben, verwendet DevOps Guru dieses Thema, um Sie über wichtige Ereignisse zu informieren, z. B. wenn ein neuer Einblick erstellt wird.

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

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

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

1. Führen Sie den `list-notification-channels` DevOps AWS CLI Guru-Befehl in Ihrem Konto aus, von dem aus Sie Benachrichtigungen senden möchten.

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

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

   In der folgenden Antwort `arn:aws:sns:`*`region-id`*`:`*`111122223333`*`:`*`topic-name`* lautet die Kanal-ID für das Thema mit dem ARN beispielsweise *`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 mit der Themen-Eigentümer-ID in erstellt habenthe section called “Berechtigungen für ein Amazon SNS SNS-Thema in einem

anderen Konto konfigurieren". Fügen Sie in der `Condition` Erklärung der Richtlinie die Zeile hinzu, die den angibt`SourceArn`. Der ARN enthält Ihre Region-ID (z. B.`us-east-1`), die AWS Kontonummer des Absenders des Themas und die Kanal-ID, die Sie sich notiert haben.

Ihr aktualisierter `Condition` Kontoauszug 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` Sie Ihr SNS-Thema nicht hinzufügen können, überprüfen Sie, ob Ihre IAM-Richtlinie über die folgenden Berechtigungen verfügt.

```
{
     "Version": "2012-10-17",
     "Statement": [{
           "Sid": "DevOpsGuruTopicPermissions",
           "Effect": "Allow",
           "Action": [
                 "sns:CreateTopic",
                 "sns:GetTopicAttributes",
                 "sns:SetTopicAttributes",
                 "sns:Publish"
           ],
           "Resource": "arn:aws:sns:region-id:account-id:my-topic-name"
     }]
}
```

Berechtigungen für AWS KMS—verschlüsselte Amazon SNS SNS-Themen

Das von Ihnen angegebene Amazon SNS SNS-Thema wurde möglicherweise von AWS Key Management Service verschlüsselt. Damit DevOps Guru mit verschlüsselten Themen arbeiten kann, müssen Sie zuerst eine Anweisung erstellen AWS KMS key und dann die folgende Anweisung zur Richtlinie für den KMS-Schlüssel hinzufügen. Weitere Informationen finden Sie unter Verschlüsselung von auf Amazon SNS veröffentlichten Nachrichten mit AWS KMS, Schlüsselkennungen (KeyId) im

AWS KMS Benutzerhandbuch und Datenverschlüsselung im Amazon Simple Notification Service Developer Guide.

```
{
  "Version": "2012-10-17",
  "Id": "your-kms-key-policy",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> DevOpsGuru unterstützt derzeit verschlüsselte Themen für die Verwendung innerhalb eines einzigen Kontos. Die Verwendung eines verschlüsselten Themas für mehrere Konten wird derzeit nicht unterstützt.

Fehlerbehebung bei Identität und Zugriff auf Amazon DevOps Guru

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

Themen

- Ich bin nicht autorisiert, eine Aktion in DevOps Guru durchzuführen
- Ich möchte Benutzern programmatischen Zugriff gewähren
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine DevOps Guru-Ressourcen ermöglichen

Ich bin nicht autorisiert, eine Aktion in DevOps Guru durchzuführen

Wenn dir AWS Management Console mitgeteilt wird, dass du nicht berechtigt bist, eine Aktion durchzuführen, musst du dich an deinen Administrator wenden, um Unterstützung zu erhalten.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `aws:`*`GetWidget`* Berechtigungen verfügt.

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

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

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

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

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

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn du die Fehlermeldung erhältst, dass du nicht autorisiert bist, die `iam:PassRole` Aktion durchzuführen, müssen deine Richtlinien aktualisiert werden, damit du eine Rolle an DevOps Guru übergeben kannst.

Einige AWS-Services ermöglichen es dir, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in DevOps Guru auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine DevOps Guru-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, kannst du diese Richtlinien verwenden, um Personen Zugriff auf deine Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob DevOps Guru diese Funktionen unterstützt, finden Sie unter. So arbeitet Amazon DevOps Guru mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Guru für Protokollierung und Überwachung DevOps

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von DevOps Guru und Ihren anderen AWS-Lösungen. AWS bietet die folgenden Überwachungstools, um DevOps Guru zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre 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. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 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

- Monitoring DevOps Guru mit Amazon CloudWatch
- Protokollieren von Amazon DevOps Guru-API-Aufrufen mit AWS CloudTrail

Monitoring DevOps Guru mit Amazon CloudWatch

Sie können den Einsatz von DevOps Guru überwachen CloudWatch, das Rohdaten sammelt und sie zu lesbaren Kennzahlen verarbeitet, die nahezu in Echtzeit ablaufen. 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 im CloudWatch Amazon-Benutzerhandbuch.

Für DevOps Guru können Sie Messwerte für Erkenntnisse und Messwerte für Ihre DevOps Guru-Nutzung verfolgen. Möglicherweise möchten Sie nach einer großen Anzahl von erstellten Inhalten

Ausschau halten`Insights`, um festzustellen, ob bei Ihren Betriebslösungen ein ungewöhnliches Verhalten auftritt. Oder vielleicht möchten Sie die Nutzung Ihres DevOps Gurus beobachten, um Ihre Kosten im Blick zu behalten.

Der DevOps Guru-Dienst meldet die folgenden Messwerte im `AWS/DevOps-Guru` Namespace.

Themen

- Insight-Metriken
- DevOpsNutzungsmetriken von Guru

Insight-Metriken

Sie können CloudWatch eine Metrik verfolgen, die Ihnen zeigt, wie viele Erkenntnisse in Ihrem AWS Konto erstellt wurden. Sie können die `Type` Dimension angeben, die erfasst werden soll `proactive` oder welche `reactive` Erkenntnisse erfasst werden sollen. Geben Sie keine Dimension an, wenn Sie alle Erkenntnisse verfolgen möchten.

Metriken

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

Die folgende Dimension wird für die DevOps `Insight` Guru-Metrik unterstützt.

Dimensions (Abmessungen)

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

DevOpsNutzungsmetriken von Guru

Sie können CloudWatch damit Ihre Nutzung von Amazon DevOps Guru verfolgen.

Metriken

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

Metrik	Beschreibung
	Einheiten: Anzahl

Die folgenden Dimensionen werden für die DevOps Guru-Nutzungsmetriken unterstützt.

Dimensions (Abmessungen)

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

Protokollieren von Amazon DevOps Guru-API-Aufrufen mit AWS CloudTrail

Amazon DevOps Guru ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in DevOps Guru bereitstellt. CloudTrail erfasst API-Aufrufe für DevOps Guru als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der DevOps Guru-Konsole und Code-Aufrufe der DevOps Guru-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für DevOps Guru. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage

CloudTrail, die an DevOps Guru gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

DevOpsInformationen zum Guru in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in DevOps Guru eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Event-Historie als Ereignis aufgezeichnet. Du kannst aktuelle Ereignisse in deinem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in deinem AWS Konto, einschließlich der Ereignisse für DevOps Guru, erstellst du einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Pfad in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

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

DevOpsGuru unterstützt die Protokollierung all seiner Aktionen als Ereignisse in CloudTrail Protokolldateien. Weitere Informationen finden Sie unter Aktionen in der DevOpsGuru-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 AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

DevOpsGuru-Protokolldateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 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 Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateResourceCollection` Aktion demonstriert.

```
{
  "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"
}
```

DevOpsGuru- und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink

Sie können VPC-Endpunkte verwenden, wenn Sie Amazon DevOps Guru aufrufen. 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 Amazon DevOps Guru API-Referenz.

Sie stellen eine private Verbindung zwischen Ihrer VPC und DevOps Guru her, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden mit einer Technologie betrieben AWS PrivateLink, mit der Sie APIs ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder AWS Direct Connect Connect-Verbindung privat auf DevOps Guru zugreifen können. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit DevOps Guru APIs zu kommunizieren. Der 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 Interface VPC Endpoints (AWS PrivateLink) im Amazon VPC-Benutzerhandbuch.

Überlegungen zu DevOps Guru VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für DevOps Guru einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen der Schnittstellen-Endpunkte im Amazon VPC-Benutzerhandbuch lesen.

DevOpsGuru unterstützt Aufrufe all seiner API-Aktionen von Ihrer VPC aus.

Erstellen eines VPC-Schnittstellen-Endpunkts für Guru DevOps

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

Erstellen Sie einen VPC-Endpunkt für DevOps Guru mit dem folgenden Dienstnamen:

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

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anfragen an DevOps Guru stellen, indem Sie dessen Standard-DNS-Namen für die Region verwenden, zum Beispiel. `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 Guru DevOps

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf DevOps Guru steuert. 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

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für DevOps Guru. Wenn diese Richtlinie an einen Endpunkt angehängt ist, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten DevOps Guru-Aktionen.

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

Sicherheit der Infrastruktur in Guru DevOps

Als verwalteter Service ist Amazon DevOps Guru durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf DevOps Guru zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS

Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Resilienz bei Amazon DevOps Guru

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. DevOpsGuru 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 robust sind.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale 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

AWS 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-Dokumentenverlauf

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

- API-Version: aktuelle
- Letzte Aktualisierung der Dokumentation: 9. August 2023

Änderung	Beschreibung	Datum
Verwaltete Richtlinienaktualisierungen	Amazon SNS SNS-Abonnements und Zugriff auf Abonnementlisten wurden der `AmazonDevOpsGuruConsoleFullAccess` Richtlinie hinzugefügt. Der `AmazonDevOpsGuruReadOnlyAccess` Richtlinie wurde auch der Zugriff auf Abonnementlisten hinzugefügt. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien für Amazon DevOps Guru.	9. August 2023
Vom Kunden verwaltete Verschlüsselungsschlüssel	DevOpsGuru unterstützt jetzt die Verschlüsselung mit vom Kunden verwalteten Schlüsseln AWS KMS. Weitere Informationen finden Sie unter Datenschutz in DevOps Guru.	5. Juli 2023
DevOpsGuru für RDS unterstützt RDS PostgreSQL	DevOpsGuru for RDS kann Leistungsengpässe und andere Erkenntnisse in PostgreSQL-Datenbanken	30. März 2023

	erkennen. Weitere Informationen finden Sie unter Vorteile von DevOps Guru for RDS.	
DevOpsGuru for RDS unterstützt proaktive Einblicke	DevOpsGuru 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 for RDS.	28. Februar 2023
Seite „Analysierte Ressourcen“	Eine neue Seite in der DevOps Guru-Konsole listet Ressourcen in Ihrem Konto auf, die von DevOps Guru analysiert wurden. Weitere Informationen findest du unter Von DevOps Guru analysierte Ressourcen anzeigen.	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 Aktualisieren der Amazon Amazon SNS SNS-Benachrichtigungskonfigurationen.	30. September 2022

Ergänzung der verwalteten Richtlinien zur Analyse von Protokollanomalien	AWS Die verwalteten Richtlinien für DevOps Guru wurden in der IAM-Konsole aktualisiert, um den Zugriff auf die Aktion zu unterstützen. CloudWatch `FilterLogEvents` Weitere Informationen finden Sie unter Updates von DevOps Guru zu AWS verwalteten Richtlinien und serviceverknüpften Rollen.	30. August 2022
Analyse von Protokoll anomalien hinzugefügt	In der DevOps Guru-Konsole können Sie detaillierte Informationen zu Protokoll gruppen im Zusammenhang mit Insights einsehen. Es steht auch eine erweiterte dienstbezogene Rolle zur Beschreibung von CloudWatch Logs und Streams zur Verfügung. Weitere Informationen finden Sie unter Grundlegendes zu den Erkenntnissen in der DevOps Guru-Konsole und unter DevOpsGuru-Updates zu AWS verwalteten Richtlinien und serviceverknüpften Rollen.	12. Juli 2022

CodeGuru Profiler-Integration	DevOpsGuru lässt sich jetzt mit einer EventBridge verwalteten Regel in Amazon CodeGuru Profiler integrieren. Bei jedem eingehenden Ereignis von CodeGuru Profiler handelt es sich um einen proaktiven Anomaliebericht. Weitere Informationen finden Sie unter Integration mit Profiler. CodeGuru	7. März 2022
Dienstbezogene Rollen- und verwaltete Richtlinienaktualisierungen	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderungen ermöglichen es DevOps Guru, die erweiterte Integration mit Amazon Relational Database Service (Amazon RDS) zu unterstützen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen und AWS verwalteten (vordefinierten) Richtlinien für DevOps Guru.	21. Dezember 2021
Neue verwaltete Richtlinie hinzugefügt	Die `AmazonDevOpsGuruConsoleFullAccess` Richtlinie wurde hinzugefügt. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien für Amazon DevOps Guru.	6. Dezember 2021

Support bei der Definition Ihrer Anwendung mit AWS Tags	Sie können jetzt AWS Tags verwenden, um die Ressourcen zu identifizieren, die DevOps Guru analysieren soll, die Ressourcen in Ihren Anwendungen zu identifizieren und Erkenntnisse in der Konsole zu filtern. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren Anwendungen.	1. Dezember 2021
Dienstbezogene Rollen- und verwaltete Richtlinienaktualisierungen	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderungen ermöglichen es DevOps Guru, die erweiterte Integration mit Amazon Relational Database Service (Amazon RDS) zu unterstützen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen und AWS verwalteten (vordefinierten) Richtlinien für DevOps Guru.	1. Dezember 2021

Amazon RDS-Unterstützung	DevOpsGuru 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
EventBridge Amazon-Integration	DevOpsGuru lässt sich jetzt integrieren EventBridge , um Sie über bestimmte Ereignisse im Zusammenhang mit Ihren DevOps Guru-Erkenntnissen zu informieren. Weitere Informationen findest du unter Arbeiten mit EventBridge.	18. November 2021
AWS verwaltete Richtlinie hinzugefügt	Neue AWS verwaltete Richtlinie hinzugefügt. Die `AmazonDevOpsGuruOrganizationsAccess` Richtlinie ermöglicht den Zugriff auf DevOps Guru innerhalb einer Organisation. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien.	16. November 2021

Aktualisierung der Richtlinien für dienstbezogene Rollen	Erweiterte Richtlinie in der IAM-Konsole verfügbar. Diese Änderung ermöglicht es DevOps Guru, die Multi-Account-Ansicht zu unterstützen. Weitere Informationen finden Sie unter Verwenden von dienstbezogenen Rollen.	4. November 2021
Kontenübergreifende 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
Version zur allgemeinen Verfügbarkeit	Amazon DevOps Guru ist jetzt allgemein verfügbar (GA).	4. Mai 2021
Neues Thema	Sie können jetzt einen monatlichen Kostenvoranschlag für DevOps Guru erstellen, um Ihre Ressourcen zu analysieren. Weitere Informationen finden Sie unter Schätzen Sie Ihre Amazon DevOps Guru-Kosten.	27. April 2021

VPC-Endpunktunterstützung	Sie können jetzt VPC-Endpunkte verwenden, um die Sicherheit Ihrer Ressourcenanalyse und der Generierung von Erkenntnissen zu verbessern. Weitere Informationen finden Sie unter DevOpsGuru- und Schnittstellen-VPC-Endpunkte ()AWS PrivateLink.	15. April 2021
Neues Thema	Ein neues Thema zur Überwachung von DevOps Guru mit Amazon CloudWatch wurde hinzugefügt. Weitere Informationen finden Sie unter Monitoring DevOps Guru with Amazon CloudWatch.	11. Dezember 2020
Vorschauversion	Dies ist die Vorabversion des Amazon DevOps Guru-Benutzerhandbuchs.	1. Dezember 2020

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

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.