aws

Guida per l'utente

Amazon DevOps Guru

Amazon DevOps Guru: Guida per l'utente

Table of Contents

Che cos'è Amazon DevOps Guru?

Benvenuto nella guida per l'utente di Amazon DevOps Guru.

DevOpsGuru è un servizio operativo completamente gestito che consente a sviluppatori e operatori di migliorare facilmente le prestazioni e la disponibilità delle loro applicazioni. DevOpsGuru consente di alleggerire le attività amministrative associate all'identificazione dei problemi operativi in modo da poter implementare rapidamente i consigli per migliorare l'applicazione. DevOpsGuru crea informazioni reattive che puoi utilizzare subito per migliorare la tua applicazione. Crea inoltre informazioni proattive per aiutarti a evitare problemi operativi che potrebbero influire sulla tua applicazione in futuro.

DevOpsGuru applica l'apprendimento automatico per analizzare i dati operativi e le metriche e gli eventi delle applicazioni per identificare comportamenti che si discostano dai normali schemi operativi. Riceverai una notifica quando DevOps Guru rileva un problema o un rischio operativo. Per ogni numero, DevOps Guru presenta raccomandazioni intelligenti per affrontare i problemi operativi attuali e previsti per il futuro.

Per iniziare, consulta Come posso iniziare a usare DevOps Guru?

Come funziona DevOps Guru?

Il flusso di lavoro DevOps Guru inizia quando ne configuri la copertura e le notifiche. Dopo aver configurato DevOps Guru, inizia ad analizzare i dati operativi. Quando rileva un comportamento anomalo, crea un'analisi che contiene consigli ed elenchi di metriche, gruppi di log ed eventi correlati al problema. Per ogni intuizione, DevOps Guru ti avvisa. Se abilitato AWS Systems Manager OpsCenter, OpsItem viene creato un file in modo da poter utilizzare Systems Manager OpsCenter per monitorare e gestire l'indirizzamento delle informazioni acquisite. Ogni analisi contiene consigli, metriche, gruppi di log ed eventi relativi a comportamenti anomali. Utilizza le informazioni in un'analisi approfondita per aiutarti a comprendere e risolvere il comportamento anomalo.

Flusso di lavoro Guru di alto livello DevOpsPer ulteriori dettagli, consulta le tre fasi del flusso di lavoro di alto livello. Scopri Flusso di lavoro dettagliato di DevOps Guru di più sul flusso di lavoro DevOps Guru più dettagliato, incluso il modo in cui interagisce con altri servizi. AWS

Argomenti

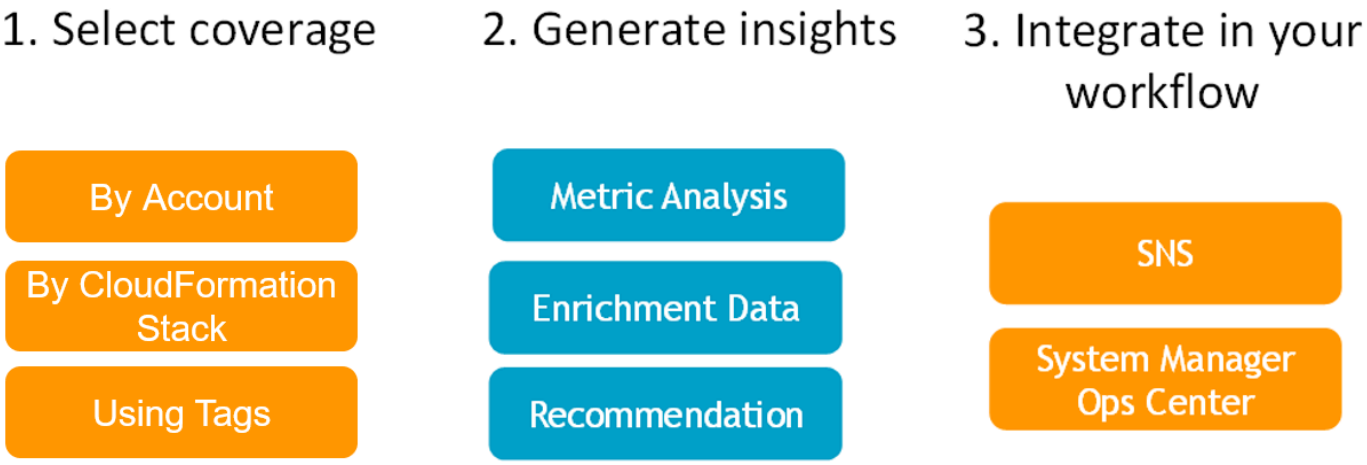
- Flusso di lavoro dettagliato di DevOps Guru

Flusso di lavoro Guru di alto livello DevOps

Il flusso di lavoro di Amazon DevOps Guru può essere suddiviso in tre fasi di alto livello.

1. Specificate la copertura di DevOps Guru indicandogli quali AWS risorse del vostro AWS account desiderate che analizzi.
2. DevOpsGuru inizia ad analizzare le CloudWatch metriche di Amazon e altri dati operativi per identificare i problemi che puoi risolvere per migliorare le tue operazioni. AWS CloudTrail
3. DevOpsGuru si assicura che tu conosca approfondimenti e informazioni importanti inviandoti una notifica per ogni evento importante di Guru. DevOps

Puoi anche configurare DevOps Guru in modo che crei un messaggio che ti aiuti OpsItem AWS Systems Manager OpsCenter a tenere traccia delle tue intuizioni. Il diagramma seguente mostra questo flusso di lavoro di alto livello.



1. Nella prima fase, scegli la tua copertura specificando quali AWS risorse del tuo AWS account vengono analizzate. DevOpsGuru può coprire o analizzare tutte le risorse di un AWS account, oppure puoi utilizzare AWS CloudFormation pile o AWS tag per specificare un sottoinsieme delle risorse del tuo account da analizzare. Assicurati che le risorse specificate costituiscano le applicazioni, i carichi di lavoro e i microservizi aziendali critici. Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.
2. Nella seconda fase, DevOps Guru analizza le risorse per generare approfondimenti. Si tratta di un processo continuo. Puoi visualizzare gli approfondimenti e vedere i consigli e le informazioni

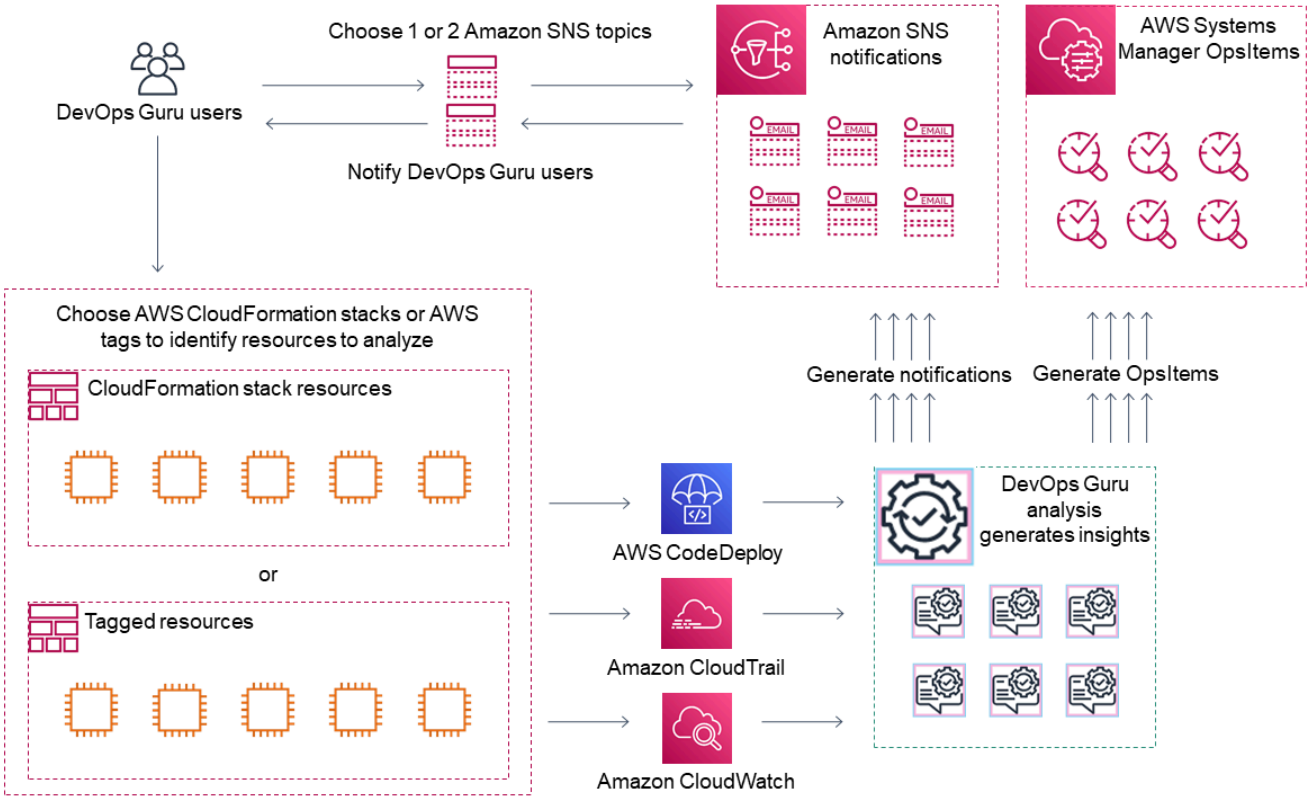
correlate che contengono nella console DevOps Guru. DevOpsGuru analizza i seguenti dati per trovare problemi e creare approfondimenti.

- CloudWatch Parametri Amazon individuali emessi dalle tue AWS risorse. Quando viene identificato un problema, DevOps Guru raccoglie insieme tali metriche.
- Anomalie dei log provenienti dai gruppi di CloudWatch log di Amazon. Se abiliti il rilevamento delle anomalie nei log, DevOps Guru visualizza le anomalie dei log correlate quando si verifica un problema.
- DevOpsGuru estrae i dati di arricchimento dai log di AWS CloudTrail gestione per trovare eventi correlati alle metriche raccolte. Gli eventi possono essere eventi di distribuzione delle risorse e modifiche alla configurazione.
- Se lo utilizzi AWS CodeDeploy, DevOps Guru analizza gli eventi di distribuzione per contribuire a generare approfondimenti. Vengono analizzati gli eventi per tutti i tipi di CodeDeploy implementazioni (server locale, server Amazon EC2, Lambda o Amazon EC2).
- Quando DevOps Guru trova uno schema specifico, genera uno o più consigli per aiutare a mitigare o risolvere il problema identificato. Le raccomandazioni vengono raccolte in un'unica analisi. L'analisi contiene anche un elenco delle metriche e degli eventi correlati al problema. I dati di analisi vengono utilizzati per affrontare e comprendere il problema identificato.

3. Nella terza fase, DevOps Guru integra la notifica approfondita nel flusso di lavoro per aiutarti a gestire i problemi e risolverli rapidamente.
   - Gli approfondimenti generati nel tuo AWS account vengono pubblicati sull'argomento Amazon Simple Notification Service (Amazon SNS) scelto DevOps durante la configurazione di Guru. In questo modo riceverai una notifica non appena viene creata un'analisi. Per ulteriori informazioni, consulta Aggiornamento delle notifiche in DevOpsGuru.
   - Se l'hai abilitato AWS Systems Manager durante la configurazione di DevOps Guru, ogni analisi ne crea una corrispondente OpsItem per aiutarti a tracciare e gestire i problemi scoperti. Per ulteriori informazioni, consulta AggiornamentoAWS Systems Managerintegrazione inDevOpsGuru.

Flusso di lavoro dettagliato di DevOps Guru

Il flusso di lavoro DevOps Guru si integra con diversi AWS servizi, tra cui Amazon CloudWatch, AWS CloudTrail Amazon Simple Notification Service e. AWS Systems Manager Il diagramma seguente mostra un flusso di lavoro dettagliato che include il modo in cui funziona con altri servizi. AWS



Questo diagramma mostra uno scenario in cui la copertura di DevOps Guru è specificata dalle AWS risorse definite in AWS CloudFormation pile o utilizzando i tag. AWS Se non vengono scelti pile o tag, DevOps Guru Coverage analizza tutte le risorse del tuo account. AWS Per ulteriori informazioni, consulta Definizione delle applicazioni utilizzandoAWSrisorse e Determina la copertura per DevOps Guru.

1. Durante la configurazione, specifichi uno o due argomenti di Amazon SNS che vengono utilizzati per informarti su importanti eventi DevOps Guru, ad esempio quando viene creata una panoramica. Successivamente, puoi specificare gli AWS CloudFormation stack che definiscono le risorse che desideri analizzare. Puoi anche consentire a Systems Manager di generare una OpsItem per ogni analisi per aiutarti a gestire le tue informazioni.
2. Dopo la configurazione, DevOps Guru inizia ad analizzare le CloudWatch metriche, i gruppi di log e gli eventi emessi dalle risorse e dai AWS CloudTrail dati relativi alle metriche. CloudWatch Se le tue operazioni includono CodeDeploy distribuzioni, Guru analizza anche gli eventi di distribuzione. DevOps

   DevOpsGuru crea approfondimenti quando identifica comportamenti insoliti e anomali nei dati analizzati. Ogni analisi contiene uno o più consigli, un elenco delle metriche utilizzate per generare

l'analisi, un elenco di gruppi di log correlati e un elenco degli eventi utilizzati per generare l'analisi. Utilizzate queste informazioni per risolvere il problema identificato.

3. Dopo aver creato ogni approfondimento, DevOps Guru invia una notifica utilizzando l'argomento o gli argomenti di Amazon SNS specificati DevOps durante la configurazione di Guru. Se hai abilitato DevOps Guru a generare un OpsItem Systems Manager OpsCenter, ogni analisi attiva anche un nuovo Systems Manager. OpsItem Puoi usare Systems Manager per gestire le tue informazioni OpsItems.

Come posso iniziare a usare DevOps Guru?

È consigliabile completare la procedura seguente:

1. Scopri di più su DevOps Guru leggendo le informazioni in. DevOpsConcetti del guru
2. Configura il tuo AWS account AWS CLI, il e un utente amministrativo seguendo la procedura riportata di seguito. Configurazione di Amazon DevOps Guru
3. Usa DevOps Guru seguendo le istruzioni riportate inGuida introduttiva a DevOps Guru.

Come faccio a smettere di incorrere in addebiti per Guru DevOps?

Per disabilitare Amazon DevOps Guru in modo da evitare addebiti per l'analisi delle risorse nel tuo AWS account e nella tua regione, aggiorna le impostazioni di copertura in modo che non analizzi le risorse. Per fare ciò, segui i passaggi indicati Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru e scegli Nessuno nel passaggio 4. È necessario eseguire questa operazione per ogni AWS account e regione in cui DevOps Guru analizza le risorse.

> **Note**
>
> Se aggiorni la copertura per interrompere l'analisi delle risorse, potresti continuare a incorrere in lievi addebiti se rivedi le informazioni esistenti generate da DevOps Guru in passato. Questi costi sono associati alle chiamate API utilizzate per recuperare e visualizzare informazioni dettagliate. Per ulteriori informazioni, consulta i prezzi di Amazon DevOps Guru.

DevOpsConcetti del guru

I seguenti concetti sono importanti per comprendere il funzionamento di Amazon DevOps Guru.

Argomenti

Anomalia

Un'anomalia rappresenta una o più metriche correlate rilevate da DevOps Guru che sono inaspettate o insolite. DevOpsGuru genera anomalie utilizzando l'apprendimento automatico per analizzare metriche e dati operativi correlati alle tueAWS risorse. Specifichi leAWS risorse che desideri analizzare quando configuri Amazon DevOps Guru. Per ulteriori informazioni, consulta Configurazione di Amazon DevOps Guru.

Informazione dettagliata

Un'intuizione è una raccolta di anomalie che vengono create durante l'analisi delleAWS risorse specificate quando configuri DevOps Guru. Ogni analisi contiene osservazioni, consigli e dati analitici che puoi utilizzare per migliorare le tue prestazioni operative. Esistono due tipi di informazioni:

- Reattivo: un'intuizione reattiva identifica un comportamento anomalo non appena si verifica. Contiene anomalie con consigli, metriche correlate ed eventi per aiutarti a comprendere e risolvere subito i problemi.
- Proattivo: un'analisi proattiva consente di conoscere il comportamento anomalo prima che si verifichi. Contiene anomalie e consigli per aiutarti a risolvere i problemi prima che si verifichino.

Parametri ed eventi operativi

Le anomalie che costituiscono un'analisi approfondita vengono generate analizzando le metriche restituite da Amazon CloudWatch e gli eventi operativi emessi dalle tueAWS risorse. È possibile visualizzare le metriche e gli eventi operativi che creano una panoramica che consente di comprendere meglio i problemi della propria applicazione.

Gruppi di registri e registro di registro

Quando si abilita il rilevamento delle anomalie di registro, i gruppi di log pertinenti vengono visualizzati nelle pagine di analisi di DevOps Guru nella console DevOps Guru. Un gruppo di log consente di conoscere informazioni diagnostiche critiche sulle prestazioni e sull'accesso a una risorsa.

Un'anomalia del registro rappresenta un gruppo di eventi di registro anomali simili trovati all'interno di un gruppo di log. Esempi di eventi di registro anomali che possono essere visualizzati in DevOps Guru includono anomalie di parole chiave, anomalie di formato, anomalie del codice HTTP e altro ancora.

È possibile utilizzare le anomalie dei log per diagnosticare la causa principale di un problema operativo. DevOpsGuru fa anche riferimento alle righe di registro nei consigli di analisi per fornire un maggiore contesto alle soluzioni consigliate.

> **Note**
>
> DevOpsGuru collabora con Amazon CloudWatch per abilitare il rilevamento delle anomalie dei log. Quando abiliti il rilevamento delle anomalie di registro, DevOps Guru aggiunge tag ai tuoi gruppi di CloudWatch log. Quando disattivi il rilevamento delle anomalie di registro, DevOps Guru rimuove i tag dai tuoi gruppi di CloudWatch log.
> Inoltre, gli amministratori devono assicurarsi che solo gli utenti con autorizzazioni per visualizzare CloudWatch i log abbiano le autorizzazioni per visualizzare CloudWatch i log anomali. Ti consigliamo di usare le policy IAM per consentire o negare l'accesso all'`ListAnomalousLogs`operazione. Per ulteriori informazioni, vedere Identity and Access Management for DevOps Guru.

Raccomandazioni

Ogni informazioni fornisce consigli e suggerimenti per migliorare le prestazioni dell'applicazione. La raccomandazione include i seguenti elementi:

- Una descrizione delle azioni raccomandate per risolvere le anomalie che costituiscono l'analisi.
- Un elenco delle metriche analizzate in cui DevOps Guru ha riscontrato un comportamento anomalo. Ogni metrica include il nome delloAWS CloudFormation stack che ha generato la risorsa associata alle metriche, il nome della risorsa e il nome delAWS servizio associato alla risorsa.

- Un elenco degli eventi correlati alle metriche anomale associate all'analisi. Ogni evento correlato contiene il nome delloAWS CloudFormation stack che ha generato la risorsa associata all'evento, il nome della risorsa che ha generato l'evento e il nome delAWS servizio associato all'evento.
- Un elenco di gruppi di log correlati al comportamento anomalo associato all'analisi. Ogni gruppo di log contiene un messaggio di registro di esempio, informazioni sui tipi di anomalie di registro segnalate, l'ora in cui si sono verificate le anomalie del registro e un collegamento per visualizzare le righe di registro CloudWatch.

DevOpsCopertura Guru

DevOpsGuru indirizza e crea approfondimenti per una serie di servizi diversi. AWS Per ogni servizio per cui DevOps Guru crea approfondimenti, DevOps Guru mostra una varietà di metriche analizzate e approfondimenti generati.

Esempio di utilizzo per approfondimenti reattivi:

Nome del servizio	Caso d'uso	Esempi	Metriche
AWS Lambda	Rileva anomalie di latenza o durata per le funzioni Lambda causate da varie cause principali come partenze a freddo, aumento delle richieste, throttling a valle o implement azioni di codice. Consiglia modi per mitigare rapidamente.	Distribuzione del codice: Amazon API Gateway la latenza è influenzata da un aumento della latenza Lambda dopo una recente implement azione del codice Lambda. Throttling a valle: l'operatore ha ridotto la capacità delle unità di lettura per DynamoDB, causando un aumento dei tentativi. Ciò si traduce in una limitazione. Avvio a freddo: il provision ing della funzione	Durata Throttles

Nome del servizio	Caso d'uso	Esempi	Metriche
		Lambda è insuffici ente, quindi Lambda impiega più tempo quando vengono effettuate le richieste.	

Esempio di utilizzo per approfondimenti proattivi:

Nome del servizio	Caso d'uso	Metriche
Amazon DynamoDB	La capacità consumata in lettura della tabella DynamoDB rischia di raggiungere il limite della tabella. Azione consigliata: se si utilizza la modalità di capacità assegnata, utilizzar e la scalabilità automatica per gestire attivamente la capacità di throughput per le tabelle o acquistare in anticipo la capacità riservata per le tabelle. Passa alla modalità di capacità su richiesta per pagare per richiesta di lettura, pagando solo per ciò che viene utilizzato. Tempo di rilevamento: 6 giorni	ConsumedReadCapacityUnits

Elenco di copertura del servizio

Per alcuni servizi, DevOps Guru crea approfondimenti reattivi. Un approfondimento reattivo identifica un comportamento anomalo nel momento in cui si verifica. Contiene anomalie con consigli, metriche correlate ed eventi per aiutarti a comprendere e risolvere subito i problemi.

Per alcuni servizi, DevOps Guru crea approfondimenti proattivi. Un'analisi proattiva ti consente di conoscere i comportamenti anomali prima che si verifichino. Contiene anomalie e consigli per aiutarvi a risolvere i problemi prima che si verifichino.

DevOpsGuru crea approfondimenti reattivi per servizi come i seguenti:

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

> **Note**
>
> DevOpsIl monitoraggio Guru avviene a livello di gruppo Auto Scaling e non a livello di singola istanza.

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Sistema di bilanciamento del carico elastico
- 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 crea approfondimenti proattivi per servizi come i seguenti:

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

Configurazione di Amazon DevOps Guru

Completa le attività in questa sezione per configurare Amazon DevOps Guru per la prima volta. Se hai già un AWS account, sai quale o quali AWS account vuoi analizzare e hai un argomento di Amazon Simple Notification Service da utilizzare per le notifiche di approfondimento, puoi passare direttamente aGuida introduttiva a DevOps Guru.

Facoltativamente, puoi utilizzare Quick Setup, una funzionalità di AWS Systems Manager, per configurare DevOps Guru e configurarne rapidamente le opzioni. Puoi usare Quick Setup per configurare DevOps Guru per un account o un'organizzazione autonomi. Per utilizzare Quick Setup in Systems Manager per configurare DevOps Guru per un'organizzazione, è necessario disporre dei seguenti prerequisiti:

- Un'organizzazione con. AWS Organizations Per ulteriori informazioni, consulta la AWS Organizations terminologia e i concetti nella Guida per l'AWS Organizations utente.
- Due o più unità organizzative (OU).
- Uno o più AWS account target in ogni unità organizzativa.
- Un account amministratore con privilegi per gestire gli account di destinazione.

Per informazioni su come configurare DevOps Guru utilizzando Quick Setup, consulta Configure DevOps Guru with Quick Setup nella Guida per l'AWS Systems Manager utente.

Usa i seguenti passaggi per configurare DevOps Guru senza Quick Setup.

- Passaggio 1: iscriviti a AWS
- Fase 2: Determinare la copertura per DevOps Guru
- Fase 3: Identifica l'argomento relativo alle notifiche di Amazon SNS

Passaggio 1: iscriviti a AWS

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.

2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i AWS servizi nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Fase 2: Determinare la copertura per DevOps Guru

La copertura dei confini determina le AWS risorse che vengono analizzate da Amazon DevOps Guru per rilevare comportamenti anomali. Ti consigliamo di raggruppare le tue risorse in applicazioni operative. Tutte le risorse nel limite delle risorse devono comprendere una o più applicazioni. Se si dispone di un'unica soluzione operativa, il limite di copertura dovrebbe includere tutte le relative risorse. Se disponi di più applicazioni, scegli le risorse che compongono ciascuna soluzione e raggruppale utilizzando AWS CloudFormation pile o AWS tag. Tutte le risorse combinate che specificate, indipendentemente dal fatto che definiscano una o più applicazioni, vengono analizzate da DevOps Guru e ne costituiscono il limite di copertura.

Utilizzate uno dei seguenti metodi per specificare le risorse nelle vostre soluzioni operative.

- Scegliete che la vostra AWS regione e il vostro account definiscano il limite di copertura. Con questa opzione, DevOps Guru analizza tutte le risorse del tuo account e della tua regione. Questa è una buona opzione da scegliere se utilizzi il tuo account per una sola applicazione.
- Utilizzate AWS CloudFormation gli stack per definire le risorse nella vostra applicazione operativa. AWS CloudFormation i modelli definiscono e generano le risorse per te. Specificate gli stack che creano le risorse dell'applicazione quando configurate DevOps Guru. Puoi aggiornare i tuoi stack in qualsiasi momento. Tutte le risorse degli stack che scegli definiscono la copertura dei confini. Per ulteriori informazioni, consulta Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru.
- Utilizzate i AWS tag per specificare AWS le risorse nelle vostre applicazioni. DevOpsGuru analizza solo le risorse che contengono i tag scelti. Queste risorse costituiscono il tuo limite.

  Un AWS tag è composto da una chiave di tag e da un valore di tag. È possibile specificare una chiave di tag e specificare uno o più valori con quella chiave. Usa un valore per tutte le risorse di una delle tue applicazioni. Se disponi di più applicazioni, utilizza un tag con la stessa chiave per tutte e raggruppa le risorse nelle applicazioni utilizzando i valori dei tag. Tutte le risorse con i tag scelti costituiscono il limite di copertura per DevOps Guru. Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.

Se la copertura dei confini include risorse che costituiscono più di un'applicazione, puoi utilizzare i tag per filtrare le tue informazioni e visualizzarle per un'applicazione alla volta. Per ulteriori informazioni, consulta la Fase 4 del VisualizzazioneDevOpsGuru Insights

Per ulteriori informazioni, consulta Definizione delle applicazioni utilizzandoAWSrisorse. Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

Fase 3: Identifica l'argomento relativo alle notifiche di Amazon SNS

Utilizzi uno o due argomenti di Amazon SNS per generare notifiche su importanti eventi DevOps Guru, ad esempio quando viene creata una panoramica. Questo ti assicura di conoscere i problemi rilevati da DevOps Guru il prima possibile. Tieni pronti i tuoi argomenti quando configuri DevOps Guru. Quando usi la console DevOps Guru per configurare DevOps Guru, specifichi un argomento di notifica usando il suo nome o il suo Amazon Resource Name (ARN). Per ulteriori informazioni, consulta Enable Guru. DevOps Puoi utilizzare la console Amazon SNS per visualizzare il nome e l'ARN per ciascuno dei tuoi argomenti. Se non hai un argomento, puoi crearne uno abilitando DevOps Guru utilizzando la DevOps console Guru. Per ulteriori informazioni, consulta Creazione di un argomento nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Autorizzazioni aggiunte al tuo argomento Amazon SNS

Un argomento di Amazon SNS è una risorsa che contiene una policy sulle risorse AWS Identity and Access Management (IAM). Quando specifichi un argomento qui, DevOps Guru aggiunge le seguenti autorizzazioni alla sua politica sulle risorse.

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

Queste autorizzazioni sono necessarie a DevOps Guru per pubblicare notifiche utilizzando un argomento. Se preferisci non avere queste autorizzazioni sull'argomento, puoi rimuoverle in tutta sicurezza e l'argomento continuerà a funzionare come prima di sceglierlo. Tuttavia, se queste autorizzazioni aggiunte vengono rimosse, DevOps Guru non può utilizzare l'argomento per generare notifiche.

Stima dei costi di analisi delle risorse di Amazon DevOps Guru

Puoi stimare il costo mensile per Amazon DevOps Guru per analizzare le tue risorse AWS. Paghi per il numero di ore analizzate per ogni risorsa AWS attiva nella copertura di risorse specificata. Una risorsa è attiva se produce metriche, eventi o log entro un'ora.

DevOps Guru analizza le risorse selezionate per creare una stima mensile dei costi. Puoi visualizzare le risorse, il loro prezzo orario fatturabile e la tariffa mensile stimata. Per impostazione predefinita, lo strumento di stima dei costi presuppone che le risorse attive analizzate vengano utilizzate il 100% delle volte. È possibile modificare questa percentuale per ogni servizio analizzato in base all'utilizzo stimato per creare una stima dei costi mensile aggiornata. La stima si riferisce al costo di analisi delle risorse e non include i costi associati alle chiamate all'API DevOps Guru.

È possibile creare una stima dei costi alla volta. Il tempo necessario per generare una stima dei costi dipende dal numero di risorse specificato al momento della creazione della stima dei costi. Quando si specificano alcune risorse, il completamento può richiedere da 1 a 2 ore. Quando si specificano molte risorse, il completamento può richiedere fino a 4 ore. I costi effettivi variano e dipendono dalla percentuale di tempo in cui vengono utilizzate le risorse attive analizzate.

> **Note**
>
> Per una stima dei costi, puoi specificare solo uno AWS CloudFormation stack. Per il limite di copertura effettivo, puoi specificare fino a 1000 pile.

Per creare una stima mensile dei costi per l'analisi delle risorse

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Scegli Cost Estimator nel pannello di navigazione.
3. Se non hai abilitato DevOps Guru, devi creare un ruolo IAM. Nella finestra popup Crea ruolo IAM per DevOps Guru che appare, scegli Accetta per creare il ruolo IAM. Ciò consente a DevOps Guru di creare un ruolo collegato ai servizi IAM per te quando scegli di iniziare l'analisi della stima dei costi o iniziare a utilizzare Guru. DevOps In questo modo, DevOps Guru dispone delle autorizzazioni necessarie per creare la stima dei costi. Se hai già abilitato DevOps Guru, il ruolo è già stato creato e questa opzione non viene visualizzata.

4. Scegli le risorse che desideri utilizzare per creare il tuo preventivo.

   - Se vuoi stimare il costo che DevOps Guru deve sostenere per analizzare le risorse definite da uno AWS CloudFormation stack, procedi come segue.

     1. Scegli CloudFormation lo stack nella regione corrente.
     2. In Scegli uno CloudFormation stack, scegli il nome di uno AWS CloudFormation stack nel tuo account. AWS Puoi anche inserire il nome di uno stack per trovarlo rapidamente. Per informazioni su come utilizzare e visualizzare gli stack, consulta Lavorare con gli stack nella Guida per l'AWS CloudFormationutente.
     3. (Facoltativo) Se utilizzi uno AWS CloudFormation stack che attualmente non stai analizzando, scegli Abilita l'analisi delle risorse per consentire a DevOps Guru di iniziare ad analizzare le sue risorse. Questa opzione non è disponibile se non hai abilitato DevOps Guru o se stai già analizzando le risorse nello stack.

   - Se vuoi stimare il costo sostenuto da DevOps Guru per analizzare le risorse con un tag, procedi come segue.

     1. Scegli Tag sulle AWS risorse nella regione corrente
     2. In Tag key scegli la chiave del tuo tag
     3. In Tag value scegli (tutti i valori) o scegli un valore.

   - Se vuoi stimare il costo che DevOps Guru deve sostenere per analizzare la risorsa nel tuo AWS account e nella tua regione, scegli l'AWSaccount nella regione corrente.

5. Scegli Costo mensile stimato.
6. (Facoltativo) Nella colonna Active resource utilization%, inserisci un valore percentuale aggiornato per uno o più servizi AWS. La percentuale di utilizzo attivo delle risorse di default è 100%. Ciò significa che DevOps Guru genera la stima per il servizio AWS calcolando il costo di un'ora di analisi delle sue risorse, quindi estrapolandolo in 30 giorni per un totale di 720 ore. Se un servizio è attivo meno del 100% del tempo, puoi aggiornare la percentuale in base all'utilizzo stimato per una stima più accurata. Ad esempio, se si aggiorna l'utilizzo attivo delle risorse di un servizio al 75%, il costo di un'ora per l'analisi delle risorse viene estrapolato su (720 x 0,75) ore o 540 ore.

Se la stima è pari a zero dollari, le risorse scelte probabilmente non includono le risorse supportate da Guru. DevOps Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

Guida introduttiva a DevOps Guru

In questa sezione, scopri come iniziare a usare Amazon DevOps Guru in modo che possa analizzare i dati e le metriche operative della tua applicazione per generare approfondimenti.

Argomenti

Fase 1: Inizia la configurazione

Prima di iniziare, preparati eseguendo i passaggi seguentiConfigurazione di Amazon DevOps Guru.

Passaggio 2: Abilita DevOps Guru

Per configurare Amazon DevOps Guru in modo che venga utilizzato per la prima volta, devi scegliere come configurare DevOps Guru. Puoi monitorare le applicazioni all'interno della tua organizzazione o monitorare le applicazioni nel tuo account corrente.

È possibile monitorare le applicazioni in tutta l'organizzazione o abilitare DevOps Guru esclusivamente per l'account corrente. Le seguenti procedure descrivono diversi modi per configurare DevOps Guru in base alle proprie esigenze.

Monitora gli account in tutta l'organizzazione

Se scegli di monitorare le applicazioni in tutta l'organizzazione, accedi al tuo account di gestione dell'organizzazione. Facoltativamente, puoi configurare un account membro dell'organizzazione come amministratore delegato. È possibile avere un solo amministratore delegato alla volta e modificare le impostazioni dell'amministratore in un secondo momento. Sia l'account di gestione che l'account amministratore delegato che configuri hanno accesso a tutte le informazioni dettagliate di tutti gli account dell'organizzazione.

Puoi aggiungere il supporto per più account per la tua organizzazione utilizzando la Console oppure puoi farlo utilizzando la AWS CLI.

Effettua il login con la DevOps console Guru

Puoi utilizzare la Console per aggiungere il supporto per gli account all'interno dell'organizzazione.

Usa la Console per consentire a DevOps Guru di visualizzare informazioni aggregate

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Scegli Monitora le applicazioni nelle tue organizzazioni come tipo di configurazione.
3. Scegli l'account che desideri utilizzare come amministratore delegato. Quindi, scegli Registra amministratore delegato. Ciò fornisce l'accesso a una visualizzazione consolidata per qualsiasi account con DevOps Guru abilitato. L'amministratore delegato ha una visione consolidata di tutte le informazioni e le metriche di DevOps Guru all'interno dell'organizzazione. Puoi abilitare altri account con la configurazione rapida SSM o i set di stack. AWS CloudFormation Per saperne di più sulla configurazione rapida, consulta Configura DevOps Guru con Quick Setup. Per ulteriori informazioni sulla configurazione con i set di stack, consulta Lavorare con gli stack nella Guida per l'AWS CloudFormation utente e. eFase 2: Determinare la copertura per DevOps Guru. Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru

Integrazione con la CLI AWS

Puoi utilizzare la AWS CLI per consentire a DevOps Guru di visualizzare approfondimenti aggregati. Esegui i comandi seguenti.

```
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
```

La tabella seguente descrive i comandi.

Comando	Descrizione
`create-service-linked-role`	

Comando	Descrizione
	Autorizza DevOps Guru a raccogliere informazioni sulla tua organizzazione. Non procedere se questo passaggio non va a buon fine.
`enable-aws-service-access`	Inserimento della tua organizzazione in DevOps Guru.
`register-delegated-administrator`	Fornisce l'accesso all'account del membro per visualizzare approfondimenti.

Monitora il tuo account corrente

Se scegli di monitorare le applicazioni nel tuo AWS account corrente, scegli quali AWS risorse del tuo account e della regione sono coperte o analizzate e specifica uno o due argomenti di Amazon Simple Notification Service da utilizzare per informarti quando viene creata un'analisi. Puoi aggiornare queste impostazioni in un secondo momento, se necessario.

Consenti a DevOps Guru di monitorare le applicazioni nel tuo account corrente AWS

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Scegli Monitora le applicazioni nell' AWS account corrente come tipo di configurazione.
3. In DevOpsGuru Analysis Coverage, scegli una delle seguenti opzioni.

   - Analizza tutte AWS le risorse dell' AWS account corrente: DevOps Guru analizza tutte le AWS risorse del tuo account.
   - Scegli le risorse AWS da analizzare in un secondo momento: scegli il limite dell'analisi in un secondo momento. Per ulteriori informazioni, consulta Determina la copertura per DevOps Guru e Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru.

   DevOpsGuru può analizzare qualsiasi risorsa associata all' AWS account che supporta. Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

4. Puoi aggiungere fino a due argomenti. DevOpsGuru usa l'argomento o gli argomenti per informarti su eventi importanti del DevOps Guru, come la creazione di una nuova intuizione. Se non specifichi un argomento ora, puoi aggiungerne uno in un secondo momento scegliendo Impostazioni nel riquadro di navigazione.

   a. In Specificare un argomento Amazon SNS, scegli un argomento da utilizzare.

   b. Per aggiungere un argomento Amazon SNS, esegui una delle seguenti operazioni.

      - Scegli Genera un nuovo argomento SNS tramite e-mail. Quindi, in Specificare l'indirizzo e-mail, inserisci l'indirizzo e-mail a cui desideri ricevere le notifiche. Per inserire altri indirizzi e-mail, scegli Aggiungi nuova email.
      - Scegli Usa un argomento SNS esistente. Quindi, da Scegli un argomento nel tuo AWS account, scegli l'argomento che desideri utilizzare.
      - Scegli Usa un argomento SNS esistente ARN per specificare un argomento esistente da un altro account. Quindi, in Inserisci un ARN per un argomento, inserisci l'argomento ARN. L'ARN è il nome della risorsa Amazon dell'argomento. Puoi specificare un argomento in un altro account. Se utilizzi un argomento in un altro account, devi aggiungere una politica sulle risorse all'argomento. Per ulteriori informazioni, consulta Autorizzazioni per argomenti di Amazon SNS.

5. Scegli Abilita .

Per configurare Amazon DevOps Guru in modo che venga utilizzato per la prima volta, devi scegliere quali AWS risorse del tuo account e della tua regione sono coperte o analizzate e specificare uno o due argomenti di Amazon Simple Notification Service da utilizzare per avvisarti quando viene creata un'analisi. Puoi aggiornare queste impostazioni in un secondo momento, se necessario.

Passaggio 3: Specificate la copertura delle risorse DevOps Guru

Se hai scelto di specificare le AWS risorse in un secondo momento, quando hai abilitato DevOps Guru, devi scegliere gli AWS CloudFormation stack del tuo AWS account che creano le risorse che desideri analizzare. Uno AWS CloudFormation stack è una raccolta di AWS risorse che gestisci come singola unità. È possibile utilizzare uno o più stack per includere tutte le risorse necessarie per eseguire le applicazioni operative, quindi specificarle in modo che vengano analizzate da DevOps Guru. Se non specifichi gli stack, DevOps Guru analizza tutte le risorse del AWS tuo account. Per ulteriori informazioni, consulta Lavorare con gli stack nella Guida per l'AWS CloudFormation utente

e. e. Determina la copertura per DevOps Guru Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru

> **Note**
>
> Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

Specificate la DevOps copertura delle risorse Guru

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Espandi Impostazioni nel riquadro di navigazione.
3. In Risorse analizzate, scegli Modifica risorse analizzate.
4. Scegli una delle seguenti opzioni di copertura.

   - Scegli Tutte le risorse dell'account se desideri che DevOps Guru analizzi tutte le risorse supportate nel tuo AWS account e nella tua regione. Se scegli questa opzione, il tuo AWS account rappresenta il limite di copertura per l'analisi delle risorse. Tutte le risorse di ogni stack del tuo account sono raggruppate nella rispettiva applicazione. Tutte le risorse rimanenti che non fanno parte di uno stack vengono raggruppate nella rispettiva applicazione.
   - CloudFormation Scegliete le pile se volete che DevOps Guru analizzi le risorse presenti nelle pile da voi scelte, allora scegliete una delle seguenti opzioni.
     - Tutte le risorse: vengono analizzate tutte le risorse presenti negli stack del tuo account. Le risorse di ogni stack sono raggruppate nella rispettiva applicazione. Le risorse dell'account che non fanno parte di uno stack non vengono analizzate.
     - Seleziona pile: seleziona le pile che desideri che DevOps Guru analizzi. Le risorse di ogni stack selezionato vengono raggruppate nella rispettiva applicazione. Puoi inserire il nome di uno stack in Trova pile per individuare rapidamente uno stack specifico. Puoi selezionare fino a 1.000 pile.

     Per ulteriori informazioni, consulta Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru.
   - Scegli Tag se vuoi che DevOps Guru analizzi tutte le risorse che contengono i tag che hai scelto. Scegli una chiave, quindi scegli una delle seguenti opzioni.

- Tutte le risorse dell'account: analizza tutte le risorse AWS nella regione e nell'account correnti. Le risorse con la chiave di tag selezionata sono raggruppate in base al valore del tag, se esistente. Le risorse prive di questa chiave di tag vengono raggruppate e analizzate separatamente.
- Scegli valori di tag specifici: vengono analizzate tutte le risorse che contengono un tag con la chiave scelta. DevOpsGuru raggruppa le tue risorse in applicazioni in base ai valori del tag.

  La chiave del tag deve iniziare con il prefisso`devops-guru-`. Questo prefisso non fa distinzione tra maiuscole e minuscole. Ad esempio, una chiave valida è. `DevOps-Guru-Production-Applications` Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.

- Scegli Nessuno se non vuoi che DevOps Guru analizzi alcuna risorsa. Questa opzione disabilita DevOps Guru in modo da evitare di incorrere in addebiti derivanti dall'analisi delle risorse.

5. Selezionare Salva.

AWSServizi abilitanti per l'DevOpsanalisi Guru

Amazon DevOps Guru può analizzare le prestazioni di qualsiasi AWS risorsa supportata. Quando rileva un comportamento anomalo, genera un'analisi con dettagli sul comportamento e su come affrontarlo. Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

DevOpsGuru utilizza le CloudWatch metriche, AWS CloudTrail gli eventi e altro ancora di Amazon per analizzare le risorse. La maggior parte delle risorse supportate genera automaticamente le metriche necessarie per l'analisi di DevOps Guru. Tuttavia, alcuni AWS servizi richiedono un'azione aggiuntiva per generare le metriche richieste. Per alcuni servizi, l'abilitazione di queste metriche fornisce un'analisi aggiuntiva della copertura DevOps Guru esistente. Per altri, l'analisi non è possibile finché non si abilitano queste metriche. Per ulteriori informazioni, consultare Determina la copertura per DevOps Guru e Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru.

Servizi che richiedono interventi per l'analisi di DevOps Guru

- Amazon Elastic Container Service: per generare parametri aggiuntivi che migliorino la copertura delle risorse di DevOps Guru, segui i passaggi indicati in Configurazione delle informazioni sui container su Amazon ECS. Questa operazione potrebbe comportare costi da AmazonCloudWatch.
- Amazon Elastic Kubernetes Service: per generare metriche da analizzare da DevOps Guru, segui i passaggi in Configurazione di informazioni sui container su Amazon EKS e Kubernetes. DevOpsGuru non analizza alcuna risorsa di Amazon EKS finché non viene impostata la generazione di queste metriche. Questa operazione potrebbe comportare costi da AmazonCloudWatch.
- Amazon Simple Storage Service: per generare metriche che DevOps Guru possa analizzare, devi abilitare le metriche delle richieste. Segui i passaggi indicati in Creazione di una configurazione CloudWatch metrica per tutti gli oggetti nel tuo bucket. DevOpsGuru non analizza alcuna risorsa Amazon S3 finché non viene impostata la generazione di queste metriche. Questa operazione potrebbe comportare costi aggiuntivi CloudWatch per Amazon S3.

Per ulteriori informazioni, consulta i CloudWatchprezzi di Amazon.

Lavorare con approfondimenti inDevOpsGuru

AmazonDevOpsGuru genera unintuizionequando rileva un comportamento anomalo nelle applicazioni operative. DevOpsGuru analizza le metriche, gli eventi e altro ancora nelAWSrisorse che hai specificato al momento della configurazioneDevOpsGuru. Ogni approfondimento contiene uno o più consigli da seguire per mitigare il problema. Contiene anche un elenco delle metriche, un elenco di gruppi di log e un elenco degli eventi utilizzati per identificare il comportamento insolito.

Esistono due tipi di informazioni.

- ReattivoInsights contiene consigli che puoi seguire per risolvere i problemi che si verificano ora.
- Proattivole informazioni hanno consigli che risolvono problemi cheDevOpsGuru prevede che accadrà in futuro.

Argomenti

VisualizzazioneDevOpsGuru Insights

Puoi visualizzare i tuoi approfondimenti utilizzandoAWS Management Console.

Visualizza il tuoDevOpsGuru Insights

1. Apri AmazonDevOpsConsolle Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. Apri il pannello di navigazione, quindi scegliapprofondimenti.
3. SulReattivoscheda, puoi visualizzare un elenco di approfondimenti reattivi. SulProattivoscheda, puoi visualizzare un elenco di approfondimenti proattivi.
4. (Facoltativo) Utilizza uno o più dei seguenti filtri per trovare le informazioni che stai cercando.
    - Scegli laReattivooProattivoscheda, a seconda del tipo di approfondimento che stai cercando.
    - ScegliFiltrare le informazioni, quindi scegli un'opzione per specificare un filtro. Puoi aggiungere una combinazione di filtri di stato, gravità, risorse e tag. Usa unAWSfiltro tag per visualizzare

le informazioni generate solo da risorse con tag specifici. Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.

> **Note**
>
> DevOpsGuru può analizzare le seguenti risorse, ma non può filtrare le loro informazioni utilizzando i tag.
>
> - Percorsi e percorsi di Amazon API Gateway
> - Flussi Amazon DynamoDB
> - Istanze di gruppo Amazon EC2 Auto Scaling
> - Ambienti AWS Elastic Beanstalk
> - Nodi Amazon Redshift

- Scegli o specifica un intervallo di tempo da filtrare in base al tempo di creazione delle informazioni.
  - 12hmostra gli approfondimenti creati nelle ultime 12 ore.
  - 1dmostra gli approfondimenti creati nell'ultimo giorno.
  - 1wmostra gli approfondimenti creati nell'ultima settimana.
  - 1 mmostra gli approfondimenti creati nell'ultimo mese.
  - Personalizzatoconsente di specificare un altro intervallo di tempo. L'intervallo di tempo massimo che puoi utilizzare per filtrare le informazioni è di 180 giorni.

5. Per visualizzare i dettagli di un'analisi, scegli il nome.

Comprendere gli approfondimenti inDevOpsConsolle Guru

Usa AmazonDevOpsConsole Guru per visualizzare informazioni utili nei tuoi approfondimenti per aiutarti a diagnosticare e risolvere comportamenti anomali. QuandoDevOpsGuru analizza le tue risorse e trova Amazon correlateCloudWatchmetriche,AWS CloudTraileventi e dati operativi che indicano un comportamento insolito, crea un'analisi che contiene consigli per affrontare il problema e informazioni sulle metriche e sugli eventi correlati. Usa i dati di analisi conBest practice in DevOps Guruper risolvere i problemi operativi rilevati daDevOpsGuru.

Per visualizzare un'analisi, segui i passaggi inVisualizzazione degli approfondimentiper trovarne uno, quindi scegli il nome. La pagina di approfondimento contiene i seguenti dettagli.

Panoramica di Insight

Usa questa sezione per ottenere una panoramica di alto livello delle informazioni. Puoi vedere lo stato dell'analisi (In corsooChiuso), quantiAWS CloudFormationgli stack sono interessati, quando l'analisi è iniziata, terminata e è stata aggiornata l'ultima volta, e l'elemento delle operazioni correlate, se presente.

Se un'analisi è raggruppata inlivello di pila, quindi puoi scegliere il numero di pile interessate per vederne i nomi. Il comportamento anomalo che ha creato le informazioni si è verificato nelle risorse create dagli stack interessati. Se un'analisi è raggruppata inlivello dell'account, quindi il numero è zero o non viene visualizzato.

Per ulteriori informazioni, consulta Comprendere come i comportamenti anomali sono raggruppati in approfondimenti.

Nome dell'informazione dettagliata

Il nome di un'analisi dipende dal fatto che sia o meno raggruppata inlivello di pilao illivello dell'account.

- Livello di pilai nomi di insight includono il nome dello stack che contiene la risorsa con il suo comportamento anomalo.
- Livello dell'accounti nomi insight non includono il nome dello stack.

Per ulteriori informazioni, consulta Comprendere come i comportamenti anomali sono raggruppati in approfondimenti.

Metriche aggregate

Scegli laMetriche aggregatescheda per visualizzare le metriche correlate all'analisi. Nella tabella, ogni riga rappresenta una metrica. Puoi vedere qualiAWS CloudFormationstack ha creato la risorsa che ha emesso la metrica, il nome della risorsa e il suo tipo. Non tutte le metriche sono associate aAWS CloudFormationimpilare o avere un nome.

Quando sono presenti più risorse anomale contemporaneamente, la visualizzazione della cronologia aggrega le risorse e presenta le relative metriche anomale in un'unica sequenza temporale per una facile analisi. Le linee rosse su una linea temporale indicano gli intervalli di tempo in cui una metrica ha emesso valori insoliti. Per ingrandire, usa il mouse per scegliere un

intervallo di tempo specifico. Puoi anche usare le icone della lente d'ingrandimento per ingrandire e rimpicciolire.

Scegli una linea rossa nella timeline per visualizzare informazioni dettagliate. Nella finestra che si apre, puoi:

- ScegliVisualizza inCloudWatchper vedere come appare la metrica nelCloudWatchconsolle. Per ulteriori informazioni, vedereStatistiche eDimensioninelAmazonCloudWatchGuida per l'utente.
- Passa il mouse sul grafico per visualizzare i dettagli sui dati metrici anomali e su quando si sono verificati.
- Scegli la casella con la freccia rivolta verso il basso per scaricare un'immagine PNG del grafico.

Anomalie grafizzate

Scegli laAnomalie grafizzatescheda per visualizzare grafici dettagliati per ciascuna delle anomalie dell'analisi. Viene visualizzato un riquadro per ogni anomalia con i dettagli sul comportamento insolito rilevato nelle metriche correlate. È possibile indagare ed esaminare un'anomalia a livello di risorsa e per statistica. I grafici sono raggruppati per nome della metrica. In ogni riquadro, puoi scegliere un intervallo di tempo specifico nella timeline per ingrandire. Puoi anche usare le icone della lente d'ingrandimento per ingrandire e rimpicciolire o scegliere una durata predefinita in ore, giorni o settimane (1H,3H,12H,1D,3D,1W, oppure2W).

ScegliVisualizza tutte le statistiche e le dimensioniper vedere i dettagli sull'anomalia. Nella finestra che si apre, puoi:

- ScegliVisualizza inCloudWatchper vedere come appare la metrica nelCloudWatchconsolle.
- Passa il mouse sul grafico per visualizzare i dettagli sui dati metrici anomali e su quando si sono verificati.
- ScegliStatisticheoDimensioneper personalizzare la visualizzazione del grafico. Per ulteriori informazioni, vedereStatistiche eDimensioninelAmazonCloudWatchGuida per l'utente.

Gruppi di log

Quando abiliti il rilevamento delle anomalie dei registri,DevOpsGuru tagga il tuoCloudWatchgruppi di log in modo da poter visualizzare i gruppi di log relativi alle tue informazioni. NelGruppi di logsezione nella pagina dei dettagli di insight, ogni riga della tabella rappresenta un gruppo di log ed elenca la risorsa correlata.

Quando sono presenti più gruppi di log anomali contemporaneamente, la vista della cronologia li aggrega e li presenta in un'unica sequenza temporale per una facile analisi. Le linee viola su una

linea temporale indicano gli intervalli di tempo in cui un gruppo di log ha registrato anomalie nei log.

Scegliete una riga viola nella timeline per visualizzare un esempio di informazioni sulle anomalie dei log, come eccezioni di parole chiave e deviazioni numeriche. ScegliVisualizza i dettagli dei gruppi di logper visualizzare le anomalie dei log. Nella finestra che si apre, puoi:

- Visualizza un grafico delle anomalie dei log e degli eventi rilevanti.
- Passa il mouse sul grafico per visualizzare i dettagli sui dati di registro anomali e su quando si sono verificati.
- Visualizza le anomalie del registro in dettaglio con messaggi di esempio, frequenza delle occorrenze, raccomandazioni correlate e ora in cui si sono verificate.
- Clicca suVisualizza i dettagli inCloudWatchper visualizzare le righe di registro da un'anomalia del registro.

Eventi correlati

NelEventi correlati, vistaAWS CloudTraileventi correlati alla tua intuizione. Usa questi eventi per comprendere, diagnosticare e affrontare la causa alla base del comportamento anomalo.

Raccomandazioni

Nelraccomandazioni, puoi visualizzare suggerimenti che potrebbero aiutarti a risolvere il problema sottostante. QuandoDevOpsGuru rileva un comportamento anomalo, tenta di creare raccomandazioni. Un'analisi può contenere uno, più o zero consigli.

Comprendere come i comportamenti anomali sono raggruppati in approfondimenti

Un approfondimento è raggruppato inlivello di pilao illivello dell'account. Se viene generata un'analisi per una risorsa che si trova in unAWS CloudFormationpila, allora è unlivello di pilaintuizione. Altrimenti, è unlivello dell'accountintuizione.

Il modo in cui uno stack viene raggruppato può dipendere da come hai configurato la copertura dell'analisi delle risorse in Amazon.DevOpsGuru.

Se la copertura è definita daAWS CloudFormationpile

Tutte le risorse contenute negli stack scelti vengono analizzate e tutte le informazioni rilevate vengono raggruppate inlivello di pila.

Se la tua copertura è la tua attualeAWSaccount e regione

Tutte le risorse del tuo account e della tua regione vengono analizzate e sono disponibili tre possibili scenari di raggruppamento per le informazioni rilevate.

- Un'analisi generata da una risorsa che non fa parte di uno stack è raggruppata inlivello dell'account.
- Un'analisi generata da una risorsa che si trova in uno dei primi 10.000 stack analizzati è raggruppata inlivello di pila.
- Un'analisi generata da una risorsa che non è presente in uno dei primi 10.000 stack analizzati è raggruppata inlivello dell'account. Ad esempio, un'analisi generata per una risorsa nel 10.001° stack analizzato è raggruppata inlivello dell'account.

Per ulteriori informazioni, consulta Determina la copertura per DevOps Guru.

Comprendere la gravità delle informazioni

Un'intuizione può avere una delle tre gravità,alto,medio, oppurebasso. Amazon crea un'intuizioneDevOpsGuru dopo aver rilevato le anomalie correlate e assegnato a ciascuna anomalia una gravità. DevOpsGuru assegna a un'anomalia una gravità dialto,medio, oppurebassoutilizzando la conoscenza del dominio e anni di esperienza collettiva. La gravità di un'intuizione è determinata dall'anomalia più grave che ha contribuito a creare l'intuizione.

- Se la gravità di tutte le anomalie che hanno generato l'analisi èbasso, quindi la gravità dell'intuizione èbasso.
- Se la massima gravità di tutte le anomalie che hanno generato l'analisi èmedio, quindi la gravità dell'intuizione èmedio. La gravità di alcune delle anomalie che hanno generato le informazioni potrebbe esserebasso.
- Se la massima gravità di tutte le anomalie che hanno generato l'analisi èalto, quindi la gravità dell'intuizione èalto. La gravità di alcune delle anomalie che hanno generato le informazioni potrebbe esserebassoomedio.

Monitoraggio dei database tramite DevOps Guru

DevOpsGuru offre un valore significativo per il funzionamento dei database su. AWS Sfruttando i suoi algoritmi di apprendimento automatico, DevOps Guru può aiutare a ottimizzare le prestazioni del database, migliorare l'affidabilità e ridurre il sovraccarico operativo. Questa sezione della guida per l'utente fornisce una panoramica di alto livello di queste funzionalità del database, inclusi casi d'uso specifici di DevOps Guru per diversi servizi di database. AWS

DevOpsGuru può fornire approfondimenti per database relazionali come Amazon RDS e. Amazon Redshift Può anche fornire approfondimenti per database non relazionali o NoSQL come e. Amazon DynamoDB Amazon ElastiCache

Argomenti

Monitoraggio dei database relazionali tramite Guru DevOps

DevOpsGuru attinge da due fonti di dati principali per cercare approfondimenti e anomalie nei database relazionali. Per Amazon RDS e Amazon Redshift, le metriche CloudWatch vendute vengono analizzate per tutti i tipi di istanze. Per Amazon RDS, i dati di Performance Insights vengono acquisiti anche per i seguenti tipi di motore: RDS per PostgreSQL, Aurora PostgreSQL e Aurora MySQL.

Monitoraggio delle operazioni del database in Amazon RDS

Questa sezione include informazioni specifiche sui casi d'uso e sulle metriche monitorate in DevOps Guru for RDS, inclusi i dati provenienti da CloudWatch vended metrics e Performance Insights. Per ulteriori informazioni su DevOps Guru for RDS, inclusi concetti chiave, configurazioni e vantaggi, vedi. the section called “Lavorare con le anomalie in Guru for RDS DevOps”

Monitoraggio di RDS utilizzando i dati delle metriche vendute CloudWatch

DevOpsGuru è in grado di monitorare ogni tipo di istanza RDS acquisendo CloudWatch metriche predefinite, come l'utilizzo della CPU e la latenza delle operazioni di lettura e scrittura. Poiché queste metriche vengono fornite di default, quando si monitorano le istanze RDS con DevOps Guru, non

sono necessarie ulteriori configurazioni per ottenere informazioni dettagliate. DevOpsGuru stabilisce automaticamente una linea di base per queste metriche sulla base di modelli storici e le confronta con i dati in tempo reale per rilevare anomalie e potenziali problemi nel database.

La tabella seguente mostra un elenco di potenziali approfondimenti reattivi per Amazon RDS da CloudWatch vended metrics.

AWS risorsa monitorata da Guru DevOps	Scenario identificato da DevOps Guru	CloudWatch metriche monitorate
Amazon RDS (tutti i tipi di istanze)	Raggiungimento dei limiti della CPU o della memoria	dbLoad, dbLoadCPU
RDS per PostgreSQL.	Elevato ritardo dello slot di replica	OldestReplicationSlotLag

CloudWatch Parametri forniti aggiuntivi dalle istanze Amazon RDS monitorate da Guru: DevOps

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- SQL non riuscito ServerAgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

Monitoraggio di RDS utilizzando i dati di Performance Insights

Per alcuni tipi di istanze Amazon RDS, come Aurora PostgreSQL, Aurora MySQL e RDS for PostgreSQL, sblocchi più funzionalità dal monitoraggio Guru assicurandoti che Performance Insights sia abilitato su tali istanze. DevOps

DevOpsGuru fornisce informazioni reattive per una varietà di situazioni, inclusi i seguenti scenari:

Scenario che DevOps Guru identifica per generare una visione reattiva
Problema di blocco della contesa
Indice mancante
Configurazione errata del pool di applicazioni
Impostazioni predefinite JDBC non ottimali

DevOpsGuru fornisce informazioni proattive per una varietà di situazioni, inclusi i seguenti scenari:

AWS risorsa monitorata da Guru DevOps	Scenario che DevOps Guru identifica per generare una visione proattiva
Aurora MySQL	L'elenco della cronologia di InnoDB diventa troppo grande, il che può portare a un peggioramento delle prestazioni, ad esempio lunghi tempi di chiusura del database
Aurora MySQL	Un aumento delle tabelle temporanee create su disco che può influire sulle prestazioni del database
RDS per PostgreSQL, Aurora PostgreSQL	Connessione rimasta inattiva durante una transazione troppo a lungo, impatto potenzial e derivante dal mantenimento dei blocchi, dal blocco di altre query e dall'impossibilità per il vuoto (incluso l'autovacuum) di eliminare le righe non funzionanti

Monitoraggio delle operazioni del database in Amazon Redshift

DevOpsGuru è in grado di monitorare le Amazon Redshift risorse acquisendo CloudWatch metriche predefinite, tra cui l'utilizzo della CPU e la percentuale di spazio su disco utilizzata. Poiché queste metriche vengono fornite di default, non sono necessarie ulteriori configurazioni per DevOps consentire a Guru di monitorare automaticamente le risorse. Amazon Redshift DevOpsGuru stabilisce

una linea di base per queste metriche sulla base di modelli storici e le confronta con dati in tempo reale per rilevare anomalie.

DevOpsScenario identificato da Guru	CloudWatch metriche monitorate
Rileva l'elevato utilizzo della CPU di un' Amazon Redshift istanza causato da fattori quali carico di lavoro del cluster, dati distorti e non ordinati o attività del nodo principale	CPUUtilization
Rileva quando un' Amazon Redshift istanza sta esaurendo lo spazio su disco a causa di problemi relativi all'elaborazione delle query, alla distribuzione e alla chiave di ordinamen to, alle operazioni di manutenzione o ai blocchi tombstone	PercentageDiskSpaceUsed

Metriche CloudWatch fornite aggiuntive dalle Amazon Redshift istanze monitorate da Guru: DevOps

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLM QueueLength
- WLM QueueWaitTime
- WLM QueryDuration
- WriteLatency

Lavorare con le anomalie in DevOps Guru for RDS

DevOpsGuru rileva, analizza e fornisce consigli per le AWS risorse supportate, inclusi i motori Amazon RDS. Per le istanze di database Amazon Aurora e RDS for PostgreSQL con Performance Insights attivato DevOps, Guru for RDS fornisce analisi dettagliate e specifiche del database dei problemi di prestazioni e consiglia azioni correttive.

Argomenti

Panoramica di Guru for RDS DevOps

Di seguito è riportato un riepilogo dei vantaggi e delle funzionalità principali di DevOps Guru for RDS. Per informazioni di base su approfondimenti e anomalie, vedi. DevOpsConcetti del guru

Argomenti

Vantaggi di DevOps Guru for RDS

Se sei responsabile di un database Amazon RDS, potresti non sapere che si sta verificando un evento o una regressione che sta interessando quel database. Quando scopri il problema, potresti non sapere perché si sta verificando o cosa fare al riguardo. Invece di rivolgerti a un amministratore di database (DBA) per ricevere assistenza o affidarti a strumenti di terze parti, puoi seguire i consigli di Guru for RDS. DevOps

L'analisi dettagliata di Guru for RDS consente di DevOps ottenere i seguenti vantaggi:

Diagnosi rapida

DevOpsGuru for RDS monitora e analizza continuamente la telemetria del database. Performance Insights, Enhanced Monitoring e Amazon CloudWatch raccolgono dati di telemetria per le tue istanze di database. DevOpsGuru for RDS utilizza tecniche statistiche e di apprendimento automatico per estrarre questi dati e rilevare anomalie. Per ulteriori informazioni sui dati di telemetria per i database Amazon Aurora, consulta Monitoraggio del carico del DB con Performance Insights su Amazon Aurora e Monitoraggio del sistema operativo utilizzando Enhanced Monitoring nella Guida per l'utente di Amazon Aurora. Per ulteriori informazioni sui dati di telemetria per altri database Amazon RDS, consulta Monitoring DB load with Performance Insights on Amazon Relational Database Service e Monitoring OS metrics with Enhanced Monitoring nella Amazon RDS User Guide.

Risoluzione rapida

Ogni anomalia identifica il problema delle prestazioni e suggerisce strade di indagine o azioni correttive. Ad esempio, DevOps Guru for RDS potrebbe consigliarti di esaminare specifici eventi di attesa. In alternativa, è consigliabile regolare le impostazioni del pool di applicazioni per limitare il numero di connessioni al database. Sulla base di questi consigli, è possibile risolvere i problemi di prestazioni più rapidamente rispetto alla risoluzione manuale dei problemi.

Approfondimenti proattivi

DevOpsGuru for RDS utilizza le metriche delle tue risorse per rilevare comportamenti potenzialmente problematici prima che diventino un problema più grave. Ad esempio, è in grado di rilevare quando le sessioni connesse al database non svolgono attività attive e potrebbe mantenere bloccate le risorse del database. DevOpsGuru fornisce quindi consigli per aiutarvi a risolvere i problemi prima che diventino problemi più gravi.

Conoscenza approfondita dei tecnici e del machine learning di Amazon

Per rilevare problemi di prestazioni e aiutarti a risolvere i problemi, DevOps Guru for RDS si affida all'apprendimento automatico (ML) e all'analisi statistica avanzata. Gli ingegneri di database di Amazon hanno contribuito allo sviluppo dei risultati di DevOps Guru for RDS, che racchiudono molti anni di gestione di centinaia di migliaia di database. Attingendo a questa conoscenza collettiva, DevOps Guru for RDS può insegnarti le migliori pratiche.

Concetti chiave per l'ottimizzazione delle prestazioni del database

DevOpsGuru for RDS presuppone che tu abbia familiarità con alcuni concetti chiave relativi alle prestazioni. Per ulteriori informazioni su questi concetti, consulta Overview of Performance Insights

nella Amazon Aurora User Guide o Overview of Performance Insights nella Amazon RDS User Guide.

Argomenti

- Metriche
- Rilevamento dei problemi
- Carico DB
- Eventi di attesa

Metriche

Un parametro rappresenta un set di punti dati in ordine cronologico. Pensa a un parametro come a una variabile da monitorare e ai punti di dati come i valori di questa variabile nel tempo. Amazon RDS fornisce parametri in tempo reale per il database e per il sistema operativo (OS) su cui viene eseguita l'istanza DB. Puoi visualizzare tutte le metriche di sistema e le informazioni di processo per le tue istanze database Amazon RDS sulla console Amazon RDS. DevOpsGuru for RDS monitora e fornisce approfondimenti per alcune di queste metriche. Per ulteriori informazioni, consulta i parametri di monitoraggio in un cluster Amazon Aurora o i parametri di monitoraggio in un'istanza di Amazon Relational Database Service.

Rilevamento dei problemi

DevOpsGuru for RDS utilizza le metriche del database e del sistema operativo (OS) per rilevare i problemi critici relativi alle prestazioni del database, siano essi imminenti o continui. Esistono due modi principali in cui funziona il rilevamento dei problemi di DevOps Guru for RDS:

- Utilizzo delle soglie
- Utilizzo di anomalie

Rilevamento di problemi con le soglie

Le soglie sono i valori limite rispetto ai quali vengono valutate le metriche monitorate. Puoi pensare a una soglia come a una linea orizzontale su un grafico metrico che separa il comportamento normale da quello potenzialmente problematico. DevOpsGuru for RDS monitora metriche specifiche e crea soglie analizzando quali livelli sono considerati potenzialmente problematici per una risorsa specifica. DevOpsGuru for RDS crea quindi approfondimenti nella console DevOps Guru quando i nuovi valori

delle metriche superano una soglia specificata in un determinato periodo di tempo in modo coerente. Gli approfondimenti contengono consigli per prevenire futuri impatti sulle prestazioni del database.

Ad esempio, DevOps Guru for RDS potrebbe monitorare il numero di tabelle temporanee che utilizzano il disco per un periodo di 15 minuti e creare informazioni quando la frequenza delle tabelle temporanee che utilizzano il disco al secondo è anormalmente elevata. L'aumento dei livelli di utilizzo delle tabelle temporanee su disco potrebbe influire sulle prestazioni del database. Esponendo questa situazione prima che diventi critica, DevOps Guru for RDS ti aiuta a intraprendere azioni correttive per prevenire i problemi.

Rilevamento di problemi con anomalie

Sebbene le soglie offrano un modo semplice ed efficace per rilevare i problemi del database, in alcune situazioni non sono sufficienti. Prendiamo in considerazione il caso in cui i valori delle metriche aumentino e si trasformino regolarmente in comportamenti potenzialmente problematici a causa di un processo noto, ad esempio un processo quotidiano di creazione di report. Poiché tali picchi sono prevedibili, la creazione di informazioni e notifiche per ciascuno di essi sarebbe controproducente e probabilmente causerebbe un affaticamento degli avvisi.

Tuttavia, è comunque necessario rilevare picchi molto insoliti, poiché metriche molto più elevate rispetto alle altre o che durano molto più a lungo potrebbero rappresentare problemi reali di prestazioni del database. Per risolvere questo problema, DevOps Guru for RDS monitora determinate metriche per rilevare quando il comportamento di una metrica diventa molto insolito o anomalo. DevOpsGuru riporta quindi queste anomalie negli approfondimenti.

Ad esempio, DevOps Guru for RDS potrebbe creare informazioni quando il carico del DB non solo è elevato, ma si discosta anche in modo significativo dal suo comportamento abituale, il che indica un grave rallentamento imprevisto delle operazioni del database. Riconoscendo solo i picchi anomali di carico del DB, DevOps Guru for RDS consente di concentrarsi sui problemi veramente importanti.

Carico DB

Il concetto chiave per l'ottimizzazione del database è la metrica del caricamento del database (carico DB). Il carico del DB rappresenta il livello di occupazione del database in un dato momento. Un aumento del carico del DB significa un aumento dell'attività del database.

Una sessione database rappresenta il dialogo di un'applicazione con un database relazionale. Una sessione attiva è una sessione che sta eseguendo una richiesta al database. Una sessione è attiva quando è in esecuzione sulla CPU o in attesa che una risorsa diventi disponibile in modo che possa

proseguire. Ad esempio, una sessione attiva potrebbe attendere la lettura di una pagina in memoria e quindi consumare la CPU mentre legge i dati dalla pagina.

La `DBLoad` metrica in Performance Insights viene misurata in sessioni attive medie (AAS). Per calcolare l'AAS, Performance Insights campiona il numero di sessioni attive ogni secondo. Per un periodo di tempo specifico, l'AAS è il numero totale di sessioni attive diviso per il numero totale di campioni. Un valore AAS pari a 2 indica che, in media, erano attive 2 sessioni nelle richieste in un dato momento.

Un'analogia per il carico DB è l'attività in un magazzino. Supponiamo che il magazzino impieghi 100 lavoratori. Se arriva 1 ordine, 1 lavoratore evade l'ordine mentre gli altri lavoratori sono inattivi. Se arrivano 100 o più ordini, tutti i 100 lavoratori eseguono gli ordini contemporaneamente. Se si periodicamente si esegue un campionamento di quanti lavoratori sono attivi in un determinato periodo di tempo, è possibile calcolare il numero medio di lavoratori attivi. Il calcolo dimostra che, in media,N lavoratori sono impegnati a gestire gli ordini in un dato momento. Se la media era di 50 lavoratori ieri e 75 lavoratori oggi, il livello di attività nel magazzino è aumentato. Allo stesso modo, il carico DB aumenta con l'aumentare dell'attività di sessione.

Per ulteriori informazioni, consulta Caricamento del database nella Guida per l'utente di Amazon Aurora o Caricamento del database nella Guida per l'utente di Amazon RDS.

Eventi di attesa

Un evento di attesa è un tipo di strumentazione del database che indica quale risorsa è in attesa una sessione di database in modo che possa procedere. Quando Performance Insights conta le sessioni attive per calcolare il carico del database, registra anche gli eventi di attesa che causano l'attesa delle sessioni attive. Questa tecnica consente a Performance Insights di mostrare quali eventi di attesa contribuiscono al carico del DB.

Ogni sessione attiva è in esecuzione sulla CPU o in attesa. Ad esempio, le sessioni consumano CPU quando effettuano ricerche nella memoria, eseguono calcoli o eseguono codice procedurale. Quando le sessioni non consumano CPU, potrebbero essere in attesa della lettura di un file di dati o della scrittura di un registro. Maggiore è il tempo in cui una sessione attende le risorse, minore è il tempo in cui viene eseguita sulla CPU.

Quando si ottimizza un database, si cerca spesso di trovare le risorse che le sessioni attendono. Ad esempio, due o tre eventi di attesa potrebbero rappresentare il 90% del carico del DB. Questa misura significa che, in media, le sessioni attive trascorrono la maggior parte del tempo in attesa di un numero limitato di risorse. Se riesci a scoprire la causa di queste attese, puoi provare a risolvere il problema.

Considera l'analogia di un addetto al magazzino. Viene fornito un ordine per un libro. Il lavoratore potrebbe subire un ritardo nell'evasione dell'ordine. Ad esempio, un altro lavoratore potrebbe attualmente rifornire gli scaffali o un carrello potrebbe non essere disponibile. Oppure il sistema utilizzato per inserire lo stato dell'ordine potrebbe essere lento. Più a lungo il lavoratore aspetta, più tempo impiega l'evasione dell'ordine. L'attesa è una parte naturale del flusso di lavoro del magazzino, ma se i tempi di attesa diventano eccessivi, la produttività diminuisce. Allo stesso modo, attese di sessione ripetute o lunghe possono compromettere le prestazioni del database.

Per ulteriori informazioni sugli eventi di attesa in Amazon Aurora, consulta Tuning with wait events for Aurora PostgreSQL e Tuning with wait events for Aurora MySQL nella Amazon Aurora User Guide.

Per ulteriori informazioni sugli eventi di attesa in altri database Amazon RDS, consulta Tuning with wait events for RDS for PostgreSQL nella Amazon RDS User Guide.

DevOpsConcetti chiave per Guru for RDS

DevOpsGuru genera un'intuizione quando rileva un comportamento anomalo o problematico nelle applicazioni operative. Un'analisi contiene anomalie per una o più risorse. Un'anomalia rappresenta una o più metriche correlate rilevate da DevOps Guru che sono inaspettate o insolite.

Un'intuizione ha una gravità alta, media o bassa. La gravità dell'analisi è determinata dall'anomalia più grave che ha contribuito alla creazione dell'analisi. Ad esempio, se l'analisi AWS-ECS_ MemoryUtilization _and_others include un'anomalia con bassa gravità e un'altra con gravità elevata, la gravità complessiva dell'analisi è elevata.

Se le istanze DB di Amazon RDS hanno Performance Insights attivato, DevOps Guru for RDS fornisce analisi dettagliate e consigli sulle anomalie per queste istanze. Per identificare un'anomalia, DevOps Guru for RDS sviluppa una linea di base per i valori delle metriche del database. DevOpsGuru for RDS confronta quindi i valori metrici correnti con la linea di base storica.

Argomenti

- Approfondimenti proattivi
- Approfondimenti reattivi
- Raccomandazioni

Approfondimenti proattivi

Un approfondimento proattivo consente di individuare i comportamenti problematici prima che si verifichino. Contiene anomalie con consigli e metriche correlate per aiutarti a risolvere i problemi prima che diventino problemi più gravi.

Ogni pagina di analisi proattiva fornisce dettagli su un'anomalia.

Approfondimenti reattivi

Un approfondimento reattivo identifica un comportamento anomalo nel momento in cui si verifica. Contiene anomalie con consigli, metriche correlate ed eventi per aiutarti a comprendere e risolvere subito i problemi.

Anomalie causali

Un'anomalia causale è un'anomalia di livello superiore all'interno di un approfondimento reattivo. Viene mostrata come metrica principale nella pagina dei dettagli dell'anomalia nella console Guru. DevOps Il caricamento del database (caricamento del DB) è l'anomalia causale di Guru for RDS. DevOps Ad esempio, l'analisi AWS-ECS_ MemoryUtilization _and_others potrebbe presentare diverse anomalie metriche, una delle quali è il caricamento del database (carico DB) per la risorsa AWS/RDS.

In un'analisi approfondita, può verificarsi l'anomalia del carico del database (carico DB) per più istanze database di Amazon RDS. La gravità dell'anomalia potrebbe essere diversa per ogni istanza DB. Ad esempio, la gravità per un'istanza DB potrebbe essere elevata mentre la gravità per le altre è bassa. Per impostazione predefinita, la console utilizza l'anomalia con la gravità più elevata.

Anomalie contestuali

Un'anomalia contestuale è un risultato del carico del database correlato a un approfondimento reattivo. Viene visualizzata nella sezione Metriche correlate della pagina dei dettagli dell'anomalia nella console Guru. DevOps Ogni anomalia contestuale descrive uno specifico problema di prestazioni di Amazon RDS che richiede un'analisi. Ad esempio, un'anomalia causale può includere le seguenti anomalie contestuali:

- Capacità della CPU superata: la coda di esecuzione della CPU o l'utilizzo della CPU sono superiori al normale.
- Memoria del database insufficiente: i processi non dispongono di memoria sufficiente.

- Connessioni al database con picchi: il numero di connessioni al database è superiore al normale.

Raccomandazioni

Ogni intuizione ha almeno un'azione suggerita. I seguenti esempi sono consigli generati da DevOps Guru per RDS:

- Ottimizza gli ID SQL *List_of_IDS* per ridurre l'utilizzo della CPU o aggiorna il tipo di istanza per aumentare la capacità della CPU.
- Esamina il picco associato delle connessioni correnti al database. Valuta la possibilità di ottimizzare le impostazioni del pool di applicazioni per evitare l'allocazione dinamica frequente di nuove connessioni al database.
- Cerca istruzioni SQL che eseguono operazioni di memoria eccessive, come l'ordinamento in memoria o i join di grandi dimensioni.
- *Esamina l'elevato utilizzo di I/O per i seguenti ID SQL: List_of_IDS.*
- Controlla le istruzioni che creano grandi quantità di dati temporanei, ad esempio quelle che eseguono ordinamenti di grandi dimensioni o utilizzano tabelle temporanee di grandi dimensioni.
- Controlla le applicazioni per vedere cosa sta causando l'aumento del carico di lavoro del database.
- Valuta la possibilità di abilitare il MySQL Performance Schema.
- Verifica la presenza di transazioni di lunga durata e terminale con un commit o un rollback.
- Configura il parametro idle_in_transaction_session_timeout per terminare qualsiasi sessione rimasta nello stato 'idle in transaction' per un periodo più lungo del tempo specificato.

Come funziona Guru for RDS DevOps

DevOpsGuru for RDS raccoglie i dati metrici, li analizza e quindi pubblica le anomalie nella dashboard.

Argomenti

Raccolta e analisi dei dati

DevOpsGuru for RDS raccoglie dati sui tuoi database Amazon RDS da Amazon RDS Performance Insights. Questa funzionalità monitora le istanze DB di Amazon RDS, raccoglie i parametri e consente

di esplorarli in un grafico. La metrica prestazionale più importante è. `DBLoad` DevOpsGuru for RDS utilizza le metriche di Performance Insights e le analizza per rilevare anomalie. Per ulteriori informazioni su Performance Insights, consulta Monitoring DB load with Performance Insights on Amazon Aurora nella Amazon Aurora User Guide o Monitoring DB load with Performance Insights on Amazon RDS nella Amazon RDS User Guide.

DevOpsGuru for RDS utilizza l'apprendimento automatico e l'analisi statistica avanzata per analizzare i dati raccolti da Performance Insights. Se DevOps Guru for RDS rileva problemi di prestazioni, passa al passaggio successivo.

Pubblicazione di anomalie

Un problema di prestazioni del database, ad esempio un carico elevato del database, può compromettere la qualità del servizio del database. Quando DevOps Guru rileva un problema in un database RDS, pubblica una panoramica nella dashboard. L'analisi contiene un'anomalia per la risorsa AWS/RDS.

Se Performance Insights è attivato per le tue istanze, l'anomalia contiene un'analisi dettagliata del problema. DevOpsGuru for RDS consiglia inoltre di eseguire un'indagine o un'azione correttiva specifica. Ad esempio, il consiglio potrebbe essere quello di esaminare una specifica istruzione SQL ad alto carico, prendere in considerazione l'aumento della capacità della CPU o chiudere le sessioni. idle-in-transaction

Motori di database supportati

DevOpsGuru for RDS è supportato per i seguenti motori di database:

Amazon Aurora con compatibilità MySQL

Per ulteriori informazioni su questo motore, consulta Working with Amazon Aurora MySQL nella Amazon Aurora User Guide.

Compatibilità di Amazon Aurora con PostgreSQL

Per ulteriori informazioni su questo motore, consulta Working with Amazon Aurora PostgreSQL nella Amazon Aurora User Guide.

Compatibilità con Amazon RDS per PostgreSQL

Per ulteriori informazioni su questo motore, consulta Amazon RDS for PostgreSQLla Amazon RDS User Guide.

DevOpsGuru segnala le anomalie e fornisce analisi di base per altri motori di database. DevOpsGuru for RDS fornisce analisi dettagliate e consigli solo per le istanze Amazon Aurora e RDS per PostgreSQL.

DevOpsAbilitazione di Guru per RDS

Quando abiliti DevOps Guru for RDS, consenti a DevOps Guru di analizzare le anomalie nelle risorse come le istanze DB. Amazon RDS semplifica l'individuazione e l'attivazione delle funzionalità consigliate per un'istanza o un cluster DB RDS. A tal fine, RDS effettua chiamate API ad altri servizi, come Amazon EC2 DevOps, Guru e IAM. Quando la console RDS effettua queste chiamate API, le AWS CloudTrail registra per renderle visibili.

Per consentire a DevOps Guru di pubblicare approfondimenti per un database Amazon RDS, completa le attività nelle seguenti sezioni.

Argomenti

- Attivazione di Performance Insights per le istanze database Amazon RDS
- Configurazione delle politiche di accesso per Guru for DevOps RDS
- Aggiungere istanze Amazon RDS DB alla copertura Guru DevOps

Attivazione di Performance Insights per le istanze database Amazon RDS

DevOpsAffinché Guru for RDS analizzi le anomalie su un'istanza DB, assicurati che Performance Insights sia attivato. Se Performance Insights non è attivato per un'istanza DB, DevOps Guru for RDS ti invia una notifica nei seguenti luoghi:

Dashboard

Se si visualizzano gli approfondimenti per tipo di risorsa, il riquadro RDS avvisa che Performance Insights non è attivo. Scegli il link per attivare Performance Insights nella console Amazon RDS.

Informazioni dettagliate

Nella sezione Consigli in fondo alla pagina, scegli Abilita Amazon RDS Performance Insights.

Impostazioni

Nella sezione Servizio: Amazon RDS, scegli il link per attivare Performance Insights nella console Amazon RDS.

Per ulteriori informazioni, consulta Attivazione e disattivazione di Performance Insights nella Guida per l'utente di Amazon Aurora o Attivazione e disattivazione di Performance Insights nella Amazon RDS User Guide.

Configurazione delle politiche di accesso per Guru for DevOps RDS

Affinché un utente possa accedere a DevOps Guru for RDS, deve disporre delle autorizzazioni previste da una delle seguenti politiche:

- La policy di AWS gestita da `AmazonRDSFullAccess`.
- Una policy gestita dal cliente che consenta le seguenti operazioni.
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

Per ulteriori informazioni, consulta Configurazione delle politiche di accesso per Performance Insights nella Guida per l'utente di Amazon Aurora o Configurazione delle politiche di accesso per Performance Insights nella Guida per l'utente di Amazon RDS.

Aggiungere istanze Amazon RDS DB alla copertura Guru DevOps

Puoi configurare DevOps Guru per monitorare i tuoi database Amazon RDS nella console DevOps Guru o nella console Amazon RDS.

Nella console DevOps Guru, sono disponibili le seguenti opzioni:

- Attiva DevOps Guru a livello di account. Questa è l'impostazione predefinita. Quando scegli questa opzione, DevOps Guru analizza tutte le AWS risorse supportate nel tuo Regione AWS eAccount AWS, inclusi i database Amazon RDS.
- Specificate gli AWS CloudFormation stack per Guru for DevOps RDS.

  Per ulteriori informazioni, consulta Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru.
- Etichetta le tue risorse Amazon RDS.

  Un tag è un'etichetta di attributo personalizzata che assegni a una AWS risorsa. Utilizzate i tag per identificare le AWS risorse che compongono l'applicazione. Puoi quindi filtrare le tue informazioni per tag per visualizzare solo quelle create dalla tua applicazione. Per visualizzare solo

gli approfondimenti generati dalle risorse Amazon RDS nella tua applicazione, aggiungi un valore, ad esempio, `Devops-guru-rds` ai tag delle risorse Amazon RDS. Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.

> **Note**
>
> Quando tagghi le risorse Amazon RDS, devi etichettare l'istanza di database e non il cluster.

Per abilitare il monitoraggio DevOps Guru dalla console Amazon RDS, consulta Turning on DevOps Guru nella console RDS. Tieni presente che per abilitare DevOps Guru dalla console Amazon RDS devi utilizzare i tag. Per ulteriori informazioni sui tag, consulta the section called “Utilizzo dei tag per identificare le risorse nelle applicazioni”.

Analisi delle anomalie in Amazon RDS

Quando DevOps Guru for RDS pubblica un'anomalia delle prestazioni nella dashboard, in genere esegui i seguenti passaggi:

1. Visualizza le informazioni dettagliate nella dashboard di Guru. DevOps DevOpsGuru for RDS riporta informazioni sia reattive che proattive.

   Per ulteriori informazioni, consulta Visualizzazione degli approfondimenti.
2. Visualizza le anomalie per le risorse AWS/RDS.

   Per ulteriori informazioni, consultare Visualizzazione delle anomalie reattive e Visualizzazione delle anomalie proattive.
3. Rispondi ai consigli di Guru for DevOps RDS.

   Per ulteriori informazioni, consulta Risposta alle raccomandazioni .
4. Monitora lo stato delle tue istanze DB per assicurarti che i problemi di prestazioni risolti non si ripresentino.

   Per ulteriori informazioni, consulta i parametri di monitoraggio in un cluster Amazon Aurora DB nella Guida per l'utente di Amazon Aurora e i parametri di monitoraggio in un'istanza Amazon RDS nella Guida per l'utente di Amazon RDS.

Visualizzazione degli approfondimenti

Accedi alla pagina Insights nella console DevOps Guru per trovare approfondimenti reattivi e proattivi. Da lì, puoi scegliere un'analisi dall'elenco per visualizzare una pagina dettagliata di metriche, consigli e ulteriori informazioni sugli approfondimenti.

Per visualizzare un approfondimento

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Apri il pannello di navigazione, quindi scegli Insights.
3. Scegli la scheda Reattivo per visualizzare gli approfondimenti reattivi oppure scegli Proattivo per visualizzare gli approfondimenti proattivi.
4. Scegli il nome di un'analisi, assegnando la priorità in base allo stato e alla gravità.

   Viene visualizzata la pagina di approfondimento dettagliata.

Visualizzazione delle anomalie reattive

All'interno di una panoramica, puoi visualizzare le anomalie per le risorse Amazon RDS. In una pagina di analisi reattiva, nella sezione Metriche aggregate, puoi visualizzare un elenco di anomalie con le tempistiche corrispondenti. Sono inoltre presenti sezioni che visualizzano informazioni sui gruppi di log e sugli eventi correlati alle anomalie. Le anomalie causali in un'analisi reattiva hanno ciascuna una pagina corrispondente con i dettagli sull'anomalia.

Visualizzazione dell'analisi dettagliata di un'anomalia reattiva RDS

In questa fase, analizza l'anomalia per ottenere analisi dettagliate e consigli per le tue istanze database Amazon RDS.

L'analisi dettagliata è disponibile solo per le istanze DB di Amazon RDS con Performance Insights attivato.

Per visualizzare in dettaglio la pagina dei dettagli dell'anomalia

1. Nella pagina di approfondimento, trova una metrica aggregata con il tipo di risorsa AWS/RDS.
2. Seleziona Visualizza dettagli.

   Viene visualizzata la pagina dei dettagli dell'anomalia. Il titolo inizia con Anomalia delle prestazioni del database e nomina la risorsa mostrata. Per impostazione predefinita, la console

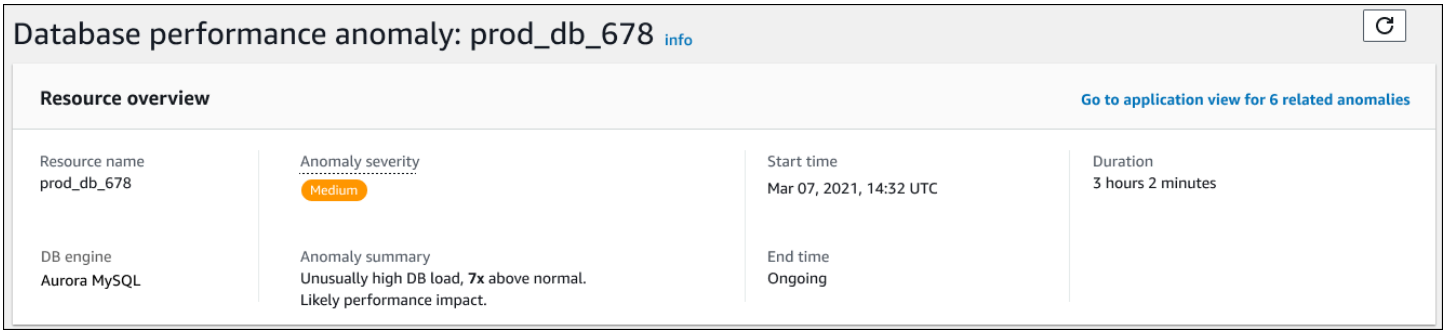
utilizza l'anomalia con la gravità più elevata, indipendentemente dal momento in cui si è verificata l'anomalia.

3. (Facoltativo) Se sono interessate più risorse, scegliete una risorsa diversa dall'elenco nella parte superiore della pagina.

Di seguito, puoi trovare le descrizioni dei componenti della pagina dei dettagli.

Panoramica delle risorse

La sezione superiore della pagina dei dettagli è Panoramica delle risorse. Questa sezione riassume l'anomalia delle prestazioni riscontrata dalla tua istanza database Amazon RDS.

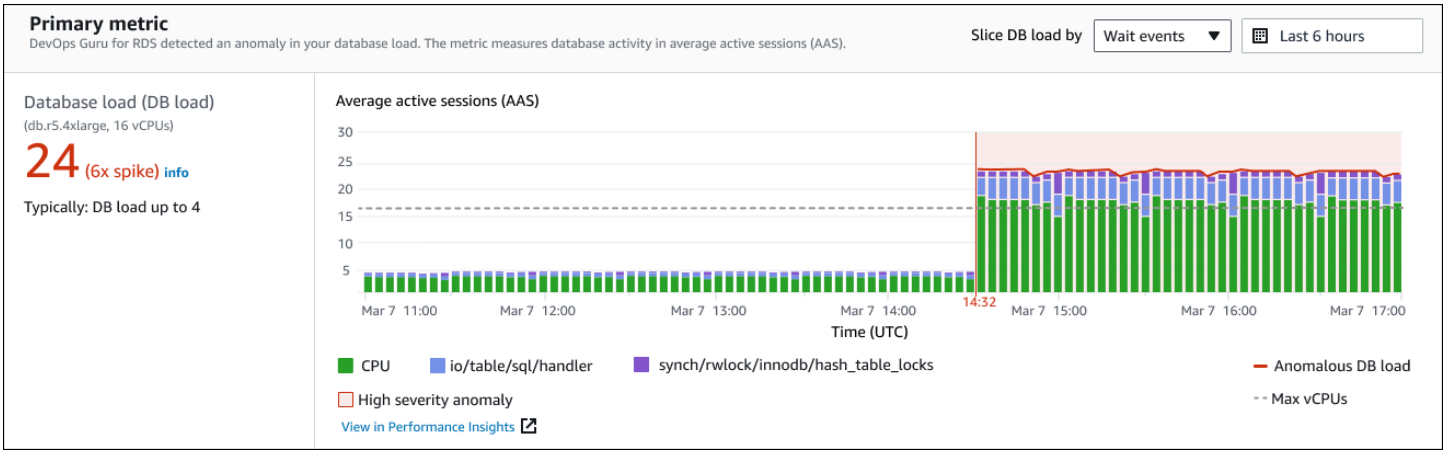


Questa sezione contiene i seguenti campi:

- Nome della risorsa: il nome dell'istanza DB che presenta l'anomalia. In questo esempio, la risorsa è denominata prod_db_678.
- Motore DB: il nome dell'istanza DB che presenta l'anomalia. In questo esempio, il motore è Aurora MySQL.
- Gravità dell'anomalia: la misura dell'impatto negativo dell'anomalia sull'istanza. I livelli di gravità possibili sono Alta, Media e Bassa.
- Riepilogo delle anomalie: breve riepilogo del problema. Un riepilogo tipico è il carico del DB insolitamente elevato.
- Ora di inizio e ora di fine: l'ora in cui l'anomalia è iniziata e terminata. Se l'ora di fine è in corso, l'anomalia si verifica ancora.
- Durata: la durata del comportamento anomalo. In questo esempio, l'anomalia è in corso e si verifica da 3 ore e 2 minuti.

Metrica principale

La sezione Metrica principale riassume l'anomalia casuale, che è l'anomalia di primo livello all'interno dell'analisi. Puoi pensare all'anomalia causale come al problema generale riscontrato dalla tua istanza DB.



Il pannello di sinistra fornisce ulteriori dettagli sul problema. In questo esempio, il riepilogo include le seguenti informazioni:

- Caricamento del database (caricamento del database): una categorizzazione dell'anomalia come problema di caricamento del database. La metrica corrispondente in Performance Insights è`DBLoad`. Questa metrica viene pubblicata anche su Amazon CloudWatch.
- db.r5.4xlarge — La classe dell'istanza DB. Il numero di vCPU, che in questo esempio è 16, corrisponde alla linea tratteggiata nel grafico delle sessioni attive medie (AAS).
- 24 (picco 6x): il carico del DB, misurato in sessioni attive medie (AAS) durante l'intervallo di tempo riportato nell'analisi. Pertanto, in qualsiasi momento durante il periodo dell'anomalia, sul database erano attive in media 24 sessioni. Il carico del DB è 6 volte il normale carico del DB per questa istanza.
- In genere: carico del DB fino a 4: la linea di base del carico del DB, misurata in AAS, durante un carico di lavoro tipico. Il valore 4 indica che, durante le normali operazioni, sul database sono attive in media 4 o meno sessioni in un dato momento.

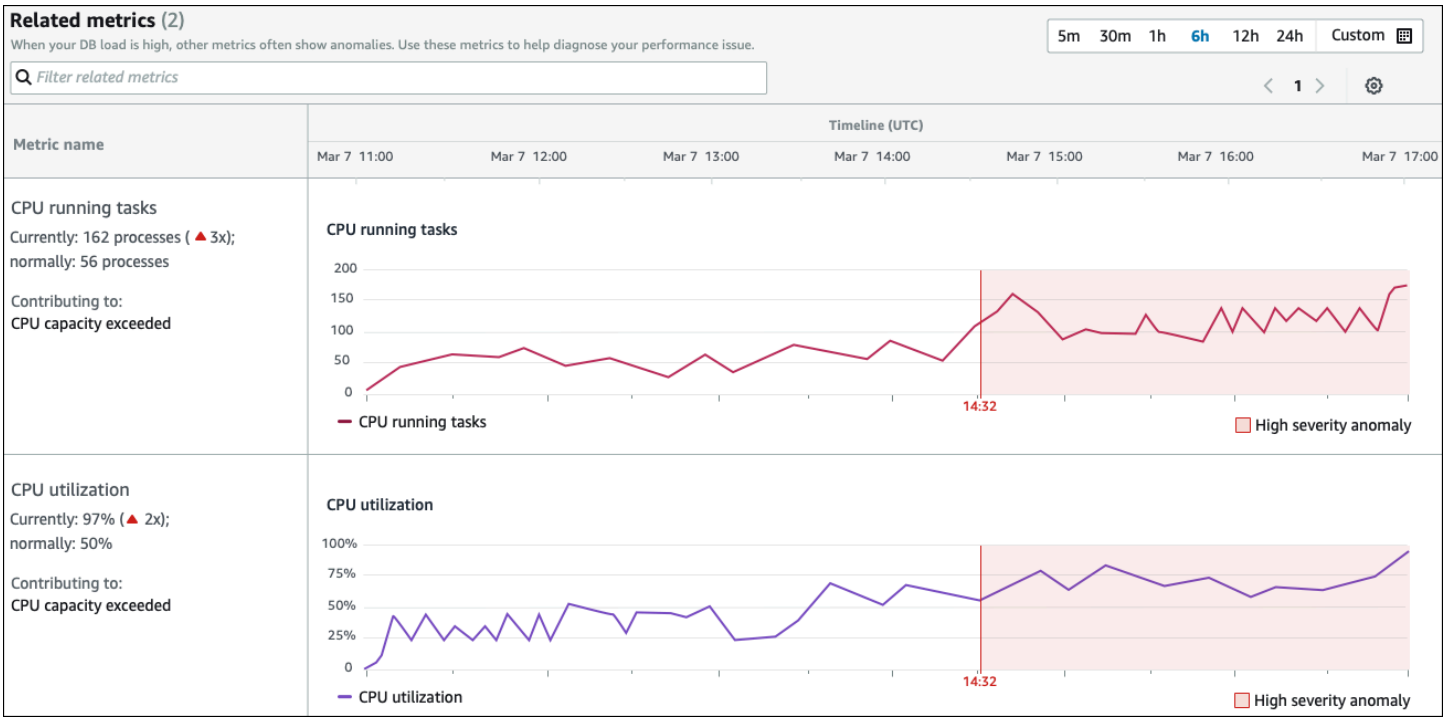
Per impostazione predefinita, il grafico di caricamento viene suddiviso in base agli eventi di attesa. Ciò significa che per ogni barra del grafico, l'area colorata più grande rappresenta l'evento di attesa che contribuisce maggiormente al carico totale del DB. Il grafico mostra l'ora (in rosso) in cui è iniziato il problema. Concentra la tua attenzione sugli eventi di attesa che occupano più spazio nella barra:

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

Gli eventi di attesa precedenti appaiono più del normale per questo database Aurora MySQL. Per informazioni su come ottimizzare le prestazioni utilizzando gli eventi di attesa in Amazon Aurora, consulta Tuning with wait events for Aurora MySQL e Tuning with wait events for Aurora PostgreSQL nella Amazon Aurora User Guide. Per informazioni su come ottimizzare le prestazioni utilizzando gli eventi di attesa in RDS per PostgreSQL, consulta Tuning with wait events for RDS for PostgreSQL nella Amazon RDS User Guide.

Metriche correlate

La sezione Metriche correlate elenca le anomalie contestuali, che sono risultati specifici all'interno dell'anomalia causale. Questi risultati forniscono informazioni aggiuntive sui problemi di prestazioni.



La tabella delle metriche correlate ha due colonne: Nome delle metriche e Cronologia (UTC). Ogni riga della tabella corrisponde a una metrica specifica.

La prima colonna di ogni riga contiene le seguenti informazioni:

- ***Nome***: il nome della metrica. La prima riga identifica la metrica come attività di esecuzione della CPU.
- Attualmente: il valore corrente della metrica. Nella prima riga, il valore corrente è 162 processi (3x).

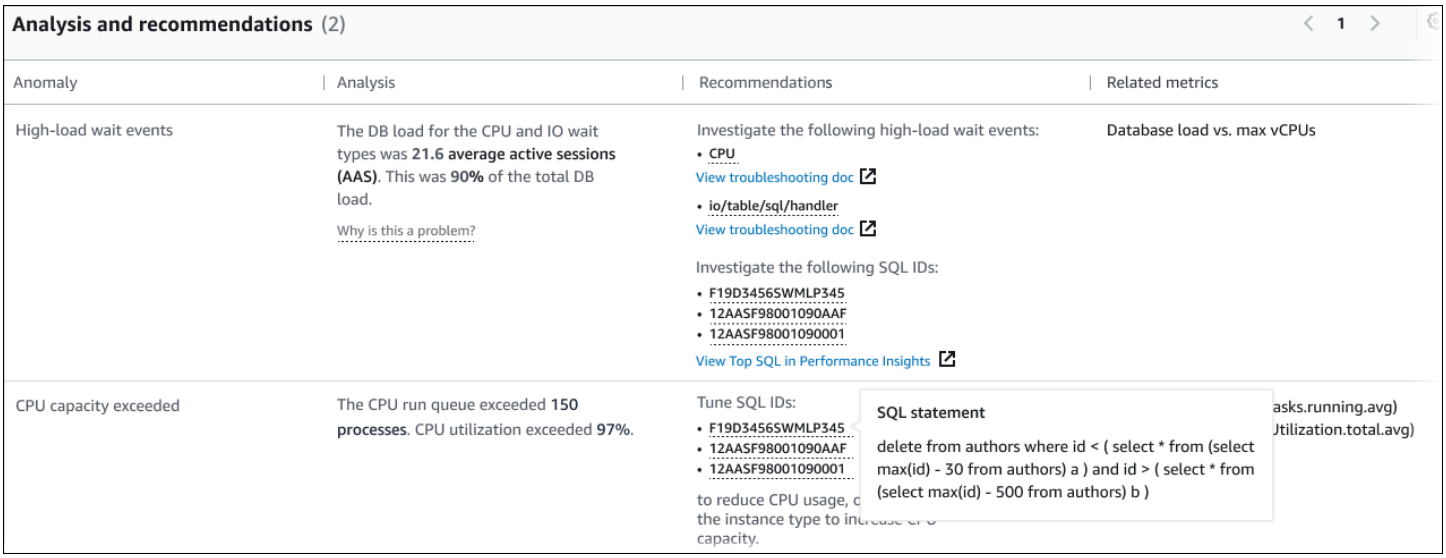
- Normalmente: la linea di base di questa metrica per questo database quando funziona normalmente. DevOpsGuru for RDS calcola la linea di base come valore del 95° percentile in 1 settimana di cronologia. La prima riga indica che sulla CPU sono in genere in esecuzione 56 processi.
- Contribuire a: il risultato associato a questa metrica. Nella prima riga, la metrica delle attività di esecuzione della CPU è associata all'anomalia della capacità della CPU superata.

La colonna Cronologia mostra un grafico a linee per la metrica. L'area ombreggiata mostra l'intervallo di tempo in cui DevOps Guru for RDS ha indicato il risultato come di elevata gravità.

Analisi e raccomandazioni

Mentre l'anomalia causale descrive il problema generale, un'anomalia contestuale descrive un risultato specifico che richiede un'indagine. Ogni risultato corrisponde a una serie di metriche correlate.

Nel seguente esempio di sezione Analisi e raccomandazioni, l'elevata anomalia di carico del DB presenta due risultati.



La tabella contiene le seguenti colonne:

- Anomalia: una descrizione generale di questa anomalia contestuale. In questo esempio, la prima anomalia è rappresentata da eventi di attesa ad alto carico e la seconda è il superamento della capacità della CPU.
- Analisi: una spiegazione dettagliata dell'anomalia.

Nella prima anomalia, tre tipi di attesa contribuiscono al 90% del carico del DB. Nella seconda anomalia, la coda di esecuzione della CPU superava i 150, il che significa che in un dato momento, più di 150 sessioni erano in attesa del tempo della CPU. L'utilizzo della CPU era superiore al 97%, il che significa che per tutta la durata del problema, la CPU è stata occupata il 97% delle volte. Pertanto, la CPU era occupata quasi ininterrottamente, mentre una media di 150 sessioni attendeva l'esecuzione sulla CPU.

- Raccomandazioni: la risposta suggerita dell'utente all'anomalia.

  Nella prima anomalia, DevOps Guru for RDS consiglia di esaminare gli eventi di attesa e. `cpu` `io/table/sql/handler` Per informazioni su come ottimizzare le prestazioni del database in base a questi eventi, consulta cpu e io/table/sql/handler nella Guida per l'utente di Amazon Aurora.

  Nella seconda anomalia, DevOps Guru for RDS consiglia di ridurre il consumo di CPU ottimizzando tre istruzioni SQL. Puoi passare il mouse sui link per visualizzare il testo SQL.

- Metriche correlate: metriche che forniscono misurazioni specifiche dell'anomalia. Per ulteriori informazioni su questi parametri, consulta il riferimento ai parametri per Amazon Aurora nella Guida per l'utente di Amazon Aurora o il riferimento ai parametri per Amazon RDS nella Guida per l'utente di Amazon RDS.

  Nella prima anomalia, DevOps Guru for RDS consiglia di confrontare il carico del DB con la CPU massima per l'istanza. Nella seconda anomalia, si consiglia di esaminare la coda di esecuzione della CPU, l'utilizzo della CPU e la frequenza di esecuzione SQL.

Visualizzazione delle anomalie proattive

All'interno di Insights, puoi visualizzare le anomalie per le risorse Amazon RDS. Ogni analisi proattiva fornisce dettagli su un'anomalia proattiva. In una pagina di analisi proattiva, puoi visualizzare una panoramica delle informazioni, metriche dettagliate sull'anomalia e consigli per prevenire problemi futuri. Per visualizzare un'anomalia proattiva, vai alla pagina di analisi proattiva.

Panoramica di Insight

La sezione panoramica di Insight fornisce dettagli sul motivo per cui l'analisi è stata creata. Visualizza la gravità dell'analisi, nonché una descrizione dell'anomalia e un periodo di tempo in cui si è verificata l'anomalia. Elenca inoltre il numero di servizi e applicazioni interessati rilevati da Guru. DevOps

Metriche

La sezione Metriche fornisce grafici dell'anomalia. Ogni grafico mostra una soglia determinata dal comportamento di base della risorsa, nonché i dati della metrica riportata dal momento dell'anomalia.

Raccomandazioni per risorse aggregate

Questa sezione suggerisce le azioni che è possibile intraprendere per mitigare i problemi segnalati prima che diventino un problema più grave. Le azioni che puoi intraprendere sono presentate nella colonna Modifica personalizzata consigliata. La logica alla base delle raccomandazioni è presentata nella sezione Perché DevOps Guru lo raccomanda? colonna. Per ulteriori informazioni su come rispondere ai consigli, vederethe section called “Risposta alle raccomandazioni ”.

Risposta alle raccomandazioni

Le raccomandazioni sono la parte più importante dell'analisi. In questa fase dell'analisi, si interviene per risolvere il problema delle prestazioni. In genere, si eseguono le seguenti operazioni:

1. Decidi se il problema di prestazioni segnalato indica un problema reale.

   In alcuni casi, un problema potrebbe essere prevedibile e benigno. Ad esempio, se si sottopone un database di test a un carico di database estremo, DevOps Guru for RDS segnala il carico come un'anomalia delle prestazioni. Tuttavia, non è necessario porre rimedio a questa anomalia perché è un risultato previsto dei test.

   Se ritieni che il problema richieda una risposta, vai al passaggio successivo.
2. Decidi se implementare la raccomandazione.

   Nella tabella dei consigli, una colonna mostra le azioni consigliate. Per approfondimenti reattivi, questa è la colonna Cosa consigliamo in una pagina di dettaglio delle anomalie reattive. Per approfondimenti proattivi, questa è la colonna Modifica personalizzata consigliata in una pagina di analisi proattiva.

   DevOpsGuru for RDS offre un elenco di consigli che coprono diversi potenziali scenari problematici. Dopo aver esaminato questo elenco, stabilite quale raccomandazione è più pertinente alla vostra situazione attuale e valutate la possibilità di applicarla. Se una raccomandazione funziona per la tua situazione, vai al passaggio successivo. In caso contrario, salta il passaggio rimanente e risolvi il problema utilizzando tecniche manuali.
3. Esegui le azioni consigliate.

DevOpsGuru for RDS consiglia di eseguire una delle seguenti operazioni:

- Eseguire un'azione correttiva specifica.

  Ad esempio, DevOps Guru for RDS potrebbe consigliare di aggiornare la capacità della CPU, ottimizzare le impostazioni del pool di applicazioni o abilitare lo schema delle prestazioni.

- Analizza la causa del problema.

  In genere, DevOps Guru for RDS consiglia di esaminare specifiche istruzioni SQL o eventi di attesa. Ad esempio, un consiglio potrebbe essere quello di esaminare l'evento di attesa. `io/table/sql/handler` Cerca l'evento di attesa elencato in Tuning with wait events for Aurora PostgreSQL o Tuning with wait events for Aurora MySQL nella Amazon Aurora User Guide o in Tuning with wait events for RDS for PostgreSQL nella Amazon RDS User Guide. Quindi esegui le azioni consigliate.

  > **Important**
  >
  > È consigliabile testare eventuali modifiche in un'istanza di test prima di modificare un'istanza di produzione. In questo modo, capisci l'impatto del cambiamento.

Monitoraggio dei database non relazionali tramite Guru DevOps

DevOpsGuru è in grado di generare approfondimenti per i tuoi database non relazionali o NoSQL che ti aiutano a mantenere le tue risorse configurate secondo le migliori pratiche. Ad esempio, DevOps Guru può aiutarti a rimanere aggiornato sulla pianificazione della capacità prevedendo le esigenze future sulla base del traffico esistente. DevOpsGuru è in grado di identificare se state utilizzando meno risorse di quelle configurate e fornire consigli per migliorare la disponibilità delle applicazioni in base all'utilizzo storico. Questo può aiutarvi a ridurre i costi inutili.

Oltre alla pianificazione della capacità, DevOps Guru rileva e aiuta a risolvere problemi operativi come limitazioni, conflitti nelle transazioni, errori nei controlli condizionali e aree di miglioramento dei parametri SDK. I database sono in genere collegati a più servizi e risorse e DevOps Guru è in grado di correlare la struttura dell'applicazione per l'analisi utilizzando gruppi basati su tag o aggregazioni. AWS CloudFormation Le anomalie possono coinvolgere più risorse, tutte interessate dalla stessa soluzione. DevOpsGuru è in grado di correlarsi tra diverse metriche di risorse, configurazioni, log ed eventi. Ad esempio, DevOps Guru può analizzare e mettere in relazione i dati di una funzione Lambda che potrebbe leggere o scrivere dati da Amazon DynamoDB una tabella. In questo modo,

DevOps Guru monitora più risorse correlate per rilevare anomalie e fornire informazioni utili per le soluzioni di database.

Monitoraggio delle operazioni del database in Amazon DynamoDB

La tabella seguente mostra esempi di scenari e approfondimenti monitorati da DevOps Guru. Amazon DynamoDB

Amazon DynamoDB caso d'uso	Esempi	Metriche
Rileva quando viene utilizzata una grande percentuale AccountProvisionedWriteCapacityUtilization di AccountProvisionedReadCapacityUtilization e, a causa di un gran numero di richieste di lettura e scrittura.	Amazon DynamoDB la capacità di consumo delle tabelle per le richieste di lettura o scrittura sta raggiungendo i limiti a livello di tabella.	AccountProvisionedReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
Rileva gli errori di controllo condizionale nelle Amazon DynamoDB richieste causati da un'espressione di condizione fornita che non corrisponde a quanto previsto nel database.	Gli errori di controllo condizionale sono causati da dati errati nella tabella, da un'espressione di condizione rigorosa o da condizioni di gara.	ConditionalCheckFailedRequests

Monitoraggio delle operazioni del database in Amazon ElastiCache

La tabella seguente mostra esempi di scenari e approfondimenti monitorati da DevOps Guru. Amazon ElastiCache

Scenario identificato da DevOps Guru	CloudWatch metriche monitorate
Rileva quando un Amazon ElastiCache cluster sta raggiungendo il limite di elaborazione per	Utilizzo della CPU, utilizzo della CPU del motore, sfratti

Scenario identificato da DevOps Guru	CloudWatch metriche monitorate
Redis o Memcached a causa delle variazioni delle richieste dei cluster.	

Integrazione con CodeGuru Profiler

Questa sezione fornisce una panoramica su come Amazon DevOps Guru si integra con Amazon CodeGuru Profiler. Puoi visualizzare i consigli da CodeGuru Profiler come informazioni sulla console DevOps Guru.

Amazon DevOps Guru si integra con Amazon CodeGuru Profiler con un EventBridge regola gestita. CodeGuru Profiler invia eventi a EventBridge. La regola gestita inoltra gli eventi inviati con il bus eventi predefinito. Ogni evento in entrata da CodeGuru Profiler è un rapporto di anomalia proattivo. Per ulteriori informazioni, consultaUtilizzo di EventBridge con CodeGuru Profiler.

DevOps Guru supporta eventi in entrata con EventBridge. Un evento indica una modifica in una raccomandazione identificata da DevOps Guru. CodeGuru Profiler invia un evento heartbeat ogni 24 ore per mostrare la continuità dell'evento. Gli eventi trasportano CodeGuru Informazioni sui suggerimenti di Profiler e metadati per le risorse di calcolo. Per informazioni sul ciclo di vita di un evento, vedereAmazon EventBridge Eventi.

Quando configuri DevOps Guru, DevOps Guru crea EventBridge Regola gestita nel tuo account che inoltra eventi da un altro servizio. Questa regola viene indirizzata a DevOps Guru. Le notifiche vengono inviate quando c'è un evento in entrata.

Un bus eventi riceve eventi da una fonte come DevOps Guru e li inoltra alle regole associate a quel bus eventi. Per ulteriori informazioni sui bus eventi, consultaBus di eventi.

Per informazioni su alcuni dei parametri, consultaEventi Amazon EventBridge.

Da ricevere CodeGuru Approfondimenti di Profiler in DevOps Guru, devi avere quanto segue.

- CodeGuru Profiler deve essere abilitato. Per informazioni su come abilitare CodeGuru Profiler, vediConfigurazione di CodeGuru Profiler.
- DevOps Guru deve essere abilitato. Per informazioni sull'abilitazione di DevOps Guru, consultaAbilita DevOps Guru.
- Le stesse risorse devono essere monitorate nella stessa regione in entrambe CodeGuru Profiler e DevOps Guru.

Definizione delle applicazioni utilizzandoAWSrisorse

Amazon DevOpsGuru raggruppa le risorse che si trovano nel limite di copertura che specifica quali risorse analizza per ottenere informazioni operative. Le risorse sono raggruppate per risorse inAWS CloudFormationpile o risorse con tag. Scegli le pile o i tag durante la configurazione DevOpsGuru. Puoi anche aggiornare gli stack o i tag in un secondo momento. Ti consigliamo di considerare i tuoi gruppi di risorse come applicazioni. Ad esempio, è possibile che tu disponga di tutte le risorse utilizzate per un'applicazione di monitoraggio definite in un unico stack. Oppure puoi aggiungere lo stesso tag a tutte le risorse che usi in un'applicazione di database. Il limite che definisce quali risorseDevOpsGuru analizza. Tutte le risorse della collezione si trovano all'interno di questo limite. Tutte le risorse dell'account che non sono incluse nella raccolta di risorse sono al di fuori dei limiti e non vengono analizzate. Per ulteriori informazioni sui servizi e sulle risorse supportati, consultaAmazon DevOpsPrezzi Guru.

È possibile definire il limite di copertura che contiene le risorse delle applicazioni in tre modi.

- Specificare che tutto sia supportatoAWSrisorse nel tuoAWSaccount e regione. Ciò rende il tuo account e la tua regione il limite delle tue risorse. Con questa opzione, DevOpsGuru analizza tutte le risorse supportate nel tuo account e nella tua regione. Tutte le risorse che si trovano in uno stack sono raggruppate in un'applicazione. Tutte le risorse che non sono in uno stack vengono raggruppate nella rispettiva applicazione.
- Utilizzo diAWS CloudFormationstack per specificare le risorse nelle tue applicazioni. Uno stack contiene risorse generate utilizzandoAWS CloudFormation. In DevOpsGuru, scegli gli stack nel tuo account. Le risorse presenti in ogni stack selezionato sono raggruppate in un'applicazione. Tutte le risorse presenti negli stack vengono analizzate da DevOpsGuru per approfondimenti.
- Utilizzo diAWStag per specificare le risorse nelle applicazioni. Un recordAWStag contiene unchiavee unvalore. In DevOpsGuru, scegli un tagchiavee opzionalmente scegli una o piùvaloriche sono abbinati a quellochiave. Puoi utilizzare il pluginvaloriper raggruppare le tue risorse in applicazioni.

Per ulteriori informazioni, consultare Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru.

Argomenti

- Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru
- Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru

Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru

Puoi utilizzare i tag per identificare le AWS risorse che Amazon DevOps Guru analizza e per specificare quali risorse sono raggruppate per il monitoraggio con la chiave e i valori dei tag selezionati. Puoi modificare queste configurazioni quando configuri DevOps Guru o quando scegli Modifica risorse analizzate dalla pagina Risorse analizzate. Dopo aver selezionato Tag, scegli una chiave di tag specifica che inizia con 'devops-guru-'. Per analizzare tutte le risorse dell'account e utilizzare i valori dei tag per raggruppare le risorse, seleziona Tutte le risorse dell'account. Per utilizzare i valori dei tag per specificare le risorse che DevOps Guru deve analizzare, seleziona Scegli valori di tag specifici.

> **Note**
>
> Quando è selezionato Tutte le risorse dell'account e non esiste alcun valore di tag, le risorse senza la chiave del tag vengono raggruppate e analizzate separatamente.

Utilizzi la chiave di un tag per identificare le risorse, quindi usi i valori con quella chiave per raggruppare le risorse nelle tue applicazioni. Ad esempio, puoi etichettare le tue risorse con la chiave`devops-guru-applications`, quindi utilizzare quella chiave con un valore diverso per ciascuna delle tue applicazioni. Puoi utilizzare le coppie di tag `devops-guru-applications/database`chiave-valore e `devops-guru-applications/monitoring` identificare tre applicazioni nel tuo account. `devops-guru-applications/cicd` Ogni applicazione è composta da risorse correlate che contengono la stessa coppia tag chiave-valore. Puoi aggiungere tag alle tue risorse utilizzando il AWS servizio a cui appartengono. Per ulteriori informazioni, consulta Aggiungere AWS tag alle AWS risorse.

Dopo aver aggiunto un tag alle risorse dell'applicazione, puoi filtrare le tue informazioni in base ai tag sulle risorse che le hanno generate. Per ulteriori informazioni su come filtrare le informazioni dettagliate utilizzando un tag, consultaVisualizzazioneDevOpsGuru Insights.

Per ulteriori informazioni sui servizi e le risorse supportati, consulta i prezzi di Amazon DevOps Guru.

Argomenti

- Che cos'è un AWS tag?
- Definizione di un'applicazione DevOps Guru utilizzando un tag

- Usare i tag con DevOps Guru
- Aggiungere AWS tag alle AWS risorse

Che cos'è un AWS tag?

I tag aiutano a identificare e a organizzare le risorse AWS. Molti servizi AWS supportano l'assegnazione di tag, perciò è possibile assegnare lo stesso tag a risorse di diversi servizi per indicare che queste sono correlate. Ad esempio, puoi assegnare a una risorsa della tabella Amazon DynamoDB lo stesso tag associato a una funzione AWS Lambda. Per ulteriori informazioni sull'utilizzo dei tag, consulta il whitepaper Tagging best practices (Best practice relative al tagging).

Ogni tag AWS è costituito da due parti.

- Una chiave di tag (ad esempio, `CostCenter`, `Environment`, `Project` o `Secret`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un campo facoltativo noto come valore del tag (ad esempio, `111122223333`, `Production` o un nome di team). Non specificare il valore del tag equivale a utilizzare una stringa vuota. Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra maiuscole e minuscole.

Tutti questi sono noti come coppie chiave-valore.

Definizione di un'applicazione DevOps Guru utilizzando un tag

Per definire la tua applicazione Amazon DevOps Guru utilizzando un tag, aggiungilo alle AWS risorse del tuo account che compongono l'applicazione. Il tag contiene una chiave e un valore. Ti consigliamo di aggiungere un tag a ciascuna delle tue AWS risorse analizzate da DevOps Guru con la stessa chiave. Usa un valore diverso nel tag per raggruppare le risorse nelle tue applicazioni. Ad esempio, è possibile assegnare tag con la chiave `devops-guru-analysis-boundary` a tutte le AWS risorse nel limite di copertura. Usa valori diversi con quella chiave per identificare le applicazioni nel tuo account. È possibile utilizzare `containers` i valori `database` e `monitoring` per tre applicazioni. Per ulteriori informazioni, consulta Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru.

Se si utilizzano i AWS tag per specificare quali risorse analizzare, è possibile utilizzare i tag con una sola chiave. Puoi abbinare la chiave dei tag a qualsiasi valore. Utilizzate il valore per raggruppare le risorse che contengono la chiave nelle vostre applicazioni operative.

> **Important**
>
> La stringa impiegata per una chiave in un tag utilizzato per definire la copertura delle risorse deve iniziare con il prefisso `Devops-guru-`. La chiave del tag potrebbe essere `DevOps-Guru-deployment-application` o `devops-guru-rds-application`. Quando crei una chiave, nella chiave puoi utilizzare indistintamente maiuscole e minuscole. Dopo la creazione di una chiave, distingue tra lettere maiuscole e minuscole. Ad esempio, DevOps Guru funziona con una chiave denominata `devops-guru-rds` e una chiave denominata`DevOps-Guru-RDS`, e queste agiscono come due chiavi diverse. Le possibili coppie chiave/valore nell'applicazione potrebbero essere `Devops-Guru-production-application/RDS` o `Devops-Guru-production-application/containers`.

Usare i tag con DevOps Guru

Specificate i AWS tag che identificano le AWS risorse che desiderate che Amazon DevOps Guru analizzi o specificate i valori dei tag che identificano le risorse da raggruppare. Queste risorse rappresentano il limite di copertura delle risorse. È possibile scegliere una chiave e zero o più valori.

Per scegliere i tuoi tag

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Apri il pannello di navigazione, quindi espandi Impostazioni.
3. In Risorse analizzate, scegli Modifica.
4. Scegli Tag se vuoi che DevOps Guru analizzi tutte le risorse che contengono i tag che hai scelto. Scegli una chiave, quindi scegli una delle seguenti opzioni.

   - Tutte le risorse dell'account: analizza tutte AWS le risorse nella regione e nell'account correnti. Le risorse con la chiave di tag selezionata sono raggruppate in base al valore del tag, se esistente. Le risorse senza questa chiave di tag vengono raggruppate e analizzate separatamente.
   - Scegli valori di tag specifici: vengono analizzate tutte le risorse che contengono un tag con la chiave scelta. DevOpsGuru raggruppa le tue risorse in applicazioni in base ai valori del tag.

La chiave del tag deve iniziare con il prefissodevops-guru-. Questo prefisso non fa distinzione tra maiuscole e minuscole. Ad esempio, una chiave valida è. DevOps-Guru-Production-Applications

5. Selezionare Salva.

Aggiungere AWS tag alle AWS risorse

Quando specifichi i AWS tag che identificano le AWS risorse che vuoi che DevOps Guru analizzi, scegli i tag a cui sono associate risorse. Puoi aggiungere tag alle tue risorse usando il AWS servizio a cui appartiene ogni risorsa o usando il AWS Tag Editor.

- Per gestire i tag utilizzando il servizio delle risorse, utilizza la console o l'SDK del servizio a cui appartiene una risorsa. AWS Command Line Interface Ad esempio, puoi taggare una risorsa di flusso Amazon Kinesis o una risorsa di CloudFront distribuzione Amazon. Questi sono due esempi di servizi con risorse che possono essere taggate. La maggior parte delle risorse che DevOps Guru può analizzare supportano i tag. Per ulteriori informazioni, consulta Tagging your stream nella Amazon Kinesis Developer Guide e Tagging a distribution nella Amazon Developer Guide. CloudFront Per sapere come aggiungere tag ad altri tipi di risorse, consulta la guida per l'utente o la guida per gli sviluppatori del AWS servizio a cui appartengono.

  > **Note**
  >
  > Quando tagghi le risorse Amazon RDS, devi etichettare l'istanza di database e non il cluster.

- Puoi utilizzare AWS Tag Editor per gestire i tag in base alle risorse nella tua regione e in base alle risorse di AWS servizi specifici. Per ulteriori informazioni, consulta Tag editor nella AWSResource Group and Tags User Guide.

Quando aggiungi un tag a una risorsa, puoi aggiungere solo la chiave o la chiave e un valore. Ad esempio, puoi creare un tag con la chiave devops-guru- per tutte le risorse che fanno parte dell' DevOps applicazione. Puoi anche aggiungere un tag con la chiave devops-guru- e il valoreRDS, quindi aggiungere quella coppia chiave-valore solo alle risorse Amazon RDS della tua applicazione. Ciò è utile se desideri visualizzare nella console gli approfondimenti generati solo dalle risorse Amazon RDS della tua applicazione.

Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru

É possibile utilizzareAWS CloudFormationpile per specificare qualiAWSrisorse che desideri DevOpsGuru da analizzare. Una pila è una raccolta diAWSrisorse gestite come una singola unità. Le risorse negli stack che scegli costituiscono le tue DevOpsLimite di copertura Guru Per ogni stack scelto, i dati operativi nelle risorse supportate vengono analizzati per individuare eventuali comportamenti anomali. Questi problemi vengono quindi raggruppati in anomalie correlate per creare approfondimenti. Ogni approfondimento include uno o più consigli per aiutarti a risolverli. Il numero massimo di stack che puoi specificare è 1000. Per ulteriori informazioni, consulta la paginaUtilizzo degli stacknelAWS CloudFormationGuida per l'utente dieAggiornamento del tuoAWScopertura di analisi in DevOpsGuru.

Dopo aver scelto una pila DevOpsGuru inizia immediatamente ad analizzare qualsiasi risorsa che aggiungi. Se rimuovi una risorsa da uno stack, questa non viene più analizzata.

Se scegli di avere DevOpsGuru analizza tutte le risorse supportate nel tuo account (questo significa il tuoAWSl'account e la regione sono tuoi DevOpsGuru (confine di copertura), quindi DevOpsGuru analizza e crea informazioni dettagliate per ogni risorsa supportata nel tuo account, comprese quelle presenti negli stack. Un'analisi creata da anomalie in una risorsa che non si trova in uno stack è raggruppata nellivello di account. Se un insight viene creato da anomalie in una risorsa che si trova in uno stack, viene raggruppato in base allivello di stack. Per ulteriori informazioni, consulta la pagina Comprendere come i comportamenti anomali sono raggruppati in approfondimenti .

Scelta degli stack per DevOpsGuru

Specifica le risorse che desideri DevOpsGuru da analizzare scegliendo ilAWS CloudFormationpile che li creano. A questo proposito, utilizzare il comandoAWS Management Consoleo l'SDK.

Argomenti

- Scelta degli stack per DevOpsGuru da analizzare (console)
- Scelta degli stack per DevOpsGuru da analizzare (DevOpsGuru

Scelta degli stack per DevOpsGuru da analizzare (console)

Puoi aggiungereAWS CloudFormationimpila utilizzando la console.

Per scegliere gli stack che contengono le risorse da analizzare

1. Aprire l'Amazon DevOpsConsole Guruhttps://console.aws.amazon.com/devops-guru/.
2. Aprire il riquadro di navigazione, quindi scegliereImpostazioni.
3. InDevOpsCopertura dell'analisi Guru, scegliManage (Gestione).
4. ScegliCloudFormation pilese vuoi DevOpsGuru

   - Tutte le risorse— Tutte le risorse presenti negli stack del tuo account vengono analizzate. Le risorse di ogni stack sono raggruppate in una propria applicazione. Tutte le risorse del tuo account che non sono incluse in uno stack non vengono analizzate.
   - Seleziona pile— Selezionare le pile desiderate DevOpsGuru da analizzare. Le risorse in ogni stack selezionato sono raggruppate nella rispettiva applicazione. Puoi inserire il nome di una pila inIndividuaper individuare rapidamente uno stack specifico. È possibile selezionare fino a 1.000 stack.
5. Seleziona Salva.

Scelta degli stack per DevOpsGuru da analizzare (DevOpsGuru

SpecificaAWS CloudFormationpile che utilizzano Amazon DevOpsGuru SDK, usa il`UpdateResourceCollection`Metodo. Per ulteriori informazioni, consulta la paginaUpdateResourceCollectionnelAmazon DevOpsDocumentazione.

Lavorare con Amazon EventBridge

Amazon DevOps Guru si integra con Amazon EventBridge per informarti di determinati eventi relativi agli approfondimenti e ai corrispondenti aggiornamenti di insight. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere avviate automaticamente includono i seguenti esempi:

- Invocare una funzione AWS Lambda
- Richiamo di un comando di esecuzione di Amazon Elastic Compute Cloud
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati Step Functions
- Notifica di Amazon SNS o Amazon SQS

Puoi selezionare uno dei seguenti modelli predefiniti per filtrare gli eventi o creare una regola di modello personalizzata per avviare azioni in una risorsa supportata. AWS

- DevOps Guru New Insight Open
- DevOps Associazione Guru New Anomaly
- DevOps Guru Insight Severity è stato aggiornato
- DevOps Creata una nuova raccomandazione per Guru
- DevOps Guru Insight è chiuso

Eventi per DevOps Guru

Di seguito sono riportati alcuni esempi di eventi tratti da DevOps Guru. Gli eventi vengono emessi sulla base del best effort. Per ulteriori informazioni sui modelli di eventi, consulta la sezione Guida introduttiva ad Amazon EventBridge o Amazon EventBridge Event Patterns.

DevOpsGuruNuovo evento Insight Open

Quando DevOps Guru apre una nuova intuizione, invia il seguente evento.

```
{
```

```
    "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"
    }
  },
```

Modello di eventi di esempio personalizzato per un nuovo Insight ad alta severità

Le regole utilizzano modelli di eventi per selezionare eventi e instradarli ai target. Di seguito è riportato un esempio di pattern di eventi DevOps Guru.

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

Aggiornamento DevOpsImpostazioni Guru

Puoi aggiornare il seguente Amazon DevOpsImpostazioni del guru:

- Vostro DevOpsCopertura Guru. Ciò determina quali risorse del tuo account vengono analizzate.
- Le tue notifiche. Ciò determina quali argomenti di Amazon Simple Notification Service vengono utilizzati per notificarti informazioni importanti DevOpsEventi Guru.
- Funzionalità per approfondimenti avanzati. Ciò include il rilevamento delle anomalie nei log, la crittografia e ilAWS Systems Managerimpostazioni di integrazione. Ciò determina se DevOpsGuru mostra i dati di registro, indica se si utilizzano chiavi di sicurezza aggiuntive e se un OpsItem viene creato in Systems Manager OpsCenter per ogni nuova intuizione.

Argomenti

Aggiornamento delle impostazioni dell'account di gestione

È possibile configurare DevOpsGuru per gli account della tua organizzazione. Se non hai registrato un amministratore delegato, puoi farlo scegliendoRegistra amministratore delegato. Per ulteriori informazioni sulla registrazione di un amministratore delegato, vedereAbilitaDevOpsGuru.

Aggiornamento del tuoAWScopertura di analisi in DevOpsGuru

Puoi aggiornare qualiAWSrisorse nel tuo account DevOpsAnalisi Guru. Per fare ciò, vai alRisorse analizzatepagina nella console e poi scegliModifica. Per ulteriori informazioni, consulta Visualizzazione delle risorse analizzate.

Aggiornamento delle notifiche in DevOpsGuru

Imposta gli argomenti di Amazon Simple Notification Service che vengono utilizzati per informarti su Amazon importanti DevOpsEventi Guru. Puoi scegliere da un elenco di nomi di argomenti già esistenti nel tuoAWSaccount, inserisci il nome di un nuovo argomento DevOpsGuru crea nel tuo account o inserisci l'Amazon Resource Name (ARN) di un argomento esistente in qualsiasiAWSaccount nella tua regione. Se specifichi l'ARN di un argomento che non è presente nel tuo account, devi concedere l'autorizzazione perDevOpsGuru per accedere a quell'argomento aggiungendovi una policy IAM. Per ulteriori informazioni, consulta Autorizzazioni per argomenti di Amazon SNS. Puoi specificare fino a due argomenti.

DevOpsGuru invia notifiche per i seguenti aggiornamenti:

- Viene creata una nuova intuizione.
- Una nuova anomalia viene aggiunta a un'analisi.
- La gravità di un'intuizione viene aggiornata da`Low`o`Medium`a`High`.
- Lo stato di un'analisi cambia da continuo a risolto.
- Viene identificata una raccomandazione per un'analisi.

DevOpsGuru invia anche notifiche se selezionatoAWS CloudFormationla chiave stack o tag non è valida quando stai tentando di aggiungere risorse al tuo DevOpsAccount Guru.

Puoi scegliere di ricevere notifiche Amazon SNS per tutti i tipi di aggiornamenti relativi a un problema o di ricevere notifiche Amazon SNS solo quando il problema viene aperto, chiuso o ha un cambiamento di gravità. Per impostazione predefinita, ricevi notifiche per tutti gli aggiornamenti.

Per aggiornare le notifiche, accedi prima alla pagina delle notifiche e poi scegli se aggiungere, rimuovere o aggiornare le configurazioni per gli argomenti relativi alle notifiche di Amazon SNS.

Argomenti

- Passa alle impostazioni di notifica nel DevOpsConsolle Guru
- Aggiungere argomenti di notifica di Amazon SNS nel DevOpsConsolle Guru
- Rimozione degli argomenti di notifica di Amazon SNS nel DevOpsConsolle Guru
- Aggiornamento delle configurazioni di notifica di Amazon SNS
- Autorizzazioni aggiunte al tuo argomento Amazon SNS

Passa alle impostazioni di notifica nel DevOpsConsolle Guru

Per aggiornare le notifiche, devi prima accedere alla sezione delle impostazioni di notifica.

Per accedere alla sezione delle impostazioni di notifica

1. Apri Amazon DevOpsConsole Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.

   La pagina Impostazioni includeNotifichesezione, con informazioni sugli argomenti configurati di Amazon SNS.

Aggiungere argomenti di notifica di Amazon SNS nel DevOpsConsolle Guru

Per aggiungere un argomento di notifica di Amazon SNS nel DevOpsConsolle Guru

1. the section called “Passa alle impostazioni di notifica nel DevOpsConsolle Guru”.
2. Scegliere Add notification (Aggiungi notifica).
3. Per aggiungere un argomento Amazon SNS, esegui una delle seguenti operazioni.

   - ScegliGenera un nuovo argomento SNS tramite e-mail. Quindi, daSpecificare l'indirizzo e-mail, inserisci l'indirizzo email a cui desideri ricevere le notifiche. Per inserire indirizzi e-mail aggiuntivi, scegliAggiungi una nuova email.
   - ScegliUsa un argomento SNS esistente. Quindi, daScegli un argomento nel tuoAWSconto, scegli l'argomento che desideri utilizzare.
   - ScegliUsa un argomento SNS esistente (ARN) per specificare un argomento esistente da un altro account. Poi, nelInserisci un ARN per un argomento, inserisci l'argomento ARN. L'ARN è il nome della risorsa Amazon dell'argomento. Puoi specificare un argomento in un altro account. Se utilizzi un argomento in un altro account, devi aggiungere una politica sulle risorse all'argomento. Per ulteriori informazioni, consulta Autorizzazioni per argomenti di Amazon SNS.
4. Seleziona Save (Salva.

Rimozione degli argomenti di notifica di Amazon SNS nel DevOpsConsolle Guru

Per rimuovere gli argomenti di Amazon SNS nel DevOpsConsolle Guru

1. the section called “Passa alle impostazioni di notifica nel DevOpsConsolle Guru”.
2. ScegliSeleziona un argomento esistente.
3. Dal menu a discesa, seleziona l'argomento che desideri rimuovere.
4. Scegliere Remove (Rimuovi).
5. Seleziona Salva.

Aggiornamento delle configurazioni di notifica di Amazon SNS

Esistono due tipi di configurazioni di notifica per gli argomenti relativi alle notifiche di Amazon SNS in DevOpsGuru. Puoi scegliere di ricevere notifiche di tutti i livelli di gravità o solo notifiche conAltoeMediolivelli di gravità. Puoi anche scegliere di ricevere notifiche per tutti i tipi di aggiornamenti o solo per alcuni tipi di aggiornamenti.

Quando scegli di ricevere notifiche Amazon SNS per tutti i tipi di aggiornamenti relativi al problema, DevOpsGuru invia notifiche per i seguenti aggiornamenti:

- Viene creata una nuova intuizione.
- Una nuova anomalia viene aggiunta a un'analisi.
- La gravità di un'intuizione viene aggiornata da`Low`o`Medium`a`High`.
- Lo stato di un'analisi cambia da continuo a risolto.
- Viene identificata una raccomandazione per un approfondimento.

Per impostazione predefinita, ricevi soloAltoeMedionotifiche a livello di gravità e ricevi notifiche per tutti i tipi di aggiornamenti.

Per aggiornare le configurazioni delle notifiche per gli argomenti relativi alle notifiche di Amazon SNS

1. the section called “Passa alle impostazioni di notifica nel DevOpsConsolle Guru”.
2. ScegliSeleziona un argomento esistente.
3. Dal menu a discesa, seleziona l'argomento a cui desideri apportare aggiornamenti.

4. ScegliTutti i livelli di gravitàper ricevere notifiche con livelli di gravità alto, medio e basso oppure scegliSolo alto e medioper ricevere notifiche con livelli di gravità alti e medi.
5. ScegliAvvisami su tutti gli aggiornamenti di The Insight, oppure scegliAvvisami quando un'analisi viene aperta o chiusa o il livello di gravità cambia da Basso o Medio ad Alto.
6. Seleziona Salva.

Autorizzazioni aggiunte al tuo argomento Amazon SNS

Un argomento di Amazon SNS è una risorsa che contiene unAWS Identity and Access Managementpolitica delle risorse (IAM). Quando specifichi un argomento qui, DevOpsGuru aggiunge le seguenti autorizzazioni alla sua politica delle risorse.

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

Queste autorizzazioni sono necessarie per DevOpsGuru per pubblicare notifiche utilizzando un argomento. Se preferisci non avere queste autorizzazioni sull'argomento, puoi rimuoverle in tutta sicurezza e l'argomento continuerà a funzionare come prima di sceglierlo. Tuttavia, se queste autorizzazioni aggiunte vengono rimosse, DevOpsGuru non può usare l'argomento per generare notifiche.

Filtrare i tuoi DevOpsNotifiche Guru

Puoi filtrare i tuoi DevOpsNotifiche Guru dithe section called “Aggiornamento delle configurazioni di notifica di Amazon SNS”o utilizzando una politica di filtro degli abbonamenti Amazon SNS.

Argomenti

Filtraggio delle notifiche con una politica di filtro di abbonamento Amazon SNS

Puoi creare una politica di filtro degli abbonamenti Amazon Simple Notification Service (Amazon SNS) per ridurre il numero di notifiche che ricevi da Amazon DevOpsGuru.

Utilizza una politica di filtro per specificare i tipi di notifiche che ricevi. Puoi filtrare i tuoi messaggi Amazon SNS utilizzando le seguenti parole chiave.

- `NEW_INSIGHT`— Ricevi una notifica quando viene creata una nuova analisi.
- `CLOSED_INSIGHT`— Ricevi una notifica quando un approfondimento esistente viene chiuso.
- `NEW_RECOMMENDATION`— Ricevi una notifica quando viene creata una nuova raccomandazione da un'analisi.
- `NEW_ASSOCIATION`— Ricevi una notifica quando viene rilevata una nuova anomalia da un'analisi.
- `CLOSED_ASSOCIATION`— Ricevi una notifica quando un'anomalia esistente viene chiusa.
- `SEVERITY_UPGRADED`— Ricevi una notifica quando la gravità di un'analisi viene aggiornata

Per informazioni su come creare una politica di filtro per gli abbonamenti Amazon SNS, consultaPolitiche di filtro degli abbonamenti Amazon SNSnelGuida per gli sviluppatori di Amazon Simple Notification Service. Nella tua politica di filtro, specifichi una delle parole chiave con la politica`MessageType`. Ad esempio, quanto segue apparirebbe in un filtro che specifica l'argomento Amazon SNS: invia notifiche solo quando viene rilevata una nuova anomalia da un'analisi.

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

Esempio di notifica Amazon SNS filtrata per Amazon DevOpsGuru

Di seguito è riportato un esempio di notifica Amazon Simple Notification Service (Amazon SNS) relativa a un argomento Amazon SNS con una politica di filtro. È`MessageType`è impostato

suNEW_ASSOCIATION, quindi invia notifiche solo quando viene rilevata una nuova anomalia da un'analisi.


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

AggiornamentoAWS Systems Managerintegrazione inDevOpsGuru

È possibile abilitare la creazione di un OpsItem per ogni nuova conoscenza diAWS Systems Manager OpsCenter. OpsCenter è un sistema centralizzato in cui è possibile visualizzare, esaminare e rivedere gli elementi di lavoro operativi (OpsItems). La OpsItems for your insights può aiutarti a gestire il lavoro volto a risolvere il comportamento anomalo che ha innescato la creazione di ogni analisi. Per ulteriori informazioni, vedereAWS Systems Manager OpsCentereLavorare con OpsItemnelAWS Systems ManagerGuida per l'utente.

> **Note**
>
> Se si modifica la chiave o il valore del campo tag di un OpsItem, allora DevOpsGuru non è in grado di aggiornarlo OpsItem. Ad esempio, se si modifica il tag di un OpsItem da`"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"`a qualcos'altro, allora DevOpsGuru non può aggiornarlo OpsItem.

Per gestire l'integrazione con Systems Manager

1. Apri Amazon DevOpsConsole Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. NelAWS Systems Managerintegrazione, selezionaAbilita DevOpsGuru per creare unAWS OpstItem nel OpsCenter per ogni approfondimentoavere un OpsItem creato per ogni nuova intuizione. Deselezionalo per smettere di avere un OpsItemcreato per ogni nuova intuizione.

Ti viene addebitato OpsItems creato nel tuo account. Per ulteriori informazioni, consulta Prezzi di AWS Systems Manager.

Aggiornamento del rilevamento delle anomalie nei registri inDevOpsGuru

Per gestire le impostazioni di rilevamento delle anomalie nei registri

1. Apri Amazon DevOpsConsole Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. NelRilevamento di anomalie nei registri, selezionaAbilita il rilevamento delle anomalie nei log concedendo DevOpsAutorizzazioni Guru per visualizzare i dati di registro associati a un'analisi.avereDevOpsGuru visualizza i dati di registro relativi agli approfondimenti.

Aggiornamento delle impostazioni di crittografia inDevOpsGuru

È possibile aggiornare le impostazioni di crittografia da utilizzareAWSchiavi possedute oAWS KMSchiavi gestite dal cliente. Quando si passa a un nuovo cliente gestitoAWS KMSchiave gestita da un cliente esistenteAWS KMSchiave, DevOpsGuru inizia automaticamente a crittografare i metadati appena inseriti utilizzando la nuova chiave. I dati storici rimarranno crittografati con la configurazione precedente gestita dal clienteAWS KMSchiave.

> **Note**
>
> Se revochi la concessione o disabiliti o elimini la precedenteAWS KMSchiave, DevOpsGuru non sarà in grado di accedere a nessuno dei dati crittografati da questa chiave e potresti vedere il`AccessDeniedException`quando si esegue un'operazione di lettura.

Per gestire le impostazioni di crittografia

1. Apri Amazon DevOpsConsole Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. NelCriptazionesezione, scegliModifica la crittografia.
4. Seleziona il tipo di crittografia che desideri utilizzare per proteggere i tuoi dati. Puoi usare un valore predefinitoAWSchiave proprietaria, scegli una chiave gestita dal cliente esistente o creane una nuova gestita dal clienteAWS KMSchiave.
5. Seleziona Salva.

La crittografia è una parte importante di DevOps Guru Security. Per ulteriori informazioni, consulta the section called “Protezione dei dati”.

Visualizzazione delle notifiche

Esistono diversi tipi di notifiche in DevOps Guru.

Argomenti

Le sezioni di questa pagina mostrano esempi di ogni tipo di notifica.

Nuove informazioni

Le notifiche relative a nuovi approfondimenti contengono le seguenti informazioni:


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

Informazioni chiuse

Le notifiche relative agli approfondimenti chiusi contengono le seguenti informazioni:

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

Nuova associazione

Le notifiche per le nuove associazioni contengono le seguenti informazioni:

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

Nuova raccomandazione

Le notifiche relative a nuove raccomandazioni contengono le seguenti informazioni:

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

Severità aggiornata

Le notifiche per gli aggiornamenti di gravità contengono le seguenti informazioni:

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

Errore di convalida delle risorse

Puoi usare AWS CloudFormation pile e AWS tag per filtrare e identificare le AWS risorse che vuoi che DevOps Guru analizzi. Quando scegli uno stack o un tag non valido con cui DevOps Guru deve identificare le risorse, DevOps Guru crea una notifica. `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` Ciò può accadere quando il nome del tag o dello stack specificato non ha risorse associate. Per ottenere il massimo dai metodi di filtraggio DevOps Guru, scegli pile e tag a cui sono associate risorse.

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

Visualizzazione delle risorse analizzate daDevOpsGuru

DevOpsGuru fornisce un elenco dei nomi delle risorse e dei relativi limiti di applicazione in fase di analisi utilizzando il`ListMonitoredResources`azione. Queste informazioni vengono raccolte da AmazonCloudWatch,AWS CloudTraile altroAWSservizi che utilizzanoDevOpsRuolo legato al servizio Guru.

Tieni presente che, anche se un utente non dispone dell'autorizzazione esplicita per accedere alle API di un altro servizio, ad esempioAWS Lambdao Amazon RDS,DevOpsGuru fornisce ancora un elenco di risorse di quel servizio purché`ListMonitoredResources`l'azione è consentita.

Argomenti

- Aggiornamento delAWScopertura dell'analisi inDevOpsGuru
- Rimozione della visualizzazione delle risorse analizzate per gli utenti

Aggiornamento delAWScopertura dell'analisi inDevOpsGuru

Puoi aggiornare qualiAWSrisorse nel tuo accountDevOpsAnalisi Guru. Le risorse che vengono analizzate costituiscono il tuoDevOpsLimite di copertura Guru. Quando si specifica il limite, le risorse vengono raggruppate in applicazioni. Sono disponibili quattro opzioni di copertura perimetrale.

- Scegli di avereDevOpsGuru analizza tutte le risorse supportate nel tuo account. Tutte le risorse del tuo account che sono in uno stack sono raggruppate in un'applicazione. Se hai più stack nel tuo account, le risorse di ogni stack costituiscono la propria applicazione. Se le risorse del tuo account non sono in pila, vengono raggruppate nella rispettiva applicazione.
- Specifica le risorse scegliendoAWS CloudFormationpile che definiscono tali risorse. Se lo fai,DevOpsGuru analizza ogni risorsa specificata negli stack che scegli. Se una risorsa nel tuo account non è definita da uno stack scelto, non viene analizzata. Per ulteriori informazioni, vedereLavorare con gli stacknelAWS CloudFormationGuida per l'utenteeDetermina la copertura per DevOps Guru.
- Specifica le risorse utilizzandoAWSetichette. DevOpsGuru analizza tutte le risorse del tuo account e della tua Regione o tutte le risorse che contengono la chiave di tag che scegli. Le risorse sono raggruppate in base ai valori dei tag selezionati. Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.
- Specifica di non far analizzare alcuna risorsa in modo da non dover più incorrere in addebiti derivanti dall'analisi delle risorse.

> **Note**
>
> Se aggiorni la copertura per interrompere l'analisi delle risorse, potresti continuare a incorrere in addebiti minori se esamini le informazioni esistenti generate daDevOpsGuru in passato. Questi addebiti sono associati alle chiamate API utilizzate per recuperare e visualizzare informazioni dettagliate. Per ulteriori informazioni, vedereAmazonDevOpsPrezzi Guru.

DevOpsGuru supporta tutte le risorse associate ai servizi supportati. Per ulteriori informazioni sui servizi e le risorse supportati, vedereAmazonDevOpsPrezzi Guru.

Per gestire il tuoDevOpsCopertura dell'analisi Guru

1. Apri AmazonDevOpsConsolle Guru pressohttps://console.aws.amazon.com/devops-guru/.
2. EspandiRisorse analizzatenel riquadro di navigazione.
3. Scegliere Modifica.
4. Scegli una delle seguenti opzioni di copertura.

   - ScegliTutte le risorse dell'accountse vuoiDevOpsGuru per analizzare tutte le risorse supportate nel tuoAWSaccount e regione. Se scegli questa opzione,AWSl'account è il limite di copertura dell'analisi delle risorse. Tutte le risorse di ogni stack del tuo account sono raggruppate nella rispettiva applicazione. Tutte le risorse rimanenti che non sono in uno stack vengono raggruppate nella rispettiva applicazione.
   - ScegliCloudFormationpilese vuoiDevOpsGuru per analizzare le risorse che si trovano negli stack che scegli, quindi scegli una delle seguenti opzioni.
     - Tutte le risorse— Tutte le risorse presenti nel tuo account vengono analizzate. Le risorse in ogni stack sono raggruppate nella rispettiva applicazione. Le risorse del tuo account che non sono in pila non vengono analizzate.
     - Seleziona pile— Seleziona le pile che desideriDevOpsGuru da analizzare. Le risorse in ogni stack selezionato sono raggruppate nella rispettiva applicazione. Puoi inserire il nome di una pila inTrova pileper individuare rapidamente uno stack specifico. Puoi selezionare fino a 1.000 pile.

     Per ulteriori informazioni, consulta Utilizzo diAWS CloudFormationpile per identificare le risorse nel tuo DevOpsApplicazioni Guru.

- ScegliEtichettese vuoiDevOpsGuru per analizzare tutte le risorse che contengono i tag che scegli. Scegli unchiave, quindi scegli una delle seguenti opzioni.
  - Tutte le risorse dell'account—Analizza tutte le risorse AWS nella regione e nell'account correnti. Le risorse con la chiave tag selezionata sono raggruppate in base al valore del tag, se presente. Le risorse senza questa chiave di tag vengono raggruppate e analizzate separatamente.
  - Scegli valori di tag specifici— Tutte le risorse che contengono un tag conchiaveche hai scelto vengono analizzati. DevOpsGuru raggruppa le tue risorse in applicazioni in base ai tuoi tagvalori.

  I tagchiavedeve iniziare con il prefissodevops-guru-. Questo prefisso non fa distinzione tra maiuscole e minuscole. Ad esempio, un validochiaveèDevOps-Guru-Production-Applications. Per ulteriori informazioni, consulta Utilizzo dei tag per identificare le risorse nelle applicazioni DevOps Guru.
- ScegliNessunose non vuoiDevOpsGuru per analizzare qualsiasi risorsa. Questa opzione disabilitaDevOpsGuru in modo da smettere di incorrere in addebiti derivanti dall'analisi delle risorse.

5. Seleziona Salva.

Rimozione della visualizzazione delle risorse analizzate per gli utenti

Anche se un utente non dispone dell'autorizzazione esplicita per accedere alle API di un altro servizio come Lambda o Amazon RDS,DevOpsGuru fornisce ancora un elenco di risorse di quel servizio purchéListMonitoredResourcesl'azione è consentita. Per modificare questo comportamento, puoi aggiornare il tuoAWSPolitica IAM per negare questa azione.

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

Best practice in DevOps Guru

Le seguenti best practice possono aiutarti a comprendere, diagnosticare e correggere comportamenti anomali rilevati da Amazon DevOps Guru. Usa Best practice conComprendere gli approfondimenti inDevOpsConsolle Guruper risolvere i problemi operativi rilevati da DevOps Guru.

- Nella vista della timeline di una panoramica, guarda prima le metriche evidenziate. Spesso sono indicatori chiave del problema.
- Utilizza Amazon CloudWatch per visualizzare le metriche che si sono verificate immediatamente prima della prima metrica evidenziata in un approfondimento per individuare quando e come è cambiato il comportamento. Questo può aiutarti a diagnosticare e risolvere il problema.
- Per le risorse Amazon RDS, consulta le metriche di Performance Insights. Correlando le metriche del contatore con il caricamento del database, è possibile ottenere informazioni dettagliate sui problemi di prestazioni. Per ulteriori informazioni, consultaAnalisi delle anomalie delle prestazioni con DevOps Gurufor Amazon RDS.
- Le dimensioni multiple della stessa metrica possono spesso essere anomale. Osservate le dimensioni nella vista grafica per avere una comprensione più approfondita del problema.
- Consulta la sezione eventi di un approfondimento per gli eventi di distribuzione o infrastruttura che si sono verificati nel momento in cui è stata creata l'analisi. Conoscere quali eventi si sono verificati quando si è verificato un comportamento anomalo di un'intuizione può aiutarti a capire e diagnosticare il problema.
- Cerca i ticket nel tuo sistema operativo che si sono verificati nello stesso periodo di una panoramica per gli indizi.
- In un approfondimento, leggi i consigli e visita i link nei consigli. Questi spesso includono passaggi per la risoluzione dei problemi che possono aiutarti a diagnosticare e risolvere rapidamente i problemi.
- Non ignorare le informazioni risolte a meno che tu non abbia già risolto il problema. Una volta al giorno, guarda nuove intuizioni, anche se sono state risolte. Cerca di capire la causa principale dietro il maggior numero possibile di intuizioni. Cerca uno schema che potrebbe essere il segno di un problema sistemico. Se un problema sistemico viene lasciato irrisolto, potrebbe causare problemi più gravi in futuro. Risolvere i problemi transitori ora può aiutare a prevenire incidenti futuri, più gravi.

Sicurezza in Amazon DevOps Guru

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon DevOps Guru, consulta AWS Services in Scope by Compliance Program .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi DevOps Guru. I seguenti argomenti mostrano come configurare DevOps Guru per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a usare altri servizi AWS che ti aiutano a monitorare e proteggere le tue risorse DevOps Guru.

Argomenti

Protezione dei dati in Amazon DevOps Guru

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon DevOps Guru. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i AWS servizi utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con DevOps Guru o altri utenti AWS servizi utilizzando la console, l'API o gli SDK. AWS CLI AWS I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati in Guru DevOps

La crittografia è una parte importante della sicurezza di DevOps Guru. Alcune crittografie, ad esempio per i dati in transito, sono fornite di default e non richiedono alcuna operazione da parte dell'utente. Altre forme di crittografia, ad esempio per i dati inattivi, possono essere configurate durante la creazione del progetto o della build.

- Crittografia dei dati in transito: tutte le comunicazioni tra clienti e DevOps Guru e tra DevOps Guru e le sue dipendenze a valle sono protette tramite TLS e autenticate utilizzando il processo di firma Signature Version 4. Tutti DevOps gli endpoint Guru utilizzano certificati gestiti da. AWS Private Certificate Authority Per ulteriori informazioni consulta la pagina relativa al processo di firma Signature Version 4 e la pagina Che cos'è ACM PCA.
- Crittografia dei dati inattivi: per tutte le AWS risorse analizzate da DevOps Guru, i CloudWatch parametri e i dati di Amazon, gli ID delle risorse e AWS CloudTrail gli eventi vengono archiviati utilizzando Amazon S3, Amazon DynamoDB e Amazon Kinesis. Se si utilizzano AWS CloudFormation gli stack per definire le risorse analizzate, vengono raccolti anche i dati dello stack. DevOpsGuru utilizza le politiche di conservazione dei dati di Amazon S3, DynamoDB e Kinesis. I dati archiviati in Kinesis possono essere conservati per un massimo di un anno e dipendono dalle politiche impostate. I dati archiviati in Amazon S3 e DynamoDB vengono archiviati per un anno.

  I dati archiviati vengono crittografati utilizzando le funzionalità di data-at-rest crittografia di Amazon S3, DynamoDB e Kinesis.

  Chiavi gestite dal cliente: DevOps Guru supporta la crittografia dei contenuti dei clienti e dei metadati sensibili, come le anomalie dei log generate dai registri con chiavi gestite dal cliente. CloudWatch Questa funzionalità offre la possibilità di aggiungere un livello di sicurezza autogestito per aiutarti a soddisfare i requisiti di conformità e normativi della tua organizzazione. Per informazioni sull'attivazione delle chiavi gestite dai clienti nelle impostazioni DevOps Guru, consulta. the section called “Aggiornamento della crittografia”

  Avendo il pieno controllo di questo livello di crittografia, è possibile eseguire operazioni quali:

  - Stabilire e mantenere le policy delle chiavi
  - Stabilire e mantenere le policy e le sovvenzioni IAM
  - Abilitare e disabilitare le policy delle chiavi
  - Ruotare i materiali crittografici delle chiavi
  - Aggiungere tag
  - Creare alias delle chiavi

- Pianificare l’eliminazione delle chiavi

Per ulteriori informazioni, consulta Customer managed keys nella AWS Key Management Service Developer Guide.

> **Note**
>
> DevOpsGuru abilita automaticamente la crittografia a riposo utilizzando chiavi AWS proprietarie per proteggere gratuitamente i metadati sensibili. Tuttavia, l'utilizzo di una chiave gestita dal cliente comporta dei AWS KMS costi. Per ulteriori informazioni sui prezzi, consulta i AWS Key Management Service prezzi.

In che modo DevOps Guru utilizza le sovvenzioni in AWS KMS

DevOpsGuru richiede una concessione per utilizzare la chiave gestita dal cliente.

Quando scegli di abilitare la crittografia con una chiave gestita dal cliente, DevOps Guru crea una concessione per tuo conto inviando una CreateGrant richiesta a. AWS KMS Le sovvenzioni AWS KMS vengono utilizzate per consentire a DevOps Guru di accedere a una AWS KMS chiave in un account cliente.

DevOpsGuru richiede la concessione per utilizzare la chiave gestita dal cliente per le seguenti operazioni interne:

- Invia DescribeKey richieste AWS KMS a per verificare che l'ID della chiave KMS simmetrica gestita dal cliente inserito durante la creazione di un tracker o di una raccolta di geofence sia valido.
- Invia GenerateDataKey richieste per generare chiavi dati AWS KMS crittografate dalla chiave gestita dal cliente.
- Invia le richieste Decrypt a per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati.

Puoi revocare l'accesso alla concessione o rimuovere l'accesso del servizio alla chiave gestita dal cliente in qualsiasi momento. Se lo fai, DevOps Guru non sarà in grado di accedere a nessuno dei dati crittografati dalla chiave gestita dal cliente, il che influirà sulle operazioni che dipendono da quei dati. Ad esempio, se si tenta di ottenere informazioni crittografate sulle anomalie di registro a cui DevOps Guru non può accedere, l'operazione restituirà un errore. AccessDeniedException

Monitoraggio delle chiavi di crittografia in Guru DevOps

Quando utilizzi una chiave gestita AWS KMS dal cliente con le tue risorse DevOps Guru, puoi usare AWS CloudTrail or CloudWatch Logs per tenere traccia delle richieste a cui DevOps Guru invia. AWS KMS

Creazione di una chiave gestita dal cliente

Puoi creare una chiave simmetrica gestita dal cliente utilizzando le o le API. AWS Management Console AWS KMS

Per creare una chiave simmetrica gestita dal cliente, consulta Creazione di chiavi KMS con crittografia simmetrica.

Policy della chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta Autenticazione e controllo degli accessi nella Guida per gli AWS KMS sviluppatori. AWS Key Management Service

Per utilizzare la chiave gestita dal cliente con le risorse DevOps Guru, nella policy chiave devono essere consentite le seguenti operazioni API:

- `kms:CreateGrant`: aggiunge una concessione a una chiave gestita dal cliente. Concede l'accesso di controllo a una AWS KMS chiave specificata, che consente l'accesso alle operazioni di concessione richieste da DevOps Guru. Per ulteriori informazioni sull'utilizzo delle sovvenzioni, consulta la AWS Key Management Service Guida per gli sviluppatori.

Ciò consente a DevOps Guru di fare quanto segue:

- Chiama GenerateDataKey per generare una chiave dati crittografata e archiviarla, poiché la chiave dati non viene utilizzata immediatamente per crittografare.
- Chiama Decrypt per utilizzare la chiave dati crittografata memorizzata per accedere ai dati crittografati.
- Configura un preside in pensione per consentire al servizio di farlo. RetireGrant
- Usa kms: DescribeKey per fornire i dettagli chiave gestiti dal cliente per consentire a DevOps Guru di convalidare la chiave.

La seguente dichiarazione include esempi di dichiarazioni politiche che è possibile aggiungere per Guru: DevOps

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

Privacy del traffico

Puoi migliorare la sicurezza dell'analisi delle risorse e della generazione di informazioni configurando DevOps Guru per utilizzare un endpoint VPC di interfaccia. Per far ciò, non hai bisogno di un gateway Internet, di un dispositivo NAT o di un gateway privato virtuale. Inoltre, non è necessario configurarlo PrivateLink, sebbene sia consigliato. Per ulteriori informazioni, consulta DevOpsEndpoint VPC Guru e interfaccia ()AWS PrivateLink. Per ulteriori informazioni sugli endpoint VPC, consulta PrivateLink e AWS PrivateLinkAccesso ai servizi AWS tramite. PrivateLink

Identity and Access Management per Amazon DevOps Guru

AWS Identity and Access Management (IAM) è uno strumento AWS servizio che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Guru. DevOps IAM è uno strumento AWS servizio che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- DevOpsGuru aggiorna le politiche AWS gestite e il ruolo collegato ai servizi
- Come funziona Amazon DevOps Guru con IAM
- Politiche basate sull'identità per Amazon Guru DevOps
- Utilizzo di ruoli collegati ai servizi per Guru DevOps
- Riferimento alle autorizzazioni di Amazon DevOps Guru
- Autorizzazioni per argomenti di Amazon SNS
- Autorizzazioni per argomenti AWS KMS Amazon SNS crittografati

- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DevOps Guru

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che svolgi in DevOps Guru.

Utente del servizio: se utilizzi il servizio DevOps Guru per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di DevOps Guru per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di DevOps Guru, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DevOps Guru

Amministratore del servizio: se sei responsabile delle risorse DevOps Guru della tua azienda, probabilmente hai pieno accesso a DevOps Guru. Il tuo compito è determinare a quali funzionalità e risorse DevOps Guru devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con DevOps Guru, consulta. Come funziona Amazon DevOps Guru con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso a DevOps Guru. Per visualizzare esempi di policy basate sull'identità di DevOps Guru che puoi utilizzare in IAM, consulta. Politiche basate sull'identità per Amazon Guru DevOps

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte AWS servizi le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere AWS servizi utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le AWS servizi credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni AWS servizi, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni AWS servizi utilizzano le funzionalità di altri AWS servizi. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an AWS servizio, combinate con la richiesta AWS servizio per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I

ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per sapere come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

DevOpsGuru aggiorna le politiche AWS gestite e il ruolo collegato ai servizi

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite e al ruolo collegato ai servizi per DevOps Guru da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS di Guru. DevOps AmazonDevOpsStoria dei documenti Guru

Modifica	Descrizione	Data
AmazonDevOpsGuruConsoleFullAccess: aggiorna a una policy esistente.	La policy `AmazonDevOpsGuruFullAccess` gestita ora supporta gli abbonamenti Amazon SNS.	9 agosto 2023
AmazonDevOpsGuruReadOnlyAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruReadOnlyAccess` gestita ora supporta l'accesso in sola lettura agli elenchi di abbonamenti Amazon SNS.	9 agosto 2023
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora supporta l'accesso alle azioni GET di API Gateway sulle API REST.	11 gennaio 2023
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora supporta diverse azioni di Amazon Simple Storage Service e Service Quotas.	19 ottobre 2022

Modifica	Descrizione	Data
AmazonDevOpsGuruFullAccess: aggiornamento a una policy esistente	La policy gestita `AmazonDevOpsGuruFullAccess` ora supporta l'accesso all'azione. CloudWatch `FilterLogEvents`	30 agosto 2022
AmazonDevOpsGuruConsoleFullAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruConsoleFullAccess` gestita ