aws

Benutzerhandbuch

DevOps Amazon-Guru

DevOps Amazon-Guru: Benutzerhandbuch

Table of Contents

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.

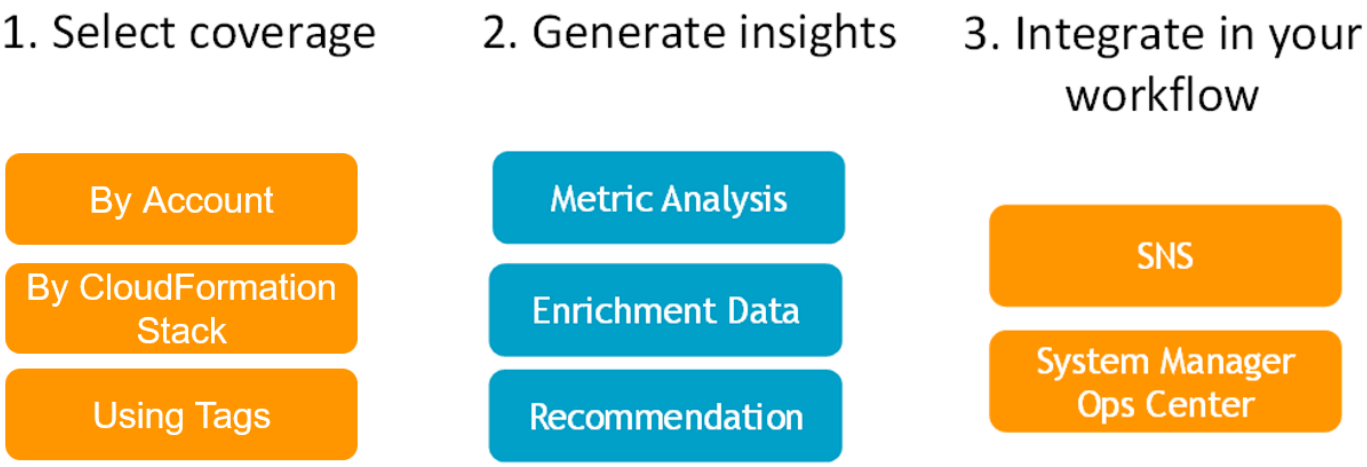
Themen

DevOpsGuru-Workflow auf hohem Niveau

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.



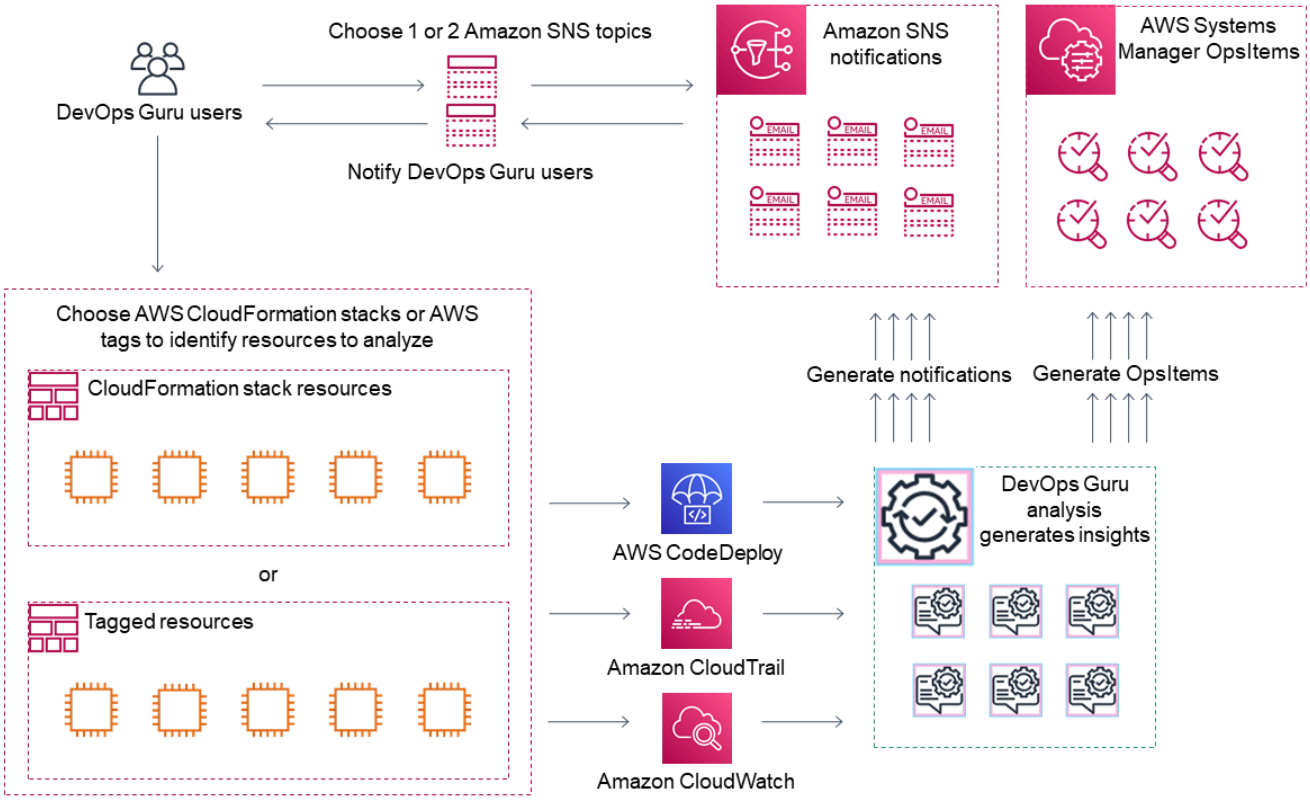
1. Im ersten Schritt wählen Sie Ihren Versicherungsschutz aus, indem Sie angeben, welche AWS Ressourcen in Ihrem AWS Konto analysiert werden. DevOpsGuru kann alle Ressourcen in einem AWS Konto abdecken oder analysieren, oder du kannst AWS CloudFormation Stapel oder AWS Tags verwenden, um eine Teilmenge 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. DevOpsGuru 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, Amazon EC2-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 Ihrer Benachrichtigungen in DevOpsGuru.
   - 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 AktualisierungAWS Systems ManagerIntegration inDevOpsGuru.

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 finden Sie unter Definieren von Anwendungen mitAWSRessourcen 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 deinerAWSBerichterstattung über Analysen in DevOpsGuru 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 für ein Verständnis der Funktionsweise von Amazon DevOps Guru.

Themen

Anomalie

Eine Anomalie steht für eine oder mehrere verwandte Metriken, die von DevOps Guru entdeckt wurden und die unerwartet oder ungewöhnlich sind. DevOpsGuru generiert Anomalien, indem es maschinelles Lernen verwendet, um Metriken und Betriebsdaten zu analysieren, die sich auf IhreAWS Ressourcen beziehen. Sie geben dieAWS Ressourcen an, die analysiert werden sollen, wenn Sie Amazon DevOps Guru einrichten. Weitere Informationen finden Sie unter Amazon DevOps Guru einrichten.

Insight

Ein Insight ist eine Sammlung von Anomalien, die bei der Analyse derAWS Ressourcen entstehen, die du bei der Einrichtung von DevOps Guru angegeben hast. Jeder Einblick enthält Beobachtungen,

Empfehlungen und analytische Daten, die Sie zur Verbesserung Ihrer Betriebsleistung verwenden können. Es gibt zwei Arten von -Erkenntnissen:

- Reaktiv: Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Es enthält Anomalien mit Empfehlungen, zugehörigen Metriken und Ereignissen, damit Sie die Probleme jetzt besser verstehen und lösen 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 lösen, bevor sie vorhergesagt werden.

Metriken und betriebliche Ereignisse

Die Anomalien, die einen Einblick ausmachen, werden durch die Analyse der von Amazon zurückgegebenen Kennzahlen CloudWatch und der betrieblichen Ereignisse, die von IhrenAWS Ressourcen ausgelöst wurden, generiert. Sie können die Kennzahlen und die betrieblichen Ereignisse einsehen, die Ihnen einen Einblick geben, damit Sie Probleme in Ihrer Anwendung besser verstehen können.

Protokollgruppen und Protokollanomalien

Wenn Sie die Erkennung von Protokollanomalien aktivieren, werden relevante 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 auf welche zugegriffen wird.

Eine Protokollanomalie stellt einen Cluster ähnlicher anomaler Protokollereignisse dar, die innerhalb einer Protokollgruppe gefunden wurden. Beispiele für anomale Log-Ereignisse, die in DevOps Guru angezeigt werden können, umfassen Keyword-Anomalien, Formatanomalien, HTTP-Code-Anomalien und mehr.

Mithilfe von Protokollanomalien können Sie die Grundursache eines Betriebsproblems diagnostizieren. DevOpsGuru verweist auch auf Logzeilen in Insight-Empfehlungen, um mehr Kontext für empfohlene Lösungen zu bieten.

> **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 du die Erkennung von Protokollanomalien deaktivierst, entfernt DevOps Guru Tags aus deinen CloudWatch Protokollgruppen.
Darüber hinaus sollten Administratoren sicherstellen, dass nur Benutzer mit Berechtigungen zum Anzeigen von CloudWatch Protokollen berechtigt sind, ungewöhnliche CloudWatch Protokolle einzusehen. Wir empfehlen die Verwendung von IAM-Richtlinien, um den Zugriff auf den`ListAnomalousLogs` Vorgang zu ermöglichen oder zu verweigern. Weitere Informationen finden Sie unter Identity and Access Management für DevOps Guru für Guru.

Empfehlungen

Jeder Einblick umfasst Empfehlungen mit Vorschlägen, um die Leistung Ihrer Anwendung zu verbessern. Die Empfehlung umfasst Folgendes:

- Eine Beschreibung der Empfehlungsmaßnahmen zur Behebung der Anomalien, aus denen sich die Erkenntnisse zusammensetzen.
- Eine Liste der analysierten Metriken, bei denen DevOps Guru ungewöhnliches Verhalten feststellte. Jede Metrik enthält den Namen desAWS CloudFormation Stacks, der die mit den Metriken verknüpfte Ressource generiert hat, den Namen der Ressource und den Namen des mit der Ressource verknüpftenAWS Dienstes.
- Eine Liste der Ereignisse, die sich auf die anomalen Metriken beziehen, die mit den Erkenntnissen verknüpft sind. Jedes zugehörige Ereignis enthält den Namen desAWS CloudFormation Stacks, der die mit dem Ereignis verknüpfte Ressource generiert hat, den Namen der Ressource, die das Ereignis generiert hat, und den Namen des mit dem Ereignis verknüpftenAWS Dienstes.
- Eine Liste von Protokollgruppen, die sich auf das mit dem Insight verknüpfte anomale Verhalten beziehen. Jede Protokollgruppe enthält eine Musterprotokollnachricht, Informationen über die Arten der gemeldeten Protokollanomalien, die Zeiten, zu denen die Protokollanomalien aufgetreten sind, und einen Link zum Anzeigen der Protokollzeilen CloudWatch.

DevOpsGuru-Abdeckung

DevOpsGuru adressiert und erstellt Einblicke für eine Reihe verschiedener - AWS Services.
Für jeden Service, für den DevOpsGuru Erkenntnisse erstellt, zeigt DevOpsGuru eine Vielzahl analysierter Metriken und generierter Erkenntnisse an.

Beispielanwendungsfall für reaktive Erkenntnisse:

Service-Name	Anwendungsfall	Beispiele	Metriken
AWS Lambda	Erkennen Sie Latenz- oder Daueranomalien für Lambda-Funktionen, die durch verschiedene Ursachen wie Kaltstarts, erhöhte Anfragen, Downstream-Drosselung oder Codebereitstellungen verursacht werden. Empfohlene Möglichkeiten zur schnellen Minderung.	Code-Bereitstellung: Amazon API Gateway Die Latenz wird durch eine Erhöhung der Lambda-Latenz nach einer kürzlichen Lambda-Code-Bereitstellung beeinflusst. Nachgelagerte Drosselung: Der Operator hat die Kapazität für Leseeinheiten für DynamoDB reduziert, was zu erhöhten Wiederholungen führte. Dies führt zu einer Drosselung. Kaltstart: Die Lambda-Funktion ist nicht ausgelastet, sodass Lambda länger dauert, wenn Anfragen gestellt werden.	Dauer Drosselungen

Beispiel-Anwendungsfall für proaktive Einblicke:

Service-Name	Anwendungsfall	Metriken
Amazon DynamoDB	Bei der verbrauchten Kapazität des DynamoDB-Tabellenlesevorgangs besteht das Risiko, dass das	ConsumedReadCapacityUnits

Service-Name	Anwendungsfall	Metriken
	Tabellenlimit erreicht wird. Empfohlene Aktion: Wenn Sie den Modus bereitges tellter Kapazität verwenden, verwenden Sie Auto Scaling, um die Durchsatzkapazität für Tabellen aktiv zu verwalten oder reservierte Kapazität im Voraus für Tabellen zu erwerben. Wechseln Sie in den On-Demand-Kapazitä tsmodus, um pro Leseanfor derung zu bezahlen und nur für das zu zahlen, was genutzt wird. Erkennungszeit: 6 Tage	

Service-Abdeckungsliste

Für einige Services erstellt DevOpsGuru reaktive Einblicke. Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Es enthält Anomalien mit Empfehlungen, zugehörigen Metriken und Ereignissen, die Ihnen helfen, die Probleme jetzt zu verstehen und zu beheben.

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

DevOpsGuru erstellt reaktive Einblicke für Services wie die folgenden:

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

> **Note**
>
> DevOpsDie Guru-Überwachung erfolgt auf Auto Scaling-Gruppenebene und nicht auf einer einzelnen Instance-Ebene.

- 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
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru erstellt proaktive Einblicke für Services 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/signup.
2. Folgen Sie den Online-Anweisungen.

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

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

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

Erstellen Sie einen Benutzer mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

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

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

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

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

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

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

Melden Sie sich als Benutzer mit Administratorzugriff an

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

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

Weisen Sie weiteren Benutzern Zugriff zu

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

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

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

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

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 benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-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 angeben und Sie können 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 DevOpsGuru-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 unterAnsehenDevOpsEinblicke in Guru.

Weitere Informationen finden Sie unter Definieren von Anwendungen mitAWSRessourcen. 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- DevOpsGuru-Ressourcenanalyse

Sie können Ihre monatlichen Kosten für Amazon DevOpsGuru zur Analyse Ihrer AWS-Ressourcen schätzen. Sie zahlen für die Anzahl der Stunden, die für jede aktive AWS-Ressource in Ihrer angegebenen Ressourcenabdeckung analysiert wurden. Eine Ressource ist aktiv, wenn sie innerhalb einer Stunde Metriken, Ereignisse oder Protokolle erzeugt.

DevOps Guru scannt Ihre ausgewählten Ressourcen, um eine monatliche Kostenschätzung zu erstellen. Sie können die Ressourcen, ihren stündlichen abrechenbaren Preis und ihre geschätzte monatliche Gebühr anzeigen. Der Kostenschätzer geht davon aus, dass die analysierten aktiven Ressourcen zu 100 Prozent der Zeit genutzt werden. Sie können diesen Prozentsatz für jeden analysierten Service basierend auf 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 nicht die Kosten, die mit DevOpsGuru-API-Aufrufen verbunden sind.

Sie können jeweils eine Kostenschätzung erstellen. Die Zeit, die zum Generieren einer Kostenschätzung benötigt wird, hängt von der Anzahl der Ressourcen ab, die Sie bei der Erstellung der Kostenschätzung 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. Ihre tatsächlichen Kosten variieren und hängen davon ab, wie viel Prozent der Zeit Ihre analysierten aktiven Ressourcen genutzt werden.

> **Note**
>
> Für eine Kostenschätzung können Sie nur einen AWS CloudFormationStack angeben. Für Ihre tatsächliche Abdeckungsgrenze können Sie bis zu 1 000 Stacks angeben.

So erstellen Sie eine monatliche Kostenschätzung für die Ressourcenanalyse

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

Zustimmen aus, um die IAM-Rolle zu erstellen. Auf diese Weise kann DevOpsGuru eine serviceverknüpfte IAM-Rolle für Sie erstellen, wenn Sie die Kostenschätzungsanalyse starten oder DevOpsGuru verwenden möchten. Auf diese Weise DevOpsverfügtGuru über die Berechtigungen, die zum Erstellen der Kostenschätzung erforderlich sind. Wenn Sie DevOpsGuru bereits aktiviert haben, wurde die Rolle bereits erstellt und diese Option wird nicht angezeigt.

4. Wählen Sie die Ressourcen aus, die Sie zum Erstellen Ihrer Schätzung verwenden möchten.

   - Wenn Sie die Kosten schätzen möchten, damit DevOpsGuru die von einem AWS CloudFormationStack definierten Ressourcen analysiert, gehen Sie wie folgt vor.
     1. Wählen Sie CloudFormation Stack in der aktuellen Region aus.
     2. Wählen Sie unter CloudFormation Stack auswählen den Namen eines AWS CloudFormationStacks 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 CloudFormationStack verwenden, den Sie derzeit nicht analysieren, wählen Sie Ressourcenanalyse aktivieren, damit DevOpsGuru mit der Analyse seiner Ressourcen beginnen kann. Diese Option ist nicht verfügbar, wenn Sie DevOpsGuru nicht aktiviert haben oder wenn Sie bereits die Ressourcen im Stack analysieren.
   - Wenn Sie die Kosten für die Analyse von Ressourcen durch DevOpsGuru mit einem Tag schätzen möchten, gehen Sie wie folgt vor.
     1. Wählen Sie Tags für AWS Ressourcen in der aktuellen Region
     2. Wählen Sie unter Tag-Schlüssel den Schlüssel Ihres Tags aus
     3. Wählen Sie unter Tag-Wert (alle Werte) oder einen Wert aus.
   - Wenn Sie die Kosten schätzen möchten, damit DevOpsGuru die Ressource in Ihrem AWS Konto und Ihrer Region analysiert, wählen Sie AWS Konto in der aktuellen Region aus.
5. Wählen Sie Monatliche Kosten schätzen aus.
6. (Optional) Geben Sie in der Spalte Aktive Ressourcenauslastung in % einen aktualisierten Prozentwert für einen oder mehrere AWS-Services ein. Die standardmäßige aktive Ressourcenauslastung in % beträgt 100 %. Das bedeutet, dass DevOps Guru die Schätzung für den AWS-Service generiert, indem es die Kosten für die Analyse seiner Ressourcen für eine Stunde berechnet und diese dann über 30 Tage auf insgesamt 720 Stunden extrapoliert. Wenn ein Service in weniger als 100 % der Zeit aktiv ist, können Sie den Prozentsatz basierend auf Ihrer geschätzten Nutzung aktualisieren, um eine genauere Schätzung zu erhalten. Wenn Sie beispielsweise die aktive Ressourcenauslastung eines Services auf 75 % aktualisieren, werden

die Kosten für die Analyse seiner Ressourcen für eine Stunde über (720 x 0,75) Stunden oder 540 Stunden extrapoliert.

Wenn Ihre Schätzung null Dollar beträgt, enthalten die von Ihnen ausgewählten Ressourcen wahrscheinlich keine von DevOpsGuru unterstützten Ressourcen. Weitere Informationen zu den unterstützten Services und Ressourcen finden Sie unter Amazon DevOpsGuru – 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

Bevor Sie beginnen, bereiten Sie sich vor, indem Sie die Schritte unter 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 mithilfe der Konsole oder mithilfe der AWS CLI kontenübergreifenden Support für Ihre Organisation hinzufügen.

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. Dadurch erhalten Sie Zugriff auf eine konsolidierte Ansicht für jedes Konto, für das DevOps Guru aktiviert ist. Der delegierte Administrator hat einen konsolidierten Überblick über alle 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. undbenutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-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 finden Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru und Aktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru.

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 Amazon SNS SNS-Thema angeben ein zu verwendendes Thema aus.

   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. benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-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 du möchtest, dass DevOps Guru alle unterstützten Ressourcen in deinem AWS Konto und deiner Region analysiert. 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 benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-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.

  Der Schlüssel des Tags muss mit dem Präfix beginnen`devops-guru-`. Bei diesem Präfix wird nicht zwischen Groß- und Kleinschreibung unterschieden. Ein gültiger Schlüssel ist `DevOps-Guru-Production-Applications` beispielsweise. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOpsGuru-Anwendungen.
- Wählen Sie Keine, wenn Sie nicht möchten, dass DevOps Guru Ressourcen analysiert. Diese Option deaktiviert DevOps Guru, sodass Ihnen keine Gebühren mehr durch die Ressourcenanalyse entstehen.

5. Klicken Sie auf Speichern.

AWSDienste für die DevOps Guru-Analyse aktivieren

Amazon DevOps Guru kann die Leistung jeder AWS Ressource analysieren, die es unterstützt. Wenn es ein anormales Verhalten feststellt, generiert es Erkenntnisse 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 zusätzliche Analysen zur bestehenden DevOps Guru-Berichterstattung. Für andere ist eine Analyse erst möglich, wenn Sie diese Metriken aktivieren. Weitere Informationen erhalten Sie unter Ermitteln Sie den Versicherungsschutz für DevOps Guru und Aktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru.

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 Einrichten von Container-Insights auf Amazon ECS. Dadurch können CloudWatch Amazon-Gebühren anfallen.
- Amazon Elastic Kubernetes Service — Um Kennzahlen zu generieren, die DevOps Guru analysieren kann, folgen Sie den Schritten unter Einrichten von Container-Insights auf Amazon EKS und Kubernetes. 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 zu generieren, die DevOps Guru analysieren kann, müssen Sie Anforderungsmetriken aktivieren. Folgen Sie den Schritten unter Erstellen einer CloudWatch Metrikkonfiguration für alle Objekte in Ihrem Bucket. DevOpsGuru analysiert keine Amazon S3-Ressourcen, bis die Generierung dieser Metriken eingerichtet ist. Dadurch können Amazon S3-Gebühren anfallen. CloudWatch

Weitere Informationen finden Sie unter CloudWatchAmazon-Preise.

Arbeiten mit Erkenntnissen inDevOpsGuru

AmazonasDevOpsGuru generiert eineEinsichtwenn es anormales Verhalten in Ihren betrieblichen Anwendungen erkennt. DevOpsGuru analysiert die Kennzahlen, Ereignisse und mehr in derAWSRessourcen, die Sie bei der Einrichtung angegeben habenDevOpsGuru. Jeder Einblick enthält eine oder mehrere Empfehlungen, mit denen Sie das Problem beheben können. Es enthält auch eine Liste der Metriken, eine Liste der Protokollgruppen und eine Liste der Ereignisse, die zur Identifizierung des ungewöhnlichen Verhaltens verwendet wurden.

Es gibt zwei Arten von Erkenntnissen.

- ReaktivInsights enthält Empfehlungen, mit denen Sie Probleme lösen können, die derzeit auftreten.
- ProaktivInsights enthält Empfehlungen, die sich mit Problemen befassen, dieDevOpsGuru sagt voraus, dass dies in der Zukunft geschehen wird.

Themen

AnsehenDevOpsEinblicke in Guru

Sie können Ihre Erkenntnisse mit demAWS Management Console.

Sehen Sie sich Ihre anDevOpsEinblicke in Guru

1. Öffne den AmazonasDevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie das Navigationsfenster und wählen SieEinblicke.
3. Auf derReaktivAuf der Registerkarte sehen Sie eine Liste mit reaktiven Erkenntnissen. Auf derProaktivAuf der Registerkarte sehen Sie eine Liste mit proaktiven Erkenntnissen.
4. (Optional) Verwenden Sie einen oder mehrere der folgenden Filter, um die Erkenntnisse zu finden, nach denen Sie suchen.

- Wähle denReaktivoderProaktivTab, abhängig von der Art der Information, nach der Sie suchen.
- Wählen SieErkenntnisse filternund wählen Sie dann eine Option, um einen Filter anzugeben. Sie können eine Kombination aus Status-, Schweregrad-, Ressourcen- und Tagfiltern hinzufügen. Benutze eineAWSTag-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 DevOpsGuru-Anwendungen.

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

- Wählen oder geben Sie einen Zeitraum an, um nach der Erstellungszeit von Insights zu filtern.
  - 12 hzeigt Erkenntnisse, die in den letzten 12 Stunden erstellt wurden.
  - 1dzeigt Erkenntnisse, die am vergangenen Tag erstellt wurden.
  - 1wzeigt Erkenntnisse, die in der vergangenen Woche erstellt wurden.
  - 1 mzeigt Erkenntnisse, die im letzten Monat erstellt wurden.
  - Benutzerdefiniertermöglicht die Angabe eines anderen Zeitbereichs. Der maximale Zeitraum, den Sie zum Filtern von Erkenntnissen verwenden können, beträgt 180 Tage.

5. Um Details zu einer Insight anzuzeigen, wählen Sie ihren Namen.

Erkenntnisse verstehen in derDevOpsGuru-Konsole

Nutze den AmazonDevOpsGuru-Konsole, um nützliche Informationen in Ihren Erkenntnissen einzusehen, die Ihnen helfen, anomales Verhalten zu diagnostizieren und zu beheben. WannDevOpsGuru analysiert Ihre Ressourcen und findet verwandte AmazonCloudWatchMetriken,AWS CloudTrailEreignisse und Betriebsdaten, die auf ungewöhnliches Verhalten hinweisen, liefern Erkenntnisse, die Empfehlungen zur Behebung des Problems sowie Informationen zu den zugehörigen Kennzahlen und Ereignissen enthalten. Verwenden Sie Insight-Daten mitBest Practices in DevOps Guruzur Behebung von Betriebsproblemen, die festgestellt wurden vonDevOpsGuru.

Um sich einen Einblick anzusehen, folgen Sie den Schritten unterEinblicke anzeigenum einen zu finden, wählen Sie seinen Namen. Die Insight-Seite enthält die folgenden Details.

Überblick über Insight

Verwenden Sie diesen Abschnitt, um sich einen allgemeinen Überblick über die Erkenntnisse zu verschaffen. Sie können den Status des Insights sehen (Laufendodergeschlossen), wie vieleAWS CloudFormationStacks sind davon betroffen, wann der Insight gestartet, beendet und zuletzt aktualisiert wurde, sowie das zugehörige Operationselement, falls es eines gibt.

Wenn eine Einsicht gruppiert ist unterStapelebene, dann können Sie die Anzahl der betroffenen Stapel wählen, um deren Namen zu sehen. Das ungewöhnliche Verhalten, das zu den Erkenntnissen geführt hat, trat bei Ressourcen auf, die von den betroffenen Stacks erstellt wurden. Wenn eine Einsicht gruppiert ist unterKontoebene, dann ist die Zahl Null oder erscheint nicht.

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

Insight-Name

Der Name einer Insight hängt davon ab, ob sie in derStapelebeneoder derKontoebene.

- StapelebeneInsight-Namen beinhalten den Namen des Stacks, der die Ressource mit ihrem anomalen Verhalten enthält.
- KontoebeneInsight-Namen enthalten keinen Stack-Namen.

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

Aggregierte Kennzahlen

Wähle denAggregierte KennzahlenTabulatortaste, um Metriken anzuzeigen, die sich auf den Insight beziehen. In der Tabelle steht jede Zeile für eine Metrik. Du kannst sehen, welcheAWS CloudFormationstack hat die Ressource erstellt, die die Metrik ausgegeben hat, den Namen der Ressource und ihren Typ. Nicht alle Metriken sind mit einem verknüpftAWS CloudFormationstapeln oder einen Namen haben.

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

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

- Wählen SieAnsicht inCloudWatchum zu sehen, wie die Metrik in derCloudWatchKonsole. Weitere Informationen finden Sie unterStatistikenundAbmessungenin derAmazonasCloudWatchBenutzerleitfaden.
- Zeigen Sie mit der Maus auf das Diagramm, um Details zu den anomalen Metrikdaten und zu dem Zeitpunkt ihres Auftretens anzuzeigen.
- Wählen Sie das Feld mit dem Abwärtspfeil, um ein PNG-Bild des Diagramms herunterzuladen.

Graphische Anomalien

Wähle denGraphische AnomalienTabulator, 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 anhand von Statistiken untersuchen und untersuchen. Die Grafiken sind nach Metriknamen gruppiert. In jeder Kachel können Sie einen bestimmten Zeitbereich in der Zeitleiste 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 (1 H,3H,12 H,1D,3D,1W, oder2 W).

Wählen SieAlle Statistiken und Dimensionen anzeigenum Details über die Anomalie zu sehen. In dem sich öffnenden Fenster können Sie:

- Wählen SieAnsicht inCloudWatchum zu sehen, wie die Metrik in derCloudWatchKonsole.

- Zeigen Sie mit der Maus auf das Diagramm, um Details zu den anomalen Metrikdaten und zu dem Zeitpunkt ihres Auftretens anzuzeigen.
- Wählen SieStatistikenoderAbmessungum die Anzeige des Diagramms anzupassen. Weitere Informationen finden Sie unterStatistikenundAbmessungeninderAmazonasCloudWatchBenutzerleitfaden.

Protokollgruppen

Wenn Sie die Erkennung von Protokollanomalien aktivieren,DevOpsGuru markiert deineCloudWatchProtokollgruppen, damit Sie Protokollgruppen einsehen können, die sich auf Ihre Erkenntnisse beziehen. In derGruppen protokollierenIm Abschnitt 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 Zeitspannen an, in denen in einer Protokollgruppe Protokollanomalien auftraten.

Wählen Sie eine violette Linie in der Zeitleiste, um ein Beispiel mit Informationen zu Log-Anomalien wie Keyword-Ausnahmen und numerischen Abweichungen anzuzeigen. Wählen SieDetails zur Protokollgruppe anzeigenum Log-Anomalien anzuzeigen. In dem sich öffnenden Fenster können Sie:

- Sehen Sie sich ein Diagramm mit Protokollanomalien und relevanten Ereignissen an.
- Zeigen Sie mit der Maus auf das Diagramm, um Details zu den anomalen Protokolldaten und dem Zeitpunkt ihres Auftretens anzuzeigen.
- Lassen Sie sich Protokollanomalien detailliert mit Beispielmeldungen, Häufigkeit des Auftretens, entsprechenden Empfehlungen und Zeitpunkt des Auftretens anzeigen.
- Klicken Sie aufDetails anzeigen inCloudWatchum Protokollzeilen aus einer Log-Anomalie anzuzeigen.

Zugehörige Ereignisse

InVerwandte Ereignisse, ansehenAWS CloudTrailEreignisse, die mit Ihrer Einsicht zusammenhängen. Nutzen Sie diese Ereignisse, um die zugrunde liegende Ursache des anomalen Verhaltens zu verstehen, zu diagnostizieren und zu beheben.

Empfehlungen

InEmpfehlungen, können Sie sich Vorschläge ansehen, die Ihnen bei der Lösung des zugrunde liegenden Problems helfen könnten. WannDevOpsGuru erkennt anormales Verhalten und versucht, Empfehlungen auszusprechen. Ein Insight kann eine, mehrere oder gar keine Empfehlungen enthalten.

Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden

Ein Einblick ist gruppiert unterStapelebeneoder derKontoebene. Wenn eine Erkenntnis für eine Ressource generiert wird, die sich in einerAWS CloudFormationStapel, dann ist es einStapelebeneEinblick. Ansonsten ist es einKontoebeneEinblick.

Wie ein Stapel gruppiert wird, kann davon abhängen, wie Sie Ihre Ressourcenanalyse-Abdeckung in Amazon konfiguriert haben.DevOpsGuru.

Wenn Ihr Versicherungsschutz definiert ist durchAWS CloudFormationStapel

Alle Ressourcen, die in den von Ihnen ausgewählten Stacks enthalten sind, werden analysiert, und alle erkannten Erkenntnisse werden imStapelebene.

Wenn Ihr Versicherungsschutz Ihr aktueller istAWSKonto und Region

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

- Erkenntnisse, die aus einer Ressource generiert werden, die nicht Teil eines Stacks ist, werden in derKontoebene.
- Erkenntnisse, die aus einer Ressource generiert wurden, die sich in einem der ersten 10.000 analysierten Stapel befindet, sind in derStapelebene.
- Erkenntnisse, die aus einer Ressource generiert wurden, die nicht in einem der ersten 10.000 analysierten Stacks enthalten sind, werden in derKontoebene. Beispielsweise werden Erkenntnisse, die für eine Ressource im 10.001. analysierten Stapel generiert wurden, in derKontoebene.

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

Schweregrade von Erkenntnissen verstehen

Eine Einsicht kann einen von drei Schweregraden haben:hoch,Mittel, oderniedrig. Ein Einblick wird von Amazon erstelltDevOpsGuru, nachdem es verwandte Anomalien erkannt hat und jeder Anomalie einen Schweregrad zuweist. DevOpsDer Guru weist einer Anomalie einen Schweregrad vonhoch,Mittel, oderniedrigunter Verwendung von Domänenwissen und jahrelanger kollektiver Erfahrung. Der Schweregrad einer Erkenntnis wird durch die schwerwiegendste Anomalie bestimmt, die zur Entstehung der Erkenntnis beigetragen hat.

- Wenn der Schweregrad aller Anomalien, die die Erkenntnisse generiert haben,niedrig, dann ist der Schweregrad der Einsichtniedrig.
- Wenn der höchste Schweregrad aller Anomalien, die zu der Erkenntnis geführt haben,Mittel, dann ist der Schweregrad der EinsichtMittel. Der Schweregrad einiger der Anomalien, die zu den Erkenntnissen geführt haben, könnte wie folgt seinniedrig.
- Wenn der höchste Schweregrad aller Anomalien, die zu der Erkenntnis geführt haben,hoch, dann ist der Schweregrad der Einsichthoch. Der Schweregrad einiger der Anomalien, die zu den Erkenntnissen geführt haben, könnte wie folgt seinniedrigoderMittel.

Überwachen von Datenbanken mit DevOpsGuru

DevOpsGuru bietet einen erheblichen Wert für den Betrieb von Datenbanken auf AWS. Durch die Nutzung seiner Machine-Learning-Algorithmen DevOpskannGuru 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 bestimmter DevOpsGuru-Anwendungsfälle für verschiedene AWS Datenbankservices.

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

Themen

Überwachung relationaler Datenbanken mit DevOpsGuru

DevOpsGuru ruft aus zwei primären Datenquellen ab, um in relationalen Datenbanken nach Erkenntnissen und Anomalien zu suchen. Für Amazon RDS und werden Amazon Redshift CloudWatch verkaufte Metriken für alle Instance-Typen analysiert. Für Amazon RDS werden Performance-Insights-Daten auch für die folgenden Engine-Typen erfasst: RDS für PostgreSQL , Aurora PostgreSQL und Aurora MySQL .

Überwachen von Datenbankoperationen in Amazon RDS

Dieser Abschnitt enthält spezifische Informationen zu Anwendungsfällen und Metriken, die in DevOpsGuru für RDS überwacht werden, einschließlich Daten aus CloudWatch verkauften Metriken und Performance Insights. Weitere Informationen zu DevOpsGuru für RDS, einschließlich wichtiger Konzepte, Konfigurationen und Vorteile, finden Sie unter the section called “Arbeiten mit Anomalien in DevOpsGuru für RDS”.

Überwachen von RDS mithilfe von Daten aus CloudWatch verkauften Metriken

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

Da diese Metriken standardmäßig verkauft werden, ist bei der Überwachung Ihrer RDS-Instances mit DevOpsGuru keine weitere Konfiguration erforderlich, um Erkenntnisse zu gewinnen. DevOpsGuru erstellt automatisch eine Grundlage für diese Metriken auf der Grundlage historischer Muster 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 CloudWatch verkauften Metriken.

AWS Von DevOpsGuru überwachte Ressource	Szenario, das DevOpsGuru identifiziert	CloudWatch Überwachte Metriken
Amazon RDS (alle Instance-Typen)	CPU oder Arbeitsspeicher erreichen Limits	DBLoad , DBLoadCPU
RDS for PostgreSQL	Hohe Replikations-Slot-Verzögerung	OldestReplicationSlotLag

Zusätzliche CloudWatch angebotene Metriken von Amazon-RDS-Instances, die DevOpsGuru überwacht:

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- FailedSQLServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Überwachen von RDS mithilfe von Daten aus Performance Insights

Für bestimmte Arten von Amazon-RDS-Instances wie Aurora PostgreSQL, Aurora MySQL und RDS für PostgreSQL entsperren Sie mehr Funktionen von der DevOpsGuru-Überwachung, indem Sie sicherstellen, dass Performance Insights auf diesen Instances aktiviert ist.

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

Szenario, das DevOpsGuru identifiziert, um einen reaktiven Einblick zu generieren
Sperrkonflikte
Fehlender Index
Fehlkonfiguration des Anwendungspools
Suboptimale JDBC-Standardeinstellungen

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

AWS Von DevOpsGuru überwachte Ressource	Szenario, das DevOpsGuru identifiziert, um einen proaktiven Einblick zu generieren
Aurora MySQL	Die InnoDB-Verlaufsliste wächst zu groß, was zu einer Leistungseinbußen führen kann, z. B. zu langwieriger Datenbankabschaltzeit
Aurora MySQL	Eine Zunahme temporärer Tabellen, die auf der Festplatte erstellt wurden und die die Datenbankleistung beeinträchtigen können
RDS für PostgreSQL , Aurora PostgreSQL	Eine Verbindung, die bei der Transaktion zu lange inaktiv war, potenzielle Auswirkungen, wenn Sperren gehalten werden, andere Abfragen blockiert werden und verhindert wird, dass eine Bereinigung (einschließlich Selbstbereinigung) tote Zeilen bereinigt

Überwachen von Datenbankoperationen in Amazon Redshift

DevOpsGuru ist in der Lage, Ihre Amazon Redshift Ressourcen zu überwachen, indem CloudWatch Standardmetriken erfasst werden, einschließlich CPU-Auslastung und Prozentsatz des verwendeten Speicherplatzes. Da diese Metriken standardmäßig verkauft werden, ist keine weitere Konfiguration erforderlich, damit DevOpsGuru Ihre Amazon Redshift Ressourcen automatisch überwachen kann. DevOpsGuru erstellt basierend auf historischen Mustern eine Grundlage für diese Metriken und vergleicht sie mit Echtzeitdaten, um Anomalien zu erkennen.

Szenario, das DevOpsGuru identifiziert	CloudWatch Überwachte Metriken
Erkennen einer hohen CPU-Auslastung einer Amazon Redshift Instance, die durch Faktoren wie Cluster-Workload, verzerrte und unsortier te Daten oder Führungsknotenaufgaben verursacht wird	CPUUtilization
Erkennen, wenn einer Amazon Redshift Instance aufgrund von Problemen mit der Abfrageverarbeitung, Verteilung und dem Sortierschlüssel, Wartungsvorgängen oder Tomblaze-Blöcken der Speicherplatz ausgeht	PercentageDiskSpaceUsed

Zusätzliche CloudWatch angebotene Metriken von Amazon Redshift Instances, die DevOpsGuru überwacht:

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

- WLMQueueLength
- WLMQueueWaitTime
- WLMQueryDuration
- WriteLatency

Arbeiten mit Anomalien in DevOpsGuru für RDS

DevOpsGuru erkennt, analysiert und gibt Empfehlungen für unterstützte AWS Ressourcen, einschließlich Amazon-RDS-Engines. Für Datenbank-Instances von Amazon Aurora und RDS für PostgreSQL mit aktivierten Performance Insights DevOpsbietetGuru für RDS detaillierte, datenbankspezifische Analysen von Leistungsproblemen und empfiehlt Korrekturmaßnahmen.

Themen

Übersicht über DevOpsGuru für RDS

Im Folgenden finden Sie eine Zusammenfassung der wichtigsten Vorteile und Features von DevOpsGuru für RDS. Hintergrundinformationen zu Erkenntnissen und Anomalien finden Sie unter DevOpsGuru-Konzepte.

Themen

Vorteile von DevOpsGuru für RDS

Wenn Sie für eine Amazon-RDS-Datenbank verantwortlich sind, wissen Sie möglicherweise nicht, dass ein Ereignis oder eine Regression auftritt, 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 (Database Administrator, DBA) zu wenden oder sich auf Tools von Drittanbietern zu verlassen, können Sie den Empfehlungen von DevOpsGuru für RDS folgen.

Sie profitieren von den folgenden Vorteilen aus der detaillierten Analyse von DevOpsGuru für RDS:

Schnelle Diagnose

DevOpsGuru für RDS überwacht und analysiert kontinuierlich Datenbanktelemetrie. Performance Insights, Enhanced Monitoring und Amazon CloudWatch sammeln Telemetriedaten für Ihre Datenbank-Instances. DevOpsGuru for RDS verwendet statistische und Machine-Learning-Techniken, um diese Daten zu analysieren und Anomalien zu erkennen. Weitere Informationen zu Telemetriedaten für Amazon-Aurora-Datenbanken finden Sie unter Überwachen der DB-Last mit Performance Insights auf Amazon Aurora und Überwachen des Betriebssystems mithilfe von Enhanced Monitoring im Amazon-Aurora-Benutzerhandbuch. Weitere Informationen zu Telemetriedaten für andere Amazon-RDS-Datenbanken finden Sie unter Überwachen der DB-Last mit Performance Insights auf 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. Beispielsweise DevOpskönnteGuru für RDS empfehlen, dass Sie bestimmte Warteereignisse 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 für 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 ausführen und möglicherweise Datenbankressourcen blockiert lassen. DevOpsGuru bietet dann Empfehlungen, die Ihnen helfen, Probleme zu lösen, bevor sie zu größeren Problemen werden.

Fundierte Kenntnisse der Amazon-Ingenieure und Machine Learning

Um Leistungsprobleme zu erkennen und Engpässe zu beheben, stützt DevOpssichGuru für RDS auf Machine Learning (ML) und erweiterte statistische Analysen. Amazon-Datenbankingenieure

haben zur Entwicklung des DevOpsGuru für RDS-Erkenntnisse beigetragen, die viele Jahre der Verwaltung von Hunderttausenden von Datenbanken umfassen. Anhand dieses kollektiven Wissens kann DevOpsGuru für RDS Ihnen bewährte Methoden beibringen.

Wichtige Konzepte für die Optimierung der Datenbankleistung

DevOpsGuru für RDS geht davon aus, dass Sie mit einigen wichtigen Leistungskonzepten vertraut sind. Weitere Informationen zu diesen Konzepten finden Sie unter Übersicht über Performance Insights im Amazon-Aurora-Benutzerhandbuch oder Übersicht über 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 für das Betriebssystem (OS) bereit, auf dem Ihre DB-Instance ausgeführt wird. Sie können alle Systemmetriken und Prozessinformationen für Ihre Amazon-RDS-DB-Instances in der Amazon-RDS-Konsole anzeigen. DevOpsGuru für RDS überwacht und bietet Einblicke in einige dieser Metriken. Weitere Informationen finden Sie unter Überwachen von Metriken in einem Amazon-Aurora-Cluster oder Überwachen von Metriken in einer Amazon Relational Database Service-Instance.

Problemerkennung

DevOpsGuru für RDS verwendet Datenbank- und Betriebssystemmetriken (OS), um kritische Probleme mit der Datenbankleistung zu erkennen, unabhängig davon, ob diese Probleme drosseln oder anstehen. Es gibt zwei primäre Möglichkeiten, wie DevOpsGuru für die RDS-Problemerkennung funktioniert:

- Verwenden von Schwellenwerten
- Verwenden von Anomalien

Erkennen von Problemen mit Schwellenwerten

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

Beispielsweise DevOpskannGuru für RDS die Anzahl der temporären Tabellen überwachen, die die Festplatte über einen Zeitraum von 15 Minuten verwenden, und einen Einblick erstellen, wenn die Rate temporärer Tabellen, die die Festplatte pro Sekunde verwenden, ungewöhnlich hoch ist. Eine erhöhte Nutzung temporärer Tabellen auf der Festplatte kann sich auf die Datenbankleistung auswirken. Wenn Sie diese Situation an den Tag legen, bevor sie kritisch wird, hilft Ihnen DevOpsGuru für RDS dabei, Korrekturmaßnahmen zu ergreifen, um Probleme zu vermeiden.

Erkennen von Problemen mit Anomalien

Schwellenwerte bieten zwar eine einfache und effektive Möglichkeit, Datenbankprobleme zu erkennen, sind jedoch in einigen Situationen nicht ausreichend. Stellen Sie sich einen Fall vor, in dem Metrikwerte aufgrund eines bekannten Prozesses, z. B. eines täglichen Berichtsauftrags, regelmäßig in ein potenziell problematisches Verhalten steigen. Da solche Spitzen erwartet werden, wäre das Erstellen von Erkenntnissen und Benachrichtigungen für jeden davon konproduktiv und würde wahrscheinlich zu Verschlechterungen bei Warnungen führen.

Es ist jedoch immer noch erforderlich, Spitzen zu erkennen, die sehr ungewöhnlich sind, da Metriken, die viel höher als der Rest oder viel länger sind, echte Probleme mit der Datenbankleistung darstellen könnten. Um dieses Problem zu beheben, DevOpsüberwachtGuru für RDS bestimmte Metriken, um zu erkennen, wann das Verhalten einer Metrik sehr ungewöhnlich oder ungewöhnlich wird. DevOpsGuru meldet diese Anomalien dann in Erkenntnissen.

Beispielsweise DevOpskönnteGuru für RDS einen Einblick geben, wenn die DB-Last nicht nur hoch ist, sondern auch erheblich von ihrem üblichen Verhalten abweicht, was auf eine große unerwartete Verlangsamung der Datenbankoperationen hinweist. Indem Sie nur die ungewöhnlichen DB-Lastspitzen erkennen, können Sie sich mit DevOpsGuru für RDS auf die wirklich wichtigen Probleme konzentrieren.

DB-Last

Das Schlüsselkonzept für die Datenbankoptimierung ist die Datenbanklastmetrik (DB-Last). Die DB-Last gibt an, wie ausgelastet Ihre Datenbank zu einem bestimmten Zeitpunkt ist. Eine Erhöhung der DB-Last 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, nimmt Performance Insights Stichproben für die Anzahl der aktiven Sitzungen pro Sekunde. Für einen bestimmten Zeitraum ist der AAS die Gesamtzahl der aktiven Sitzungen geteilt durch die Gesamtzahl der Stichproben. Ein AAS-Wert von 2 bedeutet, dass im Durchschnitt 2 Sitzungen zu einem bestimmten Zeitpunkt in Anfragen aktiv waren.

Eine Analogie zur DB-Last ist die Aktivität in einem Lager. Angenommen, das Lager beschäftigt 100 Mitarbeiter. Wenn eine Bestellung eingeht, erfüllt 1 Mitarbeiter die Bestellung, während die anderen Mitarbeiter im Leerlauf sind. Wenn 100 oder mehr Bestellungen eingehen, erfüllen alle 100 Auftragnehmer gleichzeitig Bestellungen. 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 Datenbanklast im Amazon-Aurora-Benutzerhandbuch oder Datenbanklast im Amazon-RDS-Benutzerhandbuch.

Warteereignisse

Ein Warteereignis ist eine Art der Datenbankinstrumentierung, die Ihnen mitteilt, auf welche Ressource eine Datenbanksitzung wartet, damit sie fortfahren kann. Wenn Performance Insights aktive Sitzungen zur Berechnung der Datenbanklast zählt, werden auch die Warteereignisse aufgezeichnet, die dazu führen, dass die aktiven Sitzungen warten. Mit dieser Technik kann Performance Insights Ihnen zeigen, welche Warteereignisse zur DB-Last beitragen.

Jede aktive Sitzung läuft entweder auf der CPU oder wartet. Sitzungen verbrauchen beispielsweise CPU, wenn sie Speicher suchen, 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 häufig, die Ressourcen zu finden, auf die Sitzungen warten. Beispielsweise könnten zwei oder drei Warteereignisse 90 % der DB-Last ausmachen. Diese Maßnahme bedeutet, dass aktive Sitzungen im Durchschnitt die meiste Zeit damit verbringen, auf eine kleine Anzahl von Ressourcen zu warten. Wenn Sie die Ursache dieser 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 könnte ein anderer Auftragnehmer derzeit die Drucker neu auffüllen, oder es ist möglicherweise kein Drucker verfügbar. Oder das System, mit dem der Bestellstatus eingegeben wurde, ist möglicherweise langsam. Je länger der Auftragnehmer wartet, desto länger dauert die Erfüllung der Bestellung. Warten ist ein natürlicher Bestandteil des Lager-Workflows, aber wenn die Wartezeit übermäßig 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 Optimieren mit Warteereignissen für Aurora PostgreSQL und Optimieren mit Warteereignissen für Aurora MySQL im Amazon-Aurora-Benutzerhandbuch.

Weitere Informationen zu Warteereignissen in anderen Amazon-RDS-Datenbanken finden Sie unter Optimieren mit Warteereignissen für RDS für PostgreSQL im Amazon-RDS-Benutzerhandbuch.

Schlüsselkonzepte für DevOpsGuru für RDS

Ein Einblick wird von DevOpsGuru generiert, wenn es ungewöhnliches oder problematisches Verhalten in Ihren Betriebsanwendungen erkennt. Ein Insight enthält Anomalien für eine oder mehrere Ressourcen. Eine Anomalie stellt eine oder mehrere zugehörige Metriken dar, die von DevOpsGuru erkannt werden und unerwartet oder ungewöhnlich sind.

Ein Insight hat den Schweregrad hoch , mittel oder niedrig . Der Erkenntnisschweregrad wird durch die schwerwiegendste Anomalie bestimmt, die zur Erstellung des Einblicks beigetragen hat. Wenn die Erkenntnis AWS-ECS_MemoryUtilization_and_others beispielsweise eine Anomalie mit niedrigem Schweregrad und eine andere mit hohem Schweregrad enthält, ist der Gesamtschweregrad der Erkenntnis hoch.

Wenn für Amazon-RDS-DB-Instances Performance Insights aktiviert ist, DevOpsbietetGuru für RDS detaillierte Analysen und Empfehlungen in den Anomalien für diese Instances. Um eine Anomalie zu identifizieren, DevOpsentwickeltGuru für RDS eine Baseline für Datenbankmetrikwerte. DevOpsGuru für RDS vergleicht dann aktuelle Metrikwerte mit der historischen Baseline.

Themen

Proaktive Einblicke

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

Jede Seite mit proaktiven Einblicken enthält Details zu einer Anomalie.

Reaktive Einblicke

Ein reaktiver Einblick identifiziert anomales Verhalten, sobald es auftritt. Es enthält Anomalien mit Empfehlungen, zugehörigen Metriken und Ereignissen, die Ihnen helfen, die Probleme jetzt zu verstehen und zu beheben.

Kausale Anomalien

Eine kausale Anomalie ist eine Anomalie der obersten Ebene innerhalb eines Einblicks. Sie wird als Primäre Metrik auf der Seite mit den Anomaliedetails in der DevOpsGuru-Konsole angezeigt. Die Datenbanklast (DB-Last) ist die kausale Anomalie für DevOpsGuru für RDS. Beispielsweise könnte der Einblick AWS-ECS_MemoryUtilization_and_others mehrere Metrikanomalien aufweisen, von denen eine 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 im Abschnitt Verwandte Metriken der Seite mit den Anomaliedetails in der DevOpsGuru-Konsole angezeigt. Jede kontextbezogene Anomalie beschreibt ein bestimmtes Amazon-RDS-Leistungsproblem, das untersucht werden muss. Eine kausale Anomalie kann beispielsweise die folgenden kontextbezogenen Anomalien umfassen:

- CPU-Kapazität überschritten – Die CPU-Ausführungswarteschlange oder die CPU-Auslastung sind über normal.
- Datenbankspeicher niedrig – Prozesse haben nicht genügend Speicher.
- Datenbankverbindungen mit Spitzenwert – Die Anzahl der Datenbankverbindungen ist über normal.

Empfehlungen

Jeder Einblick enthält mindestens eine vorgeschlagene Aktion. Die folgenden Beispiele sind Empfehlungen, die von DevOpsGuru für RDS generiert wurden:

- 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 die damit verbundene Spitze 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 übermäßige Speicheroperationen ausführen, z. B. In-Memory-Sortiervorgänge oder große Joins.
- Untersuchen Sie die hohe E/A-Nutzung für die folgenden SQL-IDs *`:list_of_IDs`* .
- Suchen Sie nach Anweisungen, die große Mengen temporärer Daten erstellen, z. B. solche, die große Sortierungen durchführen oder große temporäre Tabellen verwenden.
- Überprüfen Sie Anwendungen, um zu sehen, was den Anstieg der Datenbank-Workload verursacht.
- Erwägen Sie, das MySQL-Leistungsschema zu aktivieren.
- Suchen Sie nach lang andauernden Transaktionen und beenden Sie sie mit einem Commit oder Rollback.
- Konfigurieren Sie den Parameter idle_in_transaction_session_timeout, um jede Sitzung zu beenden, die länger als die angegebene Zeit im Status „Leerlauf in Transaktion“ ist.

Funktionsweise von DevOpsGuru für RDS

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

Themen

- Datenerfassung und -analyse
- Veröffentlichung von Anomalien

Datenerfassung und -analyse

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

DevOpsGuru für RDS verwendet Machine Learning und erweiterte statistische Analysen, um die Daten zu analysieren, die es aus Performance Insights sammelt. Wenn DevOpsGuru für RDS Leistungsprobleme erkennt, fährt es mit dem nächsten Schritt fort.

Veröffentlichung von Anomalien

Ein Problem mit der Datenbankleistung wie eine hohe DB-Last kann die Servicequalität für Ihre Datenbank beeinträchtigen. Wenn DevOpsGuru ein Problem in einer RDS-Datenbank erkennt, veröffentlicht es einen Einblick im Dashboard. Der Einblick enthält eine Anomalie für die Ressource AWS/RDS .

Wenn Performance Insights für Ihre Instances aktiviert ist, enthält die Anomalie eine detaillierte Analyse des Problems. DevOpsGuru für RDS empfiehlt außerdem, dass Sie eine Untersuchung oder bestimmte Korrekturmaßnahmen durchführen. Die Empfehlung könnte beispielsweise darin bestehen, eine bestimmte SQL-Anweisung mit hoher Last zu untersuchen, eine Erhöhung der CPU-Kapazität in Betracht zu ziehen oder idle-in-transaction Sitzungen zu schließen.

Unterstützte Datenbank-Engines

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

Amazon Aurora mit MySQL-Kompatibilität

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

Amazon Aurora mit PostgreSQL-Kompatibilität

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

Kompatibilität von Amazon RDS für PostgreSQL

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

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

Aktivieren von DevOpsGuru für RDS

Wenn Sie DevOpsGuru für RDS aktivieren, aktivieren Sie DevOpsGuru, um Anomalien in Ressourcen wie DB-Instances zu analysieren. Amazon RDS macht es einfach, empfohlene Funktionen für eine RDS-DB-Instance oder einen DB-Cluster zu erkennen und zu aktivieren. Um dies zu erreichen, führt RDS API-Aufrufe an andere -Services wie Amazon EC2, DevOpsGuru und IAM durch. Wenn die RDS-Konsole diese API-Aufrufe durchführt, AWS CloudTrail protokolliert sie zur besseren Sichtbarkeit.

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

Themen

- Aktivieren von Performance Insights für Ihre Amazon RDS-DB-Instances
- Konfigurieren von Zugriffsrichtlinien für DevOpsGuru für RDS
- Hinzufügen von Amazon RDS-DB-Instances zu Ihrer DevOpsGuru-Abdeckung

Aktivieren von Performance Insights für Ihre Amazon RDS-DB-Instances

Damit DevOpsGuru für 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, DevOpsbenachrichtigtGuru for RDS Sie an den folgenden Stellen:

Dashboard

Wenn Sie Erkenntnisse nach Ressourcentyp anzeigen, warnt Sie die RDS-Kachel, dass Performance Insights nicht aktiviert ist. Wählen Sie den Link, um Performance Insights in der Amazon-RDS-Konsole zu aktivieren.

Insights

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

Einstellungen

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

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

Konfigurieren von Zugriffsrichtlinien für DevOpsGuru für RDS

Damit ein Benutzer auf DevOpsGuru für RDS zugreifen kann, muss er über Berechtigungen aus einer der folgenden Richtlinien verfügen:

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

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

Hinzufügen von Amazon RDS-DB-Instances zu Ihrer DevOpsGuru-Abdeckung

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

In der DevOpsGuru-Konsole haben Sie die folgenden Optionen:

- Aktivieren Sie DevOpsGuru auf Kontoebene. Dies ist die Standardeinstellung. Wenn Sie diese Option wählen, DevOpsanalysiertGuru alle unterstützten AWS Ressourcen in Ihrem AWS-Region und AWS-Konto, einschließlich Amazon-RDS-Datenbanken.
- Geben Sie AWS CloudFormationStacks für DevOpsGuru für RDS an.

  Weitere Informationen finden Sie unter benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-Anwendungen.
- Markieren Sie Ihre Amazon-RDS-Ressourcen.

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

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

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

Analysieren von Anomalien in Amazon RDS

Wenn DevOpsGuru für RDS eine Leistungsanomalie im Dashboard veröffentlicht, führen Sie in der Regel die folgenden Schritte aus:

1. Zeigen Sie den Einblick im DevOpsGuru-Dashboard an. DevOpsGuru für RDS meldet sowohl reaktive als auch proaktive Einblicke.

   Weitere Informationen finden Sie unter Anzeigen von Erkenntnissen.
2. Anzeigen von Anomalien für AWS/RDS-Ressourcen.

   Weitere Informationen finden Sie unter Anzeigen reaktiver Anomalien und Anzeigen proaktiver Anomalien.
3. Reagieren Sie auf DevOpsGuru 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 wiederholt werden.

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

Anzeigen von Erkenntnissen

Greifen Sie auf die Seite Insights in der DevOpsGuru-Konsole zu, um reaktive und proaktive Einblicke zu finden. Von dort aus können Sie einen Einblick aus der Liste auswählen, um eine detaillierte Seite mit Metriken, Empfehlungen und weiteren Informationen über den Einblick anzuzeigen.

So zeigen Sie einen -Einblick an

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

Die Seite mit den detaillierten Einblicken wird angezeigt.

Anzeigen reaktiver Anomalien

Innerhalb eines Insights können Sie Anomalien für Amazon-RDS-Ressourcen anzeigen. Auf einer Seite mit reaktiven Einblicken können Sie im Abschnitt Aggregierte Metriken eine Liste von Anomalien mit entsprechenden Zeitplänen anzeigen. Es gibt auch Abschnitte, in denen Informationen zu Protokollgruppen und Ereignissen im Zusammenhang mit den Anomalien angezeigt werden. Ursachenanomalien in einem reaktiven Einblick verfügen jeweils über eine entsprechende Seite mit Details zur Anomalie.

Anzeigen der detaillierten Analyse einer reaktiven RDS-Anomalie

In dieser Phase führen Sie einen Drilldown in der Anomalie durch, um die detaillierte Analyse 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.

So führen Sie einen Drilldown auf die Seite mit den Anomaliedetails durch

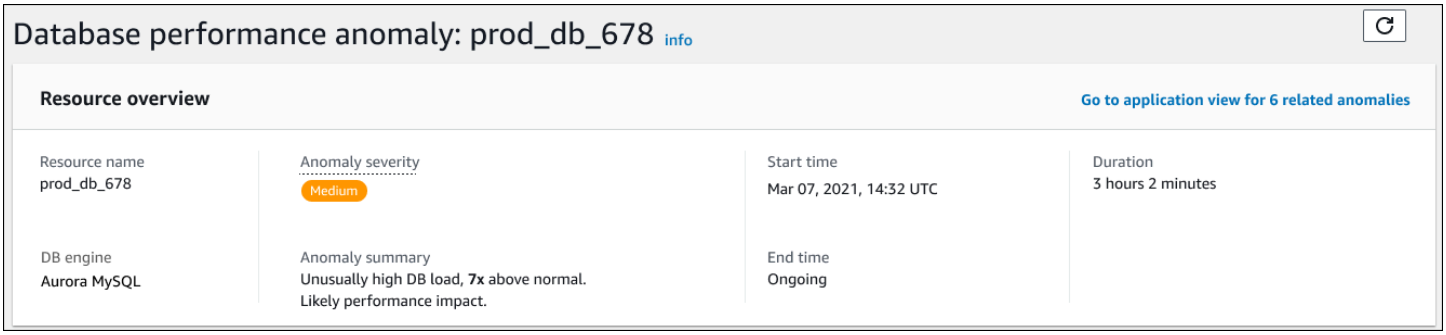
1. Suchen Sie auf der Insight-Seite eine aggregierte Metrik mit dem Ressourcentyp AWS/RDS .
2. Wählen Sie die Option View details aus.

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

Im Folgenden finden Sie Beschreibungen für die Komponenten der Detailseite.

Ressourcenübersicht

Der obere Abschnitt der Detailseite ist Ressourcenübersicht . In diesem Abschnitt wird die Leistungsanomalie zusammengefasst, die bei Ihrer Amazon RDS-DB-Instance auftritt.

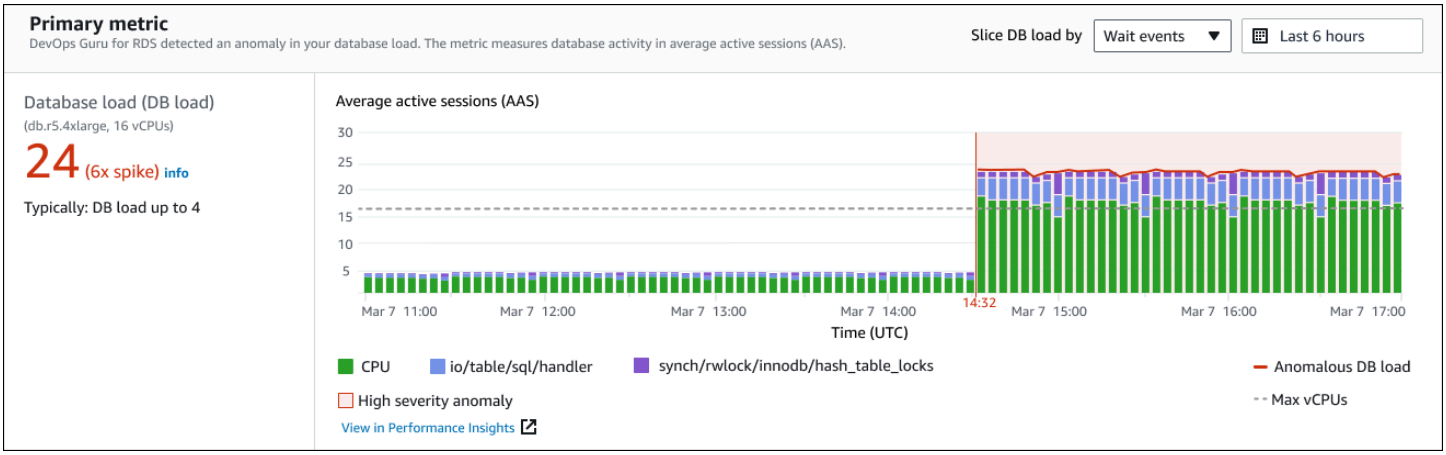


Dieser Abschnitt enthält die folgenden Felder:

- Ressourcenname – Der Name der DB-Instance, bei der die Anomalie auftritt. In diesem Beispiel heißt die Ressource prod_db_678.
- DB-Engine – Der Name der DB-Instance, bei der die Anomalie aufgetreten ist. In diesem Beispiel ist die Engine Aurora MySQL .
- Anomalieschweregrad – 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 ist Unnormal hohe DB-Last .
- Startzeit und Endzeit – Die Zeit, zu der die Anomalie begann und endete. Wenn die Endzeit Andauernd ist, tritt die Anomalie immer noch auf.
- Dauer – Die Dauer des anomalen Verhaltens. In diesem Beispiel ist die Anomalie andauernd und tritt seit 3 Stunden und 2 Minuten auf.

Primäre Metrik

Im Abschnitt Primäre Metrik wird die Telefonieanomalie zusammengefasst, bei der es sich um die Anomalie der obersten Ebene innerhalb des Insights handelt. Sie können sich die kausale Anomalie als das allgemeine Problem vorstellen, das bei Ihrer DB-Instance auftritt.



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

- Datenbanklast (DB-Last) – Eine Kategorisierung der Anomalie als Datenbanklastproblem. Die entsprechende Metrik in Performance Insights ist `DBLoad`. Diese Metrik wird auch in Amazon veröffentlicht CloudWatch.
- db.r5.4xlarge – Die DB-Instance-Klasse. Die Anzahl der vCPUs, die in diesem Beispiel 16 beträgt, entspricht der gepunkteten Linie im Diagramm Durchschnittliche aktive Sitzungen (AAS).
- 24 (6-fache Spitze) – Die DB-Last, gemessen in durchschnittlichen aktiven Sitzungen (AAS) während des im Insight gemeldeten Zeitintervalls. Daher waren zu einem bestimmten Zeitpunkt während des Zeitraums der Anomalie durchschnittlich 24 Sitzungen in der Datenbank aktiv. Die DB-Last ist das 6-fache der normalen DB-Last für diese Instance.
- In der Regel: DB-Last bis zu 4 – Die Baseline der DB-Last, gemessen in AAS, während einer typischen Workload. Der Wert 4 bedeutet, dass im normalen Betrieb durchschnittlich 4 oder weniger Sitzungen zu einem bestimmten Zeitpunkt in der Datenbank aktiv sind.

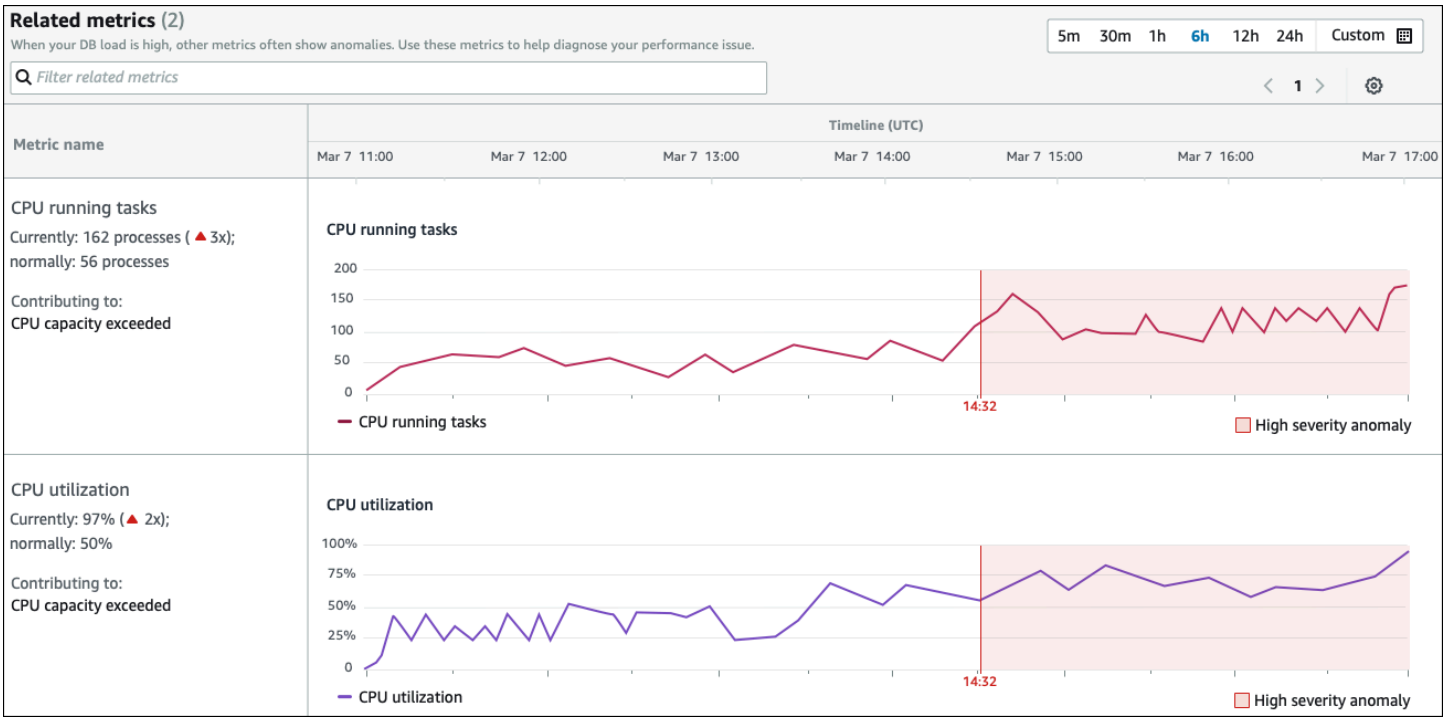
Standardmäßig wird das Lastdiagramm nach Warteereignissen aufgeteilt. Das bedeutet, dass für jeden Balken im Diagramm der größte farbige Bereich das Warteereignis darstellt, das am meisten zur gesamten DB-Last beiträgt. Das Diagramm zeigt den Zeitpunkt (in Rot), zu dem das Problem begann. Konzentrieren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

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

Die vorhergehenden Warteereignisse erscheinen für diese Aurora MySQL-Datenbank mehr als normal. 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-Benutzerhandbuch. Informationen zum Optimieren der Leistung mithilfe von Warteereignissen in RDS für PostgreSQL finden Sie unter Optimieren mit Warteereignissen für RDS für PostgreSQL im Amazon-RDS-Benutzerhandbuch.

Verwandte Metriken

Im Abschnitt Verwandte Metriken werden die kontextbezogenen Anomalien aufgeführt, bei denen es sich um spezifische Erkenntnisse innerhalb der kausalen Anomalie handelt. Diese Erkenntnisse enthalten zusätzliche Informationen zu den Leistungsproblemen.



Die Tabelle Zugehörige Metriken hat zwei Spalten: Metrikname und Timeline (UTC). Jede Zeile in der Tabelle entspricht einer bestimmten Metrik.

Die erste Spalte jeder Zeile enthält die folgenden Informationen:

- ***Name*** – Der Name der Metrik. Die erste Zeile identifiziert die Metrik als CPU-Ausführungsaufgaben.
- Derzeit – Der aktuelle Wert der Metrik. In der ersten Zeile ist der aktuelle Wert 162 Prozesse (3x).
- Normal – Die Baseline dieser Metrik für diese Datenbank, wenn sie normal funktioniert. DevOpsGuru für RDS berechnet die Baseline als 95. Perzentilwert über 1 Woche Verlauf. Die erste Zeile zeigt an, dass normalerweise 56 Prozesse auf der CPU ausgeführt werden.

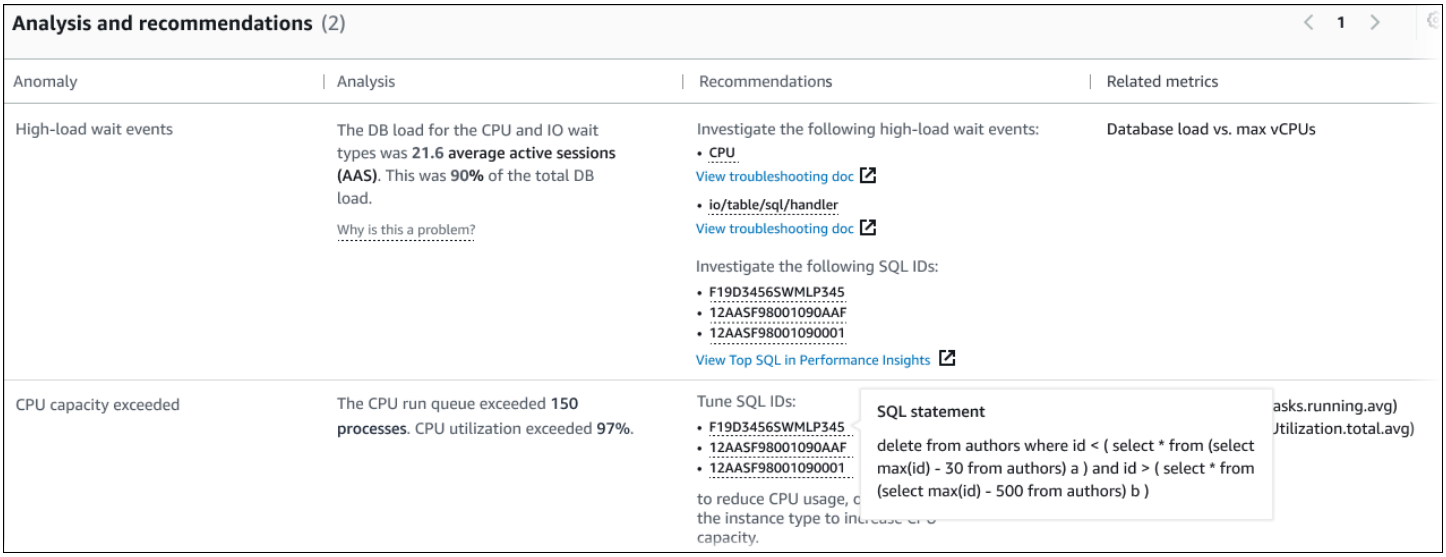
- Beitragend zu – Die Erkenntnis, die mit dieser Metrik verknüpft ist. In der ersten Zeile ist die Metrik für CPU-Ausführungsaufgaben mit der Anomalie verknüpft, bei der die CPU-Kapazität überschritten wurde.

Die Spalte Timeline zeigt ein Liniendiagramm für die Metrik. Der schattierte Bereich zeigt das Zeitintervall an, in dem DevOpsGuru für RDS die Erkenntnis als hochschwer eingestuft hat.

Analyse und Empfehlungen

Während die kausale Anomalie das Gesamtproblem beschreibt, beschreibt eine kontextbezogene Anomalie eine bestimmte Erkenntnis, die untersucht werden muss. Jede Erkenntnis entspricht einer Reihe verwandter Metriken.

Im folgenden Beispiel eines Abschnitts Analyse und Empfehlungen hat die Anomalie mit hoher DB-Last zwei Ergebnisse.



Diese Tabelle hat die folgenden Spalten:

- Anomalie – Eine allgemeine Beschreibung dieser kontextbezogenen Anomalie. In diesem Beispiel sind die erste Anomalie Warteereignisse mit hoher Last und die zweite ist eine Überschreitung der CPU-Kapazität.
- Analyse – Eine detaillierte Erklärung der Anomalie.

  In der ersten Anomalie tragen drei Wartetypen zu 90 % der DB-Last bei. In der zweiten Anomalie hat die CPU-Ausführungswarteschlange 150 überschritten, was bedeutet, dass zu einem bestimmten Zeitpunkt mehr als 150 Sitzungen auf CPU-Zeit warteten. Die CPU-Auslastung betrug

über 97 %, was bedeutet, dass die CPU während der Dauer des Problems zu 97 % ausgelastet war. Daher war die CPU fast kontinuierlich belegt, während durchschnittlich 150 Sitzungen darauf warteten, auf der CPU ausgeführt zu werden.

- Empfehlungen – Die vorgeschlagene Benutzerantwort auf die Anomalie.

  In der ersten Anomalie DevOpsempfiehltGuru für RDS, die Warteereignisse `cpu` und zu untersuchen`io/table/sql/handler`. Informationen zum Optimieren der Datenbankleistung basierend auf diesen Ereignissen finden Sie unter cpu und io/table/sql/handler im Amazon-Aurora-Benutzerhandbuch.

  In der zweiten Anomalie DevOpsempfiehltGuru für RDS, den CPU-Verbrauch zu 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 Messungen für die Anomalie liefern. Weitere Informationen zu diesen Metriken finden Sie unter Metrikreferenz für Amazon Aurora im Amazon-Aurora-Benutzerhandbuch oder Metrikreferenz für Amazon RDS im Amazon-RDS-Benutzerhandbuch.

  In der ersten Anomalie DevOpsempfiehltGuru für RDS, die DB-Last mit der maximalen CPU für Ihre Instance zu vergleichen. In der zweiten Anomalie besteht die Empfehlung darin, die CPU-Ausführungswarteschlange, die CPU-Auslastung und die SQL-Ausführungsrate zu betrachten.

Anzeigen proaktiver Anomalien

In Insights können Sie Anomalien für Amazon-RDS-Ressourcen anzeigen. Jeder proaktive Einblick enthält Details zu einer proaktiven Anomalie. Auf einer Seite mit proaktiven Einblicken können Sie eine Übersicht über Einblicke, detaillierte Metriken zur Anomalie und Empfehlungen zur Vermeidung zukünftiger Probleme anzeigen. Um eine proaktive Anomalie anzuzeigen, gehen Sie zur Seite für proaktive Einblicke.

Überblick über Insight

Der Abschnitt Insight-Übersicht enthält Details dazu, warum der Insight erstellt wurde. Es zeigt den Schweregrad der Erkenntnis sowie eine Beschreibung der Anomalie und einen Zeitrahmen für den Zeitpunkt, zu dem die Anomalie aufgetreten ist. Außerdem wird die Anzahl der betroffenen Services und Anwendungen aufgeführt, die von DevOpsGuru erkannt wurden.

Metriken

Der Abschnitt Metriken enthält Diagramme der Anomalie. Jedes Diagramm zeigt einen Schwellenwert an, der durch das Basisverhalten der Ressource bestimmt wird, sowie Daten der Metrik, die ab dem Zeitpunkt der Anomalie gemeldet wurde.

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. Aktionen, die Sie ergreifen können, werden in der Spalte Empfohlene benutzerdefinierte Änderung angezeigt. Die Gründe für die Empfehlungen sind in der Spalte Warum empfiehlt DevOps Guru dies? dargestellt. Weitere Informationen darüber, wie Sie auf Empfehlungen reagieren können, finden Sie unter the section called “Reagieren auf -Empfehlungen”.

Reagieren auf -Empfehlungen

Empfehlungen sind der wichtigste Teil des Insights. In dieser Phase der Analyse beheben Sie das Leistungsproblem. In der Regel führen Sie die folgenden Schritte aus:

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

   In einigen Fällen kann ein Problem erwartet werden und nicht akzeptabel sein. Wenn Sie beispielsweise eine Testdatenbank einer extremen DB-Last aussetzen, DevOpsmeldetGuru for RDS die Last als Leistungsanomalie. Sie müssen diese Anomalie jedoch nicht beheben, da es sich um ein erwartetes Ergebnis Ihres Tests handelt.

   Wenn Sie feststellen, dass das Problem eine Antwort erfordert, fahren Sie mit dem nächsten Schritt fort.
2. Entscheiden Sie, ob die Empfehlung implementiert werden soll.

   In der Tabelle der Empfehlungen werden in einer Spalte die empfohlenen Aktionen angezeigt. Für reaktive Erkenntnisse ist dies die Spalte Was wir empfehlen auf einer Detailseite für reaktive Anomalien. Für proaktive Einblicke ist dies die Spalte Empfohlene benutzerdefinierte Änderung auf einer Seite mit proaktiven Einblicken.

   DevOpsGuru für RDS bietet eine Liste von Empfehlungen, die mehrere potenzielle problematische Szenarien abdecken. Nachdem Sie diese Liste überprüft haben, bestimmen Sie, welche Empfehlung für Ihre aktuelle Situation relevanter ist, und erwägen Sie, sie anzuwenden. Wenn eine Empfehlung für Ihre Situation funktioniert, fahren Sie mit dem nächsten Schritt fort. Wenn

nicht, überspringen Sie den verbleibenden Schritt und beheben Sie das Problem mit manuellen Techniken.

3. Führen Sie die empfohlenen Aktionen aus.

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

   - Führen Sie eine bestimmte Korrekturmaßnahme durch.

     Beispielsweise DevOpsempfiehltGuru für RDS möglicherweise, die CPU-Kapazität zu aktualisieren, die Einstellungen des Anwendungspools zu optimieren oder das Leistungsschema zu aktivieren.

   - Untersuchen Sie die Ursache des Problems.

     In der Regel DevOpsempfiehltGuru für RDS, dass Sie bestimmte SQL-Anweisungen oder Warteereignisse untersuchen. Eine Empfehlung könnte beispielsweise darin bestehen, das Warteereignis zu untersuchen`io/table/sql/handler`. Suchen Sie das aufgeführte 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 Aktionen aus.

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

Überwachung nicht relationaler Datenbanken mit DevOpsGuru

DevOpsGuru ist in der Lage, Erkenntnisse für Ihre nicht relationalen oder NoSQL-Datenbanken zu generieren, mit denen Sie Ihre Ressourcen gemäß den bewährten Methoden konfigurieren können. DevOpsGuru kann Ihnen beispielsweise helfen, auf dem Laufenden über die Kapazitätsplanung zu bleiben, indem zukünftige Anforderungen auf der Grundlage des vorhandenen Datenverkehrs prognostiziert werden. DevOpsGuru kann feststellen, ob Sie weniger Ressourcen verbrauchen, als Sie konfiguriert haben, und Empfehlungen zur Verbesserung der Anwendungsverfügbarkeit auf der Grundlage Ihrer historischen Nutzung bereitstellen. Dies kann Ihnen helfen, unnötige Kosten zu senken.

Neben der Kapazitätsplanung erkennt DevOpsGuru betriebliche Probleme wie Drosselung, Transaktionskonflikte, Fehler bei bedingten Prüfungen und Bereiche zur Verbesserung der SDK-Parameter und hilft Ihnen bei der Behebung solcher Probleme. Datenbanken sind in der Regel mit mehreren Services und Ressourcen verbunden, und DevOpsGuru kann Ihre Anwendungsstruktur für die Analyse mithilfe von Gruppen korrelieren, die auf Tagging oder AWS CloudFormation Aggregation basieren. Anomalien können mehrere Ressourcen betreffen, die alle von derselben Lösung betroffen sind. DevOpsGuru ist in der Lage, zwischen verschiedenen Ressourcenmetriken, Konfigurationen, Protokollen und Ereignissen zu korrelieren. DevOpsGuru kann beispielsweise Daten aus einer Lambda-Funktion analysieren und verknüpfen, die möglicherweise Daten aus einer Amazon DynamoDB Tabelle liest oder schreibt. Auf diese Weise DevOpsüberwachtGuru mehrere verwandte Ressourcen, um Anomalien zu erkennen und nützliche Einblicke für Ihre Datenbanklösungen zu erhalten.

Überwachen von Datenbankoperationen in Amazon DynamoDB

Die folgende Tabelle zeigt Beispielszenarien und Einblicke, die DevOpsGuru auf überwacht Amazon DynamoDB.

Amazon DynamoDB Anwendungsfall	Beispiele	Metriken
Erkennen Sie, wann ein großer Prozentsatz von AccountProvisioned ReadCapacityUtilization und AccountProvisionedWriteCapacityUtilization verwendet wird, aufgrund einer großen Anzahl von Lese- und Schreiban forderungen.	Amazon DynamoDB -Tabellen nutzungskapazitäten für Lese- oder Schreibanforderungen erreichen Limits auf Tabellene bene.	AccountProvisioned ReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
Erkennen Sie Fehler bei bedingten Prüfungen in Amazon DynamoDB Anforderungen, die durch einen bereitgestellten Bedingungsausdruck verursacht werden, der nicht	Bedingte Prüfungsfehler werden durch fehlerhafte Daten in Ihrer Tabelle, einen strengen Bedingungsausdruck oder Race-Bedingungen verursacht.	ConditionalCheckFailedRequests

Amazon DynamoDB Anwendungsfall	Beispiele	Metriken
mit den in der Datenbank erwarteten Ergebnissen übereinstimmt.		

Überwachen von Datenbankoperationen in Amazon ElastiCache

Die folgende Tabelle zeigt Beispielszenarien und Einblicke, die DevOpsGuru auf überwacht Amazon ElastiCache.

Szenario, das DevOpsGuru identifiziert	CloudWatch Überwachte Metriken
Erkennen Sie, wenn ein - Amazon ElastiCache Cluster aufgrund sich ändernder Anforderungen an Ihre Cluster sein Rechenlimit für Redis oder Memcached erreicht.	CPUUtilization , EngineCPUUtilization , Bereinigungen

Integration mit CodeGuru Profiler

Dieser Abschnitt erhält eine Übersicht über die Integration von Amazon DevOps Guru in Amazon CodeGuru Profiler. Sie können Empfehlungen von CodeGuru Profiler als Erkenntnisse in die DevOps Guru-Konsole.

Amazon DevOps Guru kann in Amazon integriert werden CodeGuru Profiler mit einem EventBridge verwaltete Regel. CodeGuru Profiler sendet Ereignisse an EventBridge. Die verwaltete Regel leitet Ereignisse weiter, die mit dem Standardereignisbus gesendet werden. Jedes eingehende Ereignis von CodeGuru Profiler ist ein proaktiver Anomaliebericht. Weitere Informationen finden Sie unterArbeiten mit EventBridge CodeGuru Profileraus.

DevOps Guru unterstützt eingehende Ereignisse mit EventBridge. Ein Ereignis weist auf eine Änderung in einer Empfehlung hin, die DevOps Guru identifiziert hat. CodeGuru Profiler sendet alle 24 Stunden ein Heartbeat-Event, um die Kontinuität des Ereignisses zu zeigen. Veranstaltungen tragen CodeGuru -Profiler-Empfehlungsinformationen sowie Metadaten für Ihre Datenverarbeitungsressourcen. Informationen über einen Ereignislebenszyklus finden Sie unterAmazon EventBridge Eventsaus.

Wenn Sie DevOps Guru einrichten, erstellt DevOps Guru das EventBridge Verwaltete Regel in Ihrem Konto, die Ereignisse von einem anderen Dienst leitet. Diese Regel leitet an DevOps Guru. Benachrichtigungen werden gesendet, wenn ein eingehendes Ereignis vorliegt.

Ein Ereignisbus empfängt Ereignisse von einer Quelle wie DevOps Guru und leitet sie an Regeln, die mit diesem Eventbus verknüpft sind. Weitere Informationen zu Eventbussen finden Sie unterEreignisbusseaus.

Weitere Informationen zu einigen Parametern finden Sie unterAmazon EventBridge EventBridge-Ereignisseaus.

Empfangen CodeGuru Profiler-Einblicke in DevOps Guru müssen Sie über Folgendes verfügen.

- CodeGuru Profiler muss aktiviert sein. Weitere Informationen zur Aktivierung CodeGuru Profiler, sieheEinrichten von CodeGuru Profileraus.
- DevOps Guru muss aktiviert sein. Informationen zum Aktivieren von DevOps Guru finden Sie unterAktivieren Sie DevOps Guruaus.
- Die gleichen Ressourcen müssen in derselben Region in beiden CodeGuru Profiler und DevOps Guru.

Definieren von Anwendungen mitAWSRessourcen

Amazon DevOpsGuru gruppiert die Ressourcen, die sich innerhalb der Abdeckungsgrenze befinden, die angibt, welche Ressourcen für betriebliche Erkenntnisse analysiert werden. Die Ressourcen sind nach Ressourcen gruppiert inAWS CloudFormationStacks oder nach Ressourcen mit Tags. Sie wählen die Stacks oder Tags beim Einrichten aus DevOpsGuru. Sie können die Stacks oder Tags auch später aktualisieren. Wir empfehlen Ihnen, Ihre Ressourcengruppen als Anwendungen zu betrachten. Sie verfügen beispielsweise möglicherweise über alle Ressourcen, die Sie für eine Überwachungsanwendung verwenden, in einem Stack. Oder Sie fügen dasselbe Tag zu allen Ressourcen hinzu, die Sie in einer Datenbankanwendung verwenden. Die Grenze, die definiert, welche RessourcenDevOpsGuru analysiert. Alle Ressourcen in der Sammlung befinden sich innerhalb dieser Grenze. Alle Ressourcen in Ihrem Konto, die sich nicht in Ihrer Ressourcensammlung befinden, befinden sich außerhalb der Grenze und werden nicht analysiert. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unterAmazon DevOpsGuru Pricing.

Sie können Ihre Abdeckungsgrenze, die die Ressourcen in Ihren Anwendungen enthält, auf drei Arten definieren.

- Angabe, dass alle unterstützt werdenAWSRessourcen in IhremAWSKonto und Region. Dadurch werden Ihr Konto und Ihre Region zu Ihrer Ressourcengrenze. Mit dieser Option DevOpsGuru analysiert alle unterstützten Ressourcen in Ihrem Konto und Ihrer Region. Alle Ressourcen, die sich in einem Stack befinden, werden in einer Anwendung gruppiert. Alle Ressourcen, die sich nicht in einem Stack befinden, werden in einer eigenen Anwendung gruppiert.
- Verwenden vonAWS CloudFormationStacks, um die Ressourcen in Ihren Anwendungen zu spezifizieren. Ein Stack enthält Ressourcen, die mitAWS CloudFormation. In DevOpsGuru, du wählst Stapel in deinem Konto. Die Ressourcen, die Sie in jedem Stack auswählen, werden in einer Anwendung gruppiert. Alle Ressourcen in den Stacks werden analysiert von DevOpsGuru für Einblicke.
- Verwenden vonAWSTags, um die Ressourcen in Ihren Anwendungen anzugeben. Importieren in &S3;AWSTag enthält eineSchlüsselund einWert. In DevOpsGuru, wähle ein TagSchlüsselund wählen Sie optional eine oder mehrere ausWertedie damit gepaart sindSchlüssel. Sie können dasWerteum Ihre Ressourcen in Anwendungen zu gruppieren.

Weitere Informationen finden Sie unter Aktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru.

Themen

Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOpsGuru-Anwendungen

Sie können Tags verwenden, um die AWS Ressourcen zu identifizieren, die Amazon DevOpsGuru analysiert, und um anzugeben, welche Ressourcen für die Überwachung mit dem ausgewählten Tag-Schlüssel und den ausgewählten Tag-Werten gruppiert sind. Sie können diese Konfigurationen bearbeiten, wenn Sie DevOpsGuru einrichten oder auf der Seite Analysierte Ressourcen die Option Analysierte Ressourcen bearbeiten auswählen. Nachdem Sie Tags ausgewählt haben, wählen Sie einen bestimmten Tag-Schlüssel aus, der mit „devops-guru-“ beginnt. Um alle Ressourcen im Konto zu analysieren und Tag-Werte zum Gruppieren der Ressourcen zu verwenden, wählen Sie Alle Kontoressourcen aus. Um Tag-Werte zur Angabe der Ressourcen zu verwenden, die DevOpsGuru analysieren soll, wählen Sie Bestimmte Tag-Werte auswählen aus.

> **Note**
>
> Wenn Alle Kontoressourcen ausgewählt sind 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 Ihre Anwendungen zu gruppieren. Sie können beispielsweise Ihre Ressourcen mit dem Schlüssel markieren `devops-guru-applications`und dann diesen Schlüssel mit einem anderen Wert für jede Ihrer Anwendungen verwenden. Sie können die Tag-Schlüssel-Wert-Paare `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 Tags zu Ihren Ressourcen hinzu, indem Sie den AWS Service 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 für Ressourcen filtern, die sie generiert haben. Weitere Informationen zum Filtern Ihrer Erkenntnisse mithilfe eines Tags finden Sie unter AnsehenDevOpsEinblicke in Guru.

Weitere Informationen zu den unterstützten Services und Ressourcen finden Sie unter Amazon DevOpsGuru – Preise.

Themen

Was ist ein -AWSTag?

Tags helfen Ihnen, Ihre AWS-Ressourcen zu identifizieren und zu organisieren. Viele AWS-Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services dasselbe Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Sie können beispielsweise das gleiche Tag einer Amazon-DynamoDB-Tabellenressource 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.

Definieren einer DevOpsGuru-Anwendung mithilfe eines Tags

Um Ihre Amazon- DevOpsGuru-Anwendung mithilfe eines Tags zu definieren, fügen Sie dieses Tag den AWS Ressourcen in Ihrem Konto hinzu, aus denen Ihre Anwendung besteht. Ihr Tag enthält einen Schlüssel und einen Wert . Wir empfehlen, dass Sie jeder Ihrer von DevOpsGuru

analysierten AWS Ressourcen ein Tag hinzufügen, das denselben Schlüssel hat. Verwenden Sie einen anderen Wert im Tag, um Ressourcen in Ihren Anwendungen zu gruppieren. Sie können beispielsweise Tags mit dem Schlüssel `devops-guru-analysis-boundary` allen AWS Ressourcen in Ihrer Abdeckungsgrenze zuweisen. Verwenden Sie unterschiedliche Werte mit diesem Schlüssel, um Anwendungen in Ihrem Konto zu identifizieren. Sie können die Werte `containers`, `databaseund` `monitoring` für drei Anwendungen verwenden. Weitere Informationen finden Sie unter Aktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru.

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 verbinden. Verwenden Sie den Wert , um die Ressourcen, die Ihren Schlüssel enthalten, in Ihre Betriebsanwendungen zu gruppieren.

> **Important**
>
> Die Zeichenfolge für einen Schlüssel in einem Tag, das Sie zur Definition Ihrer Ressourcen-Abdeckung verwenden, muss mit dem Präfix `Devops-guru-` beginnen. Der Tag-Schlüssel könnte `DevOps-Guru-deployment-application` oder `devops-guru-rds-application` sein. 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 namens `devops-guru-rds` und einem Schlüssel namens `DevOps-Guru-RDS`, und diese fungieren als zwei verschiedene Schlüssel . Mögliche Schlüssel/Wert-Paare in Ihrer Anwendung könnten `Devops-Guru-production-application/RDS` oder `Devops-Guru-production-application/containers` sein.

Verwenden von Tags mit DevOpsGuru

Geben Sie die AWS Tags an, die die AWS Ressourcen identifizieren, die Amazon DevOpsGuru analysieren soll, oder geben Sie Tag-Werte an, die identifizieren, welche Ressourcen gruppiert werden sollen. Diese Ressourcen sind Ihre Ressourcenabdeckungsgrenze. Sie können einen Schlüssel und null oder mehrere Werte auswählen.

So wählen Sie Ihre Tags aus

1. Öffnen Sie die Amazon- DevOpsGuru-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 aus, wenn DevOpsGuru alle Ressourcen analysieren soll, die die von Ihnen ausgewählten Tags enthalten. Wählen Sie einen Schlüssel und dann eine der folgenden Optionen aus.

   - Alle Kontoressourcen – Analysieren Sie alle AWS Ressourcen in der aktuellen Region und dem aktuellen Konto. Ressourcen mit dem ausgewählten Tag-Schlüssel werden nach Tag-Wert gruppiert, sofern vorhanden. Ressourcen ohne diesen Tag-Schlüssel werden separat gruppiert und analysiert.
   - Bestimmte Tag-Werte auswählen – 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.

   Der Schlüssel des Tags muss mit dem Präfix beginnen`devops-guru-`. Bei diesem Präfix wird nicht zwischen Groß- und Kleinschreibung unterschieden. Ein gültiger Schlüssel ist beispielsweise `DevOps-Guru-Production-Applications`.
5. Wählen Sie Speichern.

Hinzufügen von AWS Tags zu AWS Ressourcen

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

- Um Tags mit dem Service Ihrer Ressourcen zu verwalten, verwenden Sie die KonsoleAWS Command Line Interface, oder das SDK des Services, zu dem eine Ressource gehört. Sie können beispielsweise eine Amazon Kinesis-Stream-Ressource oder eine Amazon- CloudFront Verteilungsressource markieren. Dies sind zwei Beispiele für Services mit Ressourcen, die markiert werden können. Die meisten Ressourcen, die DevOpsGuru analysieren kann, unterstützen Tags. Weitere Informationen finden Sie unter Markieren Ihrer Streams im Amazon Kinesis-Entwicklerhandbuch und Markieren einer Verteilung im Amazon- CloudFront Entwicklerhandbuch. Informationen zum Hinzufügen von Tags zu anderen Ressourcentypen finden Sie im Benutzerhandbuch oder Entwicklerhandbuch für den AWS Service, zu dem sie gehören.

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

- Sie können den AWS Tag-Editor verwenden, um Tags nach Ressourcen in Ihrer Region und nach Ressourcen in bestimmten AWS Services zu verwalten. Weitere Informationen finden Sie unter Tag-Editor im AWSBenutzerhandbuch für 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 hinzufügen `RDS`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 von den Amazon-RDS-Ressourcen in Ihrer Anwendung generiert werden.

benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-Anwendungen

Sie können Folgendes verwendenAWS CloudFormationStacks, um anzugeben welcheAWSRessourcen, die du willst DevOpsGuru zum Analysieren. Ein Stack ist eine Sammlung vonAWSRessourcen, die als eine Einheit verwaltet werden. Die Ressourcen in den Stacks, die du auswählst, bilden deine DevOpsGuru-Abdeckung. Für jeden Stack, den Sie auswählen, werden die Betriebsdaten in den unterstützten Ressourcen auf anomales Verhalten analysiert. Diese Probleme werden dann in verwandte Anomalien gruppiert, um Erkenntnisse zu gewinnen. Jede Erkenntnis enthält eine oder mehrere Empfehlungen, die Ihnen helfen, diese zu berücksichtigen. Die maximale Anzahl der Stapel, die Sie angeben können, ist 1000. Weitere Informationen finden Sie unterArbeiten mit Stacksin derAWS CloudFormationBenutzerhandbuchundAktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru.

Nachdem Sie einen Stack ausgewählt haben, DevOpsGuru beginnt sofort, alle Ressourcen zu analysieren, die Sie ihm hinzufügen. Wenn Sie eine Ressource aus einem Stack entfernen, wird sie nicht mehr analysiert.

Wenn du dich dafür entscheidest DevOpsGuru analysiere alle unterstützten Ressourcen in deinem Konto (das bedeutet deinAWSKonto und Region ist Ihr DevOpsGuru-Abdeckung (Grenze), dann DevOpsGuru analysiert und erstellt Erkenntnisse für jede unterstützte Ressource in Ihrem Konto, einschließlich der Ressourcen in Stapeln. Ein Einblick, der aus Anomalien in einer Ressource erstellt wurde, die sich nicht in einem Stapel befindet, wird imKonto-Ebene. Wenn eine Einsicht aus Anomalien in einer Ressource erstellt wird, die sich in einem Stack befindet, wird sie imStack-Ebene. Weitere Informationen finden Sie unter Verstehen, wie anomale Verhaltensweisen zu Erkenntnissen zusammengefasst werden.

Stapel auswählen für DevOpsGuru zum Analysieren

Geben Sie die Ressourcen an, die Amazon verwenden möchten DevOpsGuru zum Analysieren, indem erAWS CloudFormationStapel, die sie erstellen. Hierfür können Sie dasAWS Management Consoleoder das SDK.

Themen

- Stapel auswählen für DevOpsGuru zum Analysieren (Konsole)
- Stapel auswählen für DevOpsGuru zum Analysieren (DevOpsGuru (SDK)

Stapel auswählen für DevOpsGuru zum Analysieren (Konsole)

Sie können hinzufügenAWS CloudFormationStacks mithilfe der -Konsole.

So wählen Sie die Stapel aus, die die zu analysierenden Ressourcen enthalten

1. Öffnen Sie Amazon DevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Öffnen Sie den Navigationsbereich und wählen Sie dannEinstellungen.
3. InDevOpsGuru-Analyse, wählenVerwalten.
4. WählenCloudFormation Stapelwenn du willst DevOpsGuru analysiert die Ressourcen in Stacks befinden, die sich in Stacks befinden, die sich in Stacks befinden, die sich in Stacks befinden

   - Alle Ressourcen— Alle Ressourcen, die sich in Stacks in Ihrem Konto befinden, werden analysiert. Die Ressourcen in jedem Stack werden in einer eigenen Anwendung gruppiert. Alle Ressourcen in Ihrem Konto, die sich nicht in einem Stack befinden, werden nicht analysiert.
   - Stapel auswählen— Wählen Sie die gewünschten Stacks DevOpsGuru zum Analysieren. Die Ressourcen in jedem Stapel, den Sie auswählen, werden in einer eigenen Anwendung

gruppiert. Sie können den Namen eines Stacks inSuchen Sie nach Stacksum schnell einen bestimmten Stack zu finden. Sie können bis zu 1.000 Stacks auswählen.

5. Wählen Sie Save (Speichern) aus.

Stapel auswählen für DevOpsGuru zum Analysieren (DevOpsGuru (SDK)

Zur AngabeAWS CloudFormationStacks unter Verwendung von Amazon DevOpsGuru SDK, benutze das`UpdateResourceCollection`-Methode. Weitere Informationen finden Sie unterUpdateResourceCollectionin derAmazon DevOpsGuru-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 DevOpsGuru-Einstellungen

Sie können das folgende Amazon aktualisieren DevOpsGuru-Einstellungen:

- Dein DevOpsGuru-Berichterstattung. Dies bestimmt, welche Ressourcen in Ihrem Konto analysiert werden.
- Ihre Benachrichtigungen. Dies bestimmt, welche Themen von Amazon Simple Notification Service verwendet werden, um Sie über wichtige Informationen zu informieren DevOpsGuru-Ereignisse.
- Funktionen für erweiterte Einblicke. Dazu gehören die Erkennung von Protokollanomalien, Verschlüsselung und IhreAWS Systems ManagerIntegrationseinstellungen. Dies bestimmt, ob DevOpsGuru zeigt Protokolldaten an, ob Sie zusätzliche Sicherheitsschlüssel verwenden und ob OpsItem wird im Systems Manager erstellt OpsCenter für jeden neuen Einblick.

Themen

Aktualisierung der Einstellungen Ihres Verwaltungskontos

Sie können konfigurieren DevOpsGuru für Konten in Ihrer Organisation. Wenn Sie noch keinen delegierten Administrator registriert haben, können Sie dies tun, indem SieRegistrieren Sie den delegierten Administrator. Weitere Informationen zur Registrierung eines delegierten Administrators finden Sie unterAktivierenDevOpsGuru.

Aktualisierung deinerAWSBerichterstattung über Analysen in DevOpsGuru

Sie können welche aktualisierenAWSRessourcen in Ihrem Konto DevOpsGuru analysiert. Navigieren Sie dazu zumAnalysierte RessourcenSeite in der Konsole und wählen Sie dannBearbeiten. Weitere Informationen finden Sie unter Analysierte Ressourcen anzeigen.

Aktualisierung Ihrer Benachrichtigungen in DevOpsGuru

Richten Sie Amazon Simple Notification Service-Themen ein, mit denen Sie über wichtige Amazon-Nachrichten informiert werden DevOpsGuru-Ereignisse. Sie können aus einer Liste von Themennamen wählen, die bereits in IhremAWSKonto, gib den Namen für ein neues Thema ein DevOpsGuru erstellt in Ihrem Konto oder geben Sie den Amazon-Ressourcennamen (ARN) eines vorhandenen Themas in ein beliebigesAWSKonto in Ihrer Region. Wenn Sie den ARN eines Themas angeben, das nicht in Ihrem Konto enthalten ist, müssen Sie die Erlaubnis erteilenDevOpsGuru, um auf dieses Thema zuzugreifen, indem Sie ihm 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 auf folgende Werte heraufgestuft`Low`oder`Medium`zu`High`.
- Der Status einer Erkenntnis ändert sich von „Aktuell“ zu „Gelöst“.
- Es wird eine Empfehlung für einen Einblick identifiziert.

DevOpsGuru sendet auch Benachrichtigungen, wenn ein ausgewählterAWS CloudFormationDer Stack- oder Tag-Schlüssel ist ungültig, wenn Sie versuchen, Ressourcen zu Ihrem hinzuzufügen DevOpsGuru-Konto.

Sie können wählen, ob Sie Amazon SNS-Benachrichtigungen für alle Arten von Updates zu einem Problem erhalten möchten oder ob Sie Amazon 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-Benachrichtigungsthemen hinzufügen, entfernen oder aktualisieren möchten.

Themen

Navigieren Sie zu den Benachrichtigungseinstellungen im DevOpsGuru-Konsole

Um Benachrichtigungen zu aktualisieren, müssen Sie zunächst zum Abschnitt mit den Benachrichtigungseinstellungen navigieren.

Um zum Abschnitt mit den Benachrichtigungseinstellungen zu navigieren

1. Öffne den Amazon DevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.

   Die Seite mit den Einstellungen enthältBenachrichtigungenAbschnitt mit Informationen zu konfigurierten Amazon SNS-Themen.

Hinzufügen von Amazon SNS-Benachrichtigungsthemen im DevOpsGuru-Konsole

Um ein Amazon SNS-Benachrichtigungsthema hinzuzufügen DevOpsGuru-Konsole

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

- Wählen SieGenerieren Sie ein neues SNS-Thema per E-Mail. Dann, vonGeben Sie die E-Mail-Adresse an, geben Sie die E-Mail-Adresse ein, an die Sie Benachrichtigungen erhalten möchten. Um weitere E-Mail-Adressen einzugeben, wählen SieNeue E-Mail hinzufügen.
- WähleVerwenden Sie ein vorhandenes SNS-Thema. Dann, vonWählen Sie ein Thema in IhremAWSKonto, wählen Sie das Thema, das Sie verwenden möchten.
- WähleVerwenden Sie den ARN eines vorhandenen SNS-Themas, um ein vorhandenes Thema aus einem anderen Konto anzugeben. Dann, inGeben Sie einen ARN für ein Thema ein, geben Sie das Thema 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.

Entfernen von Amazon SNS-Benachrichtigungsthemen in der DevOpsGuru-Konsole

Um Amazon SNS-Themen zu entfernen DevOpsGuru-Konsole

1. the section called “Navigieren Sie zu den Benachrichtigungseinstellungen im DevOpsGuru-Konsole”.
2. WähleWählen Sie ein vorhandenes Thema.
3. Wählen Sie im Drop-down-Menü das Thema aus, das Sie entfernen möchten.
4. Wählen Sie Remove (Entfernen) aus.
5. Wählen Sie Speichern aus.

Aktualisierung der Amazon SNS-Benachrichtigungskonfigurationen

Es gibt zwei Arten von Benachrichtigungskonfigurationen für Amazon SNS-Benachrichtigungsthemen in DevOpsGuru. Sie können wählen, ob Sie Benachrichtigungen aller Schweregrade oder nur Benachrichtigungen mit erhalten möchtenHochundMittelSchweregrade. Sie können auch wählen, ob Sie Benachrichtigungen für alle Arten von Updates oder nur für einige Arten von Updates erhalten möchten.

Wenn Sie sich dafür entscheiden, Amazon SNS-Benachrichtigungen für alle Arten von Updates zu diesem Problem zu erhalten, 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 auf folgende Werte heraufgestuftLowoderMediumzuHigh.
- Der Status einer Erkenntnis ändert sich von „Aktuell“ zu „Gelöst“.
- Es wurde eine Empfehlung für einen Einblick identifiziert.

Standardmäßig erhalten Sie nurHochundMittelBenachrichtigungen zum Schweregrad, und Sie erhalten Benachrichtigungen für alle Arten von Updates.

Um die Benachrichtigungskonfigurationen für Amazon SNS-Benachrichtigungsthemen zu aktualisieren

1. the section called “Navigieren Sie zu den Benachrichtigungseinstellungen im DevOpsGuru-Konsole”.
2. WählenWählen Sie ein vorhandenes Thema.
3. Wählen Sie im Dropdownmenü das Thema aus, für das Sie Aktualisierungen vornehmen möchten.
4. Wählen SieAlle Schweregradeum Benachrichtigungen mit den Schweregraden Hoch, Mittel und Niedrig zu erhalten, oder wählen SieNur Hoch und Mittelum Benachrichtigungen mit den Schweregraden „Hoch“ und „Mittel“ zu erhalten.
5. WählenBenachrichtige mich über alle Updates zu The Insight, oder wähleBenachrichtige mich, wenn ein Insight geöffnet oder geschlossen wird oder wenn sich der Schweregrad von Niedrig oder Mittel auf Hoch ändert.
6. Wählen Sie Speichern aus.

Ihrem Amazon SNS-Thema wurden Berechtigungen hinzugefügt

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

```
{
```

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

Diese Berechtigungen sind erforderlich für DevOpsGuru, um Benachrichtigungen zu einem Thema zu veröffentlichen. Wenn du es vorziehst, diese Berechtigungen für das Thema nicht zu haben, kannst du sie getrost entfernen und das Thema funktioniert weiterhin so, wie es vor deiner Auswahl der Fall war. Wenn diese angehängten Berechtigungen jedoch entfernt werden, DevOpsGuru kann das Thema nicht verwenden, um Benachrichtigungen zu generieren.

Filtere deine DevOpsGuru-Benachrichtigungen

Sie können Ihre filtern DevOpsGuru-Benachrichtigungen vonthe section called “Aktualisierung der Amazon SNS-Benachrichtigungskonfigurationen”oder mithilfe einer Amazon SNS-Abonnementfilterrichtlinie.

Themen

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

Filtern von Benachrichtigungen mit einer Amazon 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 erhalten DevOpsGuru.

Verwenden Sie eine Filterrichtlinie, um die Arten von Benachrichtigungen anzugeben, die Sie erhalten. Sie können Ihre Amazon 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 zur Erstellung einer Amazon SNS-Abonnementfilterrichtlinie finden Sie unterRichtlinien für Amazon SNS-Abonnementfilterin derAmazon Simple Notification Service Entwicklerhandbuch. In Ihrer Filterrichtlinie geben Sie eines der Schlüsselwörter mit den Werten der Richtlinie an`MessageType`. Folgendes würde beispielsweise in einem Filter erscheinen, der angibt, dass das Amazon SNS-Thema nur dann Benachrichtigungen zustellt, wenn anhand eines Insights eine neue Anomalie erkannt wird.

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

Beispiel für eine gefilterte Amazon SNS-Benachrichtigung für Amazon DevOpsGuru

Im Folgenden finden Sie ein Beispiel für eine Amazon Simple Notification Service (Amazon SNS) -Benachrichtigung zu einem Amazon SNS-Thema mit einer Filterrichtlinie. Es ist`MessageType`eist eingestellt auf`NEW_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"
          ]
```

```
        }
      }
}
```

AktualisierungAWS Systems ManagerIntegration inDevOpsGuru

Sie können die Erstellung eines aktivieren OpsItem für jeden neuen Einblick inAWS Systems Manager OpsCenter. OpsCenter ist ein zentralisiertes System, in dem Sie betriebliche Arbeitsaufgaben einsehen, untersuchen und überprüfen können (OpsItems). Die OpsItems for your insights kann Ihnen bei der Verwaltung von Aufgaben helfen, die sich mit dem anomalen Verhalten befassen, das zur Erstellung der einzelnen Erkenntnisse geführt hat. Weitere Informationen finden Sie unterAWS Systems Manager OpsCenterundArbeitet mit OpsItemin derAWS Systems ManagerBenutzerleitfaden.

> **Note**
>
> Wenn Sie den Schlüssel oder Wert des Tag-Felds eines ändern OpsItem, dann DevOpsGuru ist nicht in der Lage, das zu aktualisieren OpsItem. Zum Beispiel, wenn Sie das Tag eines ändern OpsItem von`"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`dann zu etwas anderem DevOpsGuru kann das nicht aktualisieren OpsItem.

Um Ihre Systems Manager-Integration zu verwalten

1. Öffnen Sie Amazon DevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. InAWS Systems ManagerIntegration, wählenAktivieren DevOpsGuru, um eine zu erstellenAWS OpstItem in OpsCenter für jeden Einblickum eine zu haben OpsItem erstellt für jede neue Erkenntnis. Wählen Sie es ab, um keine mehr zu haben OpsItemwird für jede neue Erkenntnis erstellt.

Ihnen wird Folgendes in Rechnung gestellt OpsItems in Ihrem Konto erstellt. Weitere Informationen finden Sie unter AWS Systems Manager Preise.

Aktualisierung protokolliert die Erkennung von Anomalien inDevOpsGuru

Um Ihre Einstellungen für die Erkennung von Protokollanomalien zu verwalten

1. Öffnen Sie den Amazon DevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. InErkennung von Anomalien protokollieren, wählenAktivieren Sie die Erkennung von Protokollanomalien durch Erteilung DevOpsGuru berechtigt, Protokolldaten anzuzeigen, die mit einem Einblick verknüpft sind.zu habenDevOpsGuru zeigt Protokolldaten zu Erkenntnissen an.

Aktualisierung der Verschlüsselungseinstellungen inDevOpsGuru

Sie können die zu verwendenden Verschlüsselungseinstellungen aktualisierenAWSeigene Schlüssel oderAWS KMSvom Kunden verwaltete Schlüssel. Beim Wechsel zu einem neuen Kunden verwaltetAWS KMSSchlüssel von einem Bestandskunden verwaltetAWS KMSSchlüssel, DevOpsGuru beginnt automatisch, neu aufgenommene Metadaten mit dem neuen Schlüssel zu verschlüsseln. Die historischen Daten bleiben verschlüsselt, wobei der zuvor konfigurierte Kunde verwaltet wirdAWS KMSSchlüssel.

> **Note**
>
> Wenn Sie den Zuschuss widerrufen oder den vorherigen deaktivieren oder löschenAWS KMSSchlüssel, DevOpsGuru wird auf keine der mit diesem Schlüssel verschlüsselten Daten zugreifen können und du siehst möglicherweise`AccessDeniedException`wenn ein Lesevorgang ausgeführt wird.

Um Ihre Verschlüsselungseinstellungen zu verwalten

1. Öffne den Amazon DevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. In derVerschlüsselungAbschnitt, wählenVerschlüsselung bearbeiten.
4. Wählen Sie den Verschlüsselungstyp aus, den Sie zum Schutz Ihrer Daten verwenden möchten. Sie können eine Standardeinstellung verwendenAWSEigener Schlüssel, wählen Sie einen vorhandenen, vom Kunden verwalteten Schlüssel oder erstellen Sie einen neuen, vom Kunden verwalteten SchlüsselAWS KMSSchlüssel.
5. Wählen Sie Speichern aus.

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

Benachrichtigungen anzeigen

In DevOpsGuru gibt es verschiedene Arten von Benachrichtigungen.

Themen

Die Abschnitte auf dieser Seite zeigen Beispiele für jeden Benachrichtigungstyp.

Neuer Einblick

Benachrichtigungen für 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"
            ]
        },
   }
}
```

Geschlossene Einblicke

Benachrichtigungen für geschlossene Erkenntnisse 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"
            ]
        }
    }
}
```

Neue Zuordnung

Benachrichtigungen für neue Zuordnungen 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 für 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 aktualisiert

Benachrichtigungen für Schweregrad-Upgrades 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

Sie können AWS AWS CloudFormationStacks und Tags verwenden, um die AWS Ressourcen zu filtern und zu identifizieren, die DevOpsGuru analysieren soll. Wenn Sie einen ungültigen Stack oder Tag auswählen, mit dem DevOpsGuru Ressourcen identifizieren kann, erstellt DevOpsGuru eine `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE`Benachrichtigung. Dies kann passieren, wenn dem von Ihnen angegebenen Tag oder Stack-Namen keine Ressourcen zugeordnet sind. Um die DevOpsGuru-Filtermethoden optimal zu nutzen, 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"
}
```

Ressourcen anzeigen, die analysiert wurden vonDevOpsGuru

DevOpsGuru bietet eine Liste der Ressourcennamen und ihrer Anwendungsgrenzen, die analysiert werden, mithilfe des`ListMonitoredResources`Aktion. Diese Informationen werden von Amazon gesammeltCloudWatch,AWS CloudTrail, und andereAWSDienste, die denDevOpsRolle, die mit dem Guru-Service verknüpft ist.

Beachten Sie, dass selbst wenn ein Benutzer keine ausdrückliche Berechtigung hat, auf die APIs für einen anderen Dienst zuzugreifen, wieAWS Lambdaoder Amazon RDS,DevOpsGuru bietet immer noch eine Liste von Ressourcen aus diesem Dienst, solange der`ListMonitoredResources`Aktion ist erlaubt.

Themen

- Aktualisierung IhresAWSAnalyseabdeckung inDevOpsGuru
- Die analysierte Ressourcenansicht für Benutzer wird entfernt

Aktualisierung IhresAWSAnalyseabdeckung inDevOpsGuru

Sie können aktualisieren, welcheAWSRessourcen in Ihrem KontoDevOpsGuru analysiert. Die analysierten Ressourcen bilden IhreDevOpsGuru-Deckungsgrenze. Wenn Sie Ihre Grenze angeben, werden Ihre Ressourcen in Anwendungen gruppiert. Sie haben vier Optionen für die Grenzabdeckung.

- Entscheide dich fürDevOpsGuru analysiert alle unterstützten Ressourcen in deinem Konto. Alle Ressourcen in Ihrem Konto, die sich in einem Stapel befinden, werden in einer Anwendung zusammengefasst. Wenn Sie mehrere Stacks 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 zusammengefasst.
- Geben Sie Ressourcen an, indem SieAWS CloudFormationStapel, die diese Ressourcen definieren. Wenn du das tust,DevOpsGuru analysiert 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 unterMit Stacks arbeitenin derAWS CloudFormationBenutzerleitfadenundErmitteln Sie den Versicherungsschutz für DevOps Guru.

- Geben Sie Ressourcen an, indem SieAWSSchlagworte. DevOpsGuru analysiert entweder alle Ressourcen in deinem Konto und deiner Region oder alle Ressourcen, die den von dir ausgewählten Tag-Schlüssel enthalten. Ressourcen werden basierend auf ausgewählten Tag-Werten gruppiert. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOpsGuru-Anwendungen.
- Geben Sie an, dass keine Ressourcen analysiert werden sollen, damit Ihnen keine Kosten aus der Ressourcenanalyse entstehen.

> **Note**
>
> Wenn Sie Ihre Berichterstattung so aktualisieren, dass keine Ressourcen mehr analysiert werden, fallen möglicherweise weiterhin geringfügige Kosten an, wenn Sie vorhandene Erkenntnisse überprüfen, die vonDevOpsGuru in der Vergangenheit. Diese Gebühren stehen im Zusammenhang mit API-Aufrufen, die zum Abrufen und Anzeigen von Insight-Informationen verwendet werden. Weitere Informationen finden Sie unterAmazonasDevOpsGuru-Preise.

DevOpsGuru unterstützt alle Ressourcen, die mit unterstützten Diensten verbunden sind. Weitere Informationen zu den unterstützten Diensten und Ressourcen finden Sie unterAmazonasDevOpsGuru-Preise.

Um Ihre zu verwaltenDevOpsBerichterstattung über Guru-Analysen

1. Öffne den AmazonasDevOpsGuru-Konsole beihttps://console.aws.amazon.com/devops-guru/.
2. ErweiternAnalysierte Ressourcenim Navigationsbereich.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Wählen Sie eine der folgenden Deckungsoptionen.
   - Wählen SieAlle Kontoressourcenwenn du willstDevOpsGuru zur Analyse aller unterstützten Ressourcen in IhremAWSKonto und Region. Wenn Sie diese Option wählen, wird IhrAWSKonto ist Ihre Deckungsgrenze für die Ressourcenanalyse. Alle Ressourcen in jedem Stapel in Ihrem Konto sind in einer eigenen Anwendung zusammengefasst. Alle verbleibenden Ressourcen, die sich nicht in einem Stapel befinden, werden in einer eigenen Anwendung zusammengefasst.

- Wählen SieCloudFormationStapelwenn du willstDevOpsGuru, um die Ressourcen zu analysieren, die sich in von Ihnen ausgewählten Stapel befinden, und wählen Sie dann eine der folgenden Optionen.
  - Alle Ressourcen— Alle Ressourcen, die sich stapelweise in Ihrem Konto befinden, werden analysiert. Die Ressourcen in jedem Stapel sind in einer eigenen Anwendung zusammengefasst. Alle Ressourcen in Ihrem Konto, die sich nicht in einem Stapel befinden, werden nicht analysiert.
  - Stapel auswählen— Wählen Sie die gewünschten Stapel ausDevOpsGuru zum Analysieren. Die Ressourcen in jedem Stapel, den Sie auswählen, werden in einer eigenen Anwendung zusammengefasst. Sie können den Namen eines Stacks eingeben inFinde Stapelum schnell einen bestimmten Stapel zu finden. Sie können bis zu 1.000 Stapel auswählen.

  Weitere Informationen finden Sie unter benutzenAWS CloudFormationStacks zur Identifizierung von Ressourcen in Ihrem DevOpsGuru-Anwendungen.
- Wählen SieSchlagwortewenn du willstDevOpsGuru, um alle Ressourcen zu analysieren, die die von Ihnen ausgewählten Tags enthalten. Wähle einSchlüsselund wählen Sie dann eine der folgenden Optionen.
  - Alle Kontoressourcen— Analysieren Sie alle AWS-Ressourcen in der aktuellen Region und im aktuellen Konto. Ressourcen mit dem ausgewählten Tag-Schlüssel werden nach Tag-Werten gruppiert, falls vorhanden. Ressourcen ohne diesen Tag-Schlüssel werden gruppiert und separat analysiert.
  - Wählen Sie bestimmte Tag-Werte— Alle Ressourcen, die ein Tag mit dem enthaltenSchlüsseldie Sie ausgewählt haben, werden analysiert. DevOpsGuru gruppiert deine Ressourcen nach deinen Tags in AnwendungenWerte.

  Das Etikett istSchlüsselmuss mit dem Präfix beginnen`devops-guru-`. Bei diesem Präfix wird nicht zwischen Groß- und Kleinschreibung unterschieden. Zum Beispiel ein gültigesSchlüsselist`DevOps-Guru-Production-Applications`. Weitere Informationen finden Sie unter Verwenden von Tags zur Identifizierung von Ressourcen in Ihren DevOpsGuru-Anwendungen.
- Wählen SieKeinewenn du nicht willstDevOpsGuru, um alle Ressourcen zu analysieren. Diese Option deaktiviertDevOpsGuru, damit dir keine Kosten für die Ressourcenanalyse entstehen.

5. Wählen Sie Speichern aus.

Die analysierte Ressourcenansicht für Benutzer wird entfernt

Auch wenn ein Benutzer keine ausdrückliche Erlaubnis hat, auf die APIs für einen anderen Dienst wie Lambda oder Amazon RDS zuzugreifen,DevOpsGuru bietet immer noch eine Liste von Ressourcen aus diesem Dienst, solange der`ListMonitoredResources`Aktion ist erlaubt. Um dieses Verhalten zu ändern, können Sie IhrAWSIAM-Richtlinie, um diese Aktion abzulehnen.

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

Best Practices in DevOps Guru

Die folgenden Best Practices können Ihnen helfen, anomales Verhalten zu verstehen, zu diagnostizieren und zu beheben, das von Amazon DevOps Guru erkannt wurde. Verwenden Sie Bewährte Methoden mitErkenntnisse verstehen in derDevOpsGuru-Konsoleum betriebliche Probleme zu beheben, die von DevOps Guru erkannt wurden.

- Sehen Sie sich in der Timeline-Ansicht einer Insight zuerst die hervorgehobenen Metriken an. Sie sind oft Schlüsselindikatoren für das Problem.
- Verwenden Sie Amazon CloudWatch, um Metriken anzuzeigen, die unmittelbar vor der ersten hervorgehobenen Metrik aufgetreten sind, in einer Erkenntnis, um festzustellen, 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 in den Metriken von Performance Insights. Indem Sie Gegenmetriken mit der Datenbanklast korrelieren, erhalten Sie detaillierte Informationen zu Leistungsproblemen. Weitere Informationen finden Sie unterAnalysieren von Leistungsanomalien mit DevOps Gurufor Amazon RDSaus.
- 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.
- Schauen Sie im Abschnitt Ereignisse eines Einblicks nach Bereitstellungs- oder Infrastrukturereignissen nach, die zum Zeitpunkt der Erstellung der Erkenntnisse stattfanden. Zu wissen, welche Ereignisse aufgetreten sind, als das anomale Verhalten einer Erkenntnis aufgetreten ist, kann Ihnen helfen, das Problem zu verstehen und zu diagnostizieren.
- Suchen Sie nach Tickets in Ihrem Betriebssystem, die ungefähr zur gleichen Zeit mit einem Einblick für Hinweise geschehen sind.
- Lesen Sie in einem Einblick die Empfehlungen und besuchen Sie die Links in Empfehlungen. Diese haben oft Schritte zur Fehlerbehebung, mit denen Sie Probleme schnell diagnostizieren und lösen können.
- 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 Ursache für so viele Erkenntnisse wie möglich zu verstehen. Suchen Sie nach einem Muster, das das Zeichen für ein systemisches Problem sein könnte. Wenn ein systemisches Problem ungelöst bleibt, könnte es in Zukunft ernstere Probleme verursachen. Die Behebung vorübergehender Probleme kann jetzt dazu beitragen, zukünftige, 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

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

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

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung in Guru DevOps

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, Ressourcen-IDs 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 “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.

Überwachung Ihrer 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

Du kannst einen symmetrischen, vom Kunden verwalteten Schlüssel erstellen, indem du die APIs AWS Management Console oder die AWS KMS APIs verwendest.

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
- Verwenden Sie kms:DescribeKey , um dem Kunden die vom Kunden verwalteten Schlüsselinformationen 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

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 Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern 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. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von

IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit 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, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

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

AWS-Konto Root-Benutzer

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

Verbundidentität

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

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

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

IAM-Benutzer und -Gruppen

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

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

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

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

IAM-Rollen

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

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

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

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

Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

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

Verwalten des Zugriffs mit Richtlinien

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

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

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

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

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

Ressourcenbasierte Richtlinien

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

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

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 GuruAmazonasDevOpsGeschichte des Guru-Dokuments, 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 – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte Rolle unterstützt jetzt den Zugriff auf API Gateway Gateway-GET-Aktionen auf REST-APIs.	11. Januar 2023
AmazonDevOpsGuruServiceRolePolicy – Aktualisi	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte Rolle unterstützt	19. Oktober 2022

Änderung	Beschreibung	Datum
erung auf eine bestehende Richtlinie.	jetzt mehrere Amazon Simple Storage Service- und Service Quotas Quota-Aktionen.	
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
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

Änderung	Beschreibung	Datum
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
AmazonDevOpsGuruFullAccess – Aktualisierung auf eine bestehende Richtlinie	Die `AmazonDevOpsGuruFullAccess` verwaltete Richtlinie unterstützt jetzt den Zugriff auf Amazon `DescribeDBInstances` RDS-Aktionen.	1. Dezember 2021

Änderung	Beschreibung	Datum
Identitätsbasierte Richtlinien für Amazon Guru DevOps— Neue Richtlinie hinzugefügt.	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte 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` serviceverknüpfte Rolle unterstützt jetzt AWS Organizations.	4. November 2021
AmazonDevOpsGuruServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie.	Die `AWSServiceRoleForDevOpsGuru` serviceverknüpfte Rolle enthält jetzt neue Bedingungen für die Aktionen `ssm:CreateOpsItem` und`ssm:AddTagsToResource` .	11. Oktober 2021
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

Änderung	Beschreibung	Datum
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
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
Hauptberechtigungen	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 Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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

Beispiele für identitätsbasierte Richtlinien für 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 Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden 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 kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Eine Liste der 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 bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

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

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

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

Eine Liste der DevOps Guru-Ressourcentypen und ihrer ARNs 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

Schlüssel für die Bedingungen der Richtlinien für Guru DevOps

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	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

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

Attributbasierte Zugriffskontrolle (ABAC) mit Guru DevOps

Unterstützt ABAC (Tags in Richtlinien)	Nein

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

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

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

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

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

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 zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

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

Serviceübergreifende Prinzipalberechtigungen für 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 serviceverknüpfte Rollen	Ja

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. 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 im IAM-Benutzerhandbuch.

Einzelheiten zu den von DevOps Guru definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, 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 zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Verwenden der 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 CLI AWS API erstellst, erstellt DevOps Guru die dienstbezogene 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*` spezifiziert alle DevOps Guru-Aktionen, 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

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 die *`Region-ID`* durch entsprechende Werte ersetzen (z. B.`us-west-2`) und. *`my-topic-name`*

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

Hinzufügen von Berechtigungen als IAM-Benutzer

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 die *`Region-ID`* durch entsprechende Werte ersetzen (z. B.`us-west-2`) und. *`my-topic-name`*

> **Note**
>
> Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Weitere Informationen zu bewährten Methoden in IAM finden Sie unter 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 berechtigt, 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 berechtigt, 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 die AWS CLI, AWS SDKs oder APIs zu signieren. AWS	Befolgen Sie die Anweisungen für die Schnittstelle, die Sie verwenden möchten. • Informationen zu den AWS CLI finden Sie unter Konfiguration der AWS CLI

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

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. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob DevOps Guru diese Funktionen unterstützt, finden Sie unterSo 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien 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 Amazon EC2 EC2-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

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

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-APIs aufrufen. 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 von einer Technologie unterstützt AWS PrivateLink, mit der Sie privat auf DevOps Guru-APIs zugreifen können, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine AWS Direct Connect Connect-Verbindung zu benötigen. 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, `devops-guru.us-east-1.amazonaws.com` z. B.

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 AmazonDevOpsGuru

In der folgenden Tabelle ist das aktuelle Kontingent in Amazon aufgeführtDevOpsGuru. Dieses Kontingent gilt für jeden unterstütztenAWSRegion für jedenAWSKonto.

Benachrichtigungen

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

AWS CloudFormation-Stacks

Maximale Anzahl der AWS CloudFormation-Stacks, die Sie festlegen können	1000

DevOpsGrenzwerte für die Guru-Ressourcenüberwachung

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

*Für neueDevOpsGuru-Konten, die am oder nach dem 29. Juni 2023 erstellt wurden, und für bestehende Konten, die zum gleichen Datum aktiv waren und weniger als 100 Amazon SQS-Warteschlangen haben.

**Um eine Änderung dieses Limits zu beantragen, wenden Sie sich anAWS Supportbeimhttps://aws.amazon.com/contact-us. Sie können ein Amazon 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 die Erstellung, Bereitstellung und Verwaltung einer API inDevOpsGuru, benutzt denAWS CLI, die API Gateway-Konsole oder die API Gateway-REST-API und ihre SDKs.

Für eine Liste allerDevOpsGuru-APIs, sieheAmazonasDevOpsGuru-Aktionen.

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

AmazonasDevOpsGeschichte des Guru-Dokuments

In der folgenden Tabelle wird die Dokumentation für diese Version von beschriebenDevOpsGuru.

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

Änderung	Beschreibung	Datum
Verwaltete Richtlinien-Updates	Amazon SNS-Abonnements und Zugriff auf Abonnementlisten wurden dem hinzugefügt `AmazonDevOpsGuruConsoleFullAccess` Politik. Der Zugriff auf die Abonnementliste wurde ebenfalls zur `AmazonDevOpsGuruReadOnlyAccess` Politik. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien für AmazonDevOpsGuru.	9. August 2023
Vom Kunden verwaltete Verschlüsselungsschlüssel	DevOpsGuru unterstützt jetzt Verschlüsselung mit vom Kunden verwalteten Schlüsseln mithilfe von AWS KMS. Weitere Informationen finden Sie unter Datenschutz inDevOpsGuru.	5. Juli 2023
DevOpsGuru für RDS unterstützt RDS PostgreSQL	DevOpsGuru for RDS kann Leistungsengpässe und andere Erkenntnisse in PostgreSQL-Datenbanken erkennen. Weitere Informati	30. März 2023

	onen finden Sie unterVorteile vonDevOpsGuru für RDS.	
DevOpsGuru for RDS unterstützt proaktive Erkenntnisse	DevOpsGuru for RDS veröffentlicht proaktive Erkenntnisse mit Empfehlungen, die Ihnen helfen, Probleme in Ihren Aurora-Datenbanken zu beheben, bevor sie zu größeren Problemen werden. Weitere Informationen finden Sie unterArbeiten mit Anomalien inDevOpsGuru für RDS.	28. Februar 2023
Seite „Analysierte Ressourcen“	Eine neue Seite in derDevOps Die Guru-Konsole listet Ressourcen in deinem Konto auf, die analysiert werden vonDevOpsGuru. Weitere Informationen finden Sie unterRessourcen anzeigen, die analysiert wurden vonDevOpsGuru.	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 unterAktualisierung der Amazon Amazon SNS-Benachrichtigungskonfigurationen.	30. September 2022

Ergänzung der verwalteten Richtlinien zur Analyse von Protokollanomalien	AWSverwaltete Richtlinien fürDevOpsGuru a wurden in der IAM-Konsole aktualisiert, um den Zugriff auf dieCloudWatchAktion `nFilterLogEvents` . Weitere Informationen finden Sie unterDevOpsGuru aktualisiert aufAWSverwaltete Richtlinien und dienstverknüpfte Rolle.	30. August 2022
Log-Anomalieanalyse hinzugefügt	Detaillierte Informationen zu Protokollgruppen im Zusammenhang mit Insights finden Sie imDevOpsGuru-Konsole. Zur Beschreibung steht auch eine erweiterte servicebezogene Rolle zur VerfügungCloudWatchLogs und Streams. Weitere Informationen finden Sie unterErkenntnisse verstehen in derDevOpsGuru-KonsoleundDevOpsGuru aktualisiert aufAWSverwaltete Richtlinien und dienstverknüpfte Rolle.	12. Juli 2022

CodeGuruProfiler-Integration	DevOpsGuru integriert sich jetzt in AmazonCodeGuruProfiler mit einemEventBridgeverwaltete Regel. Jedes eingehende Ereignis vonCodeGuruProfiler ist ein proaktiver Anomaliebericht. Weitere Informationen finden Sie unterIntegrieren mitCodeGuruProfiler.	7. März 2022
Serviceverknüpfte Rollen- und verwaltete Richtlinienaktualisierungen	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderungen ermöglichenDevOpsGuru zur Unterstützung einer verbesserten Integration mit Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unterVerwendung von dienstverknüpften RollenundAWSverwaltete (vordefinierte) Richtlinien fürDevOpsGuru.	21. Dezember 2021
Neue verwaltete Richtlinie hinzugefügt	Der`AmazonDevOpsGuruConsoleFullAccess` Richtlinie wurde hinzugefügt. Weitere Informationen finden Sie unterIdentitätsbasierte Richtlinien für AmazonDevOpsGuru.	6. Dezember 2021

Unterstützung bei der Definition Ihrer Anwendung mitAWSTags	Sie können jetzt verwenden AWSTags, um die gewünscht en Ressourcen zu identifiz ierenDevOpsGuru analysiert, identifiziert die Ressourcen in Ihren Anwendungen und filtert Erkenntnisse in der Konsole. Weitere Informationen finden Sie unterVerwenden Sie Tags, um Ressourcen in Ihren Anwendungen zu identifiz ieren.	1. Dezember 2021
Serviceverknüpfte Rollen- und verwaltete Richtlinienaktuali sierungen	Erweiterte Richtlinien sind in der IAM-Konsole verfügbar. Die Änderunge n ermöglichenDevOpsG uru zur Unterstützung einer verbesserten Integration mit Amazon Relational Database Service (Amazon RDS). Weitere Informationen finden Sie unterVerwendun g von dienstverknüpften RollenundAWSverwaltete (vordefinierte) Richtlinien fürDevOpsGuru.	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 unterArbeiten mit Anomalien inDevOpsGuru für Amazon RDS.	1. Dezember 2021
AmazonasEventBridgeIntegration	DevOpsGuru integriert sich jetzt mitEventBridgeum Sie über bestimmte Ereignisse im Zusammenhang mit Ihrem zu informierenDevOpsEinblicke in Guru. Weitere Informationen finden Sie unter Arbeiten mit EventBridge.	18. November 2021
AWSverwaltete Richtlinie hinzugefügt	neuAWSverwaltete Richtlinie hinzugefügt. Der`AmazonDevOpsGuruOrganizationsAccess` Richtlinie bietet Zugriff aufDevOpsGuru innerhalb einer Organisation. Weitere Informationen finden Sie unteridentitätsbasierte Richtlinien.	16. November 2021

Aktualisierung der Richtlinie für dienstverknüpfte Rollen	In der IAM-Konsole ist eine erweiterte Richtlinie verfügbar . Die Änderung ermöglich tDevOpsGuru zur Unterstüt zung der Multi-Account-Ansi cht. Weitere Informationen finden Sie unterVerwendung von dienstverknüpften Rollen.	4. November 2021
Kontenübergreifender Support	Sie können jetzt Erkenntnisse und Kennzahlen für mehrere Konten in Ihrem Unternehm en einsehen. Weitere Informati onen finden Sie unterWas ist AmazonDevOpsGuru.	4. November 2021
Version mit allgemeiner Verfügbarkeit	AmazonasDevOpsGuru ist jetzt allgemein verfügbar (GA).	4. Mai 2021
Neues Thema	Sie können jetzt einen monatlichen Kostenvor anschlag erstellen fürDevOps Guru, um deine Ressource n zu analysieren. Weitere Informationen finden Sie unterSchätzen Sie Ihr AmazonDevOpsGuru kostet.	27. April 2021

Unterstützung für VPC Endpoints	Sie können jetzt VPC-Endpunkte verwenden, um die Sicherheit Ihrer Ressourcenanalyse und der Generierung von Erkenntnissen zu verbessern. Weitere Informationen finden Sie unterDevOpsGuru- und Schnittstellen-VPC-Endpunkte (AWS PrivateLink).	15. April 2021
Neues Thema	Ein neues Thema zur ÜberwachungDevOpsGuru bei AmazonCloudWatchwurde hinzugefügt. Weitere Informationen finden Sie unterÜberwachungDevOpsGuru bei AmazonCloudWatch.	11. Dezember 2020
Vorschauversion	Dies ist die Vorschauversion desAmazonasDevOpsGuru-Benutzerhandbuch.	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.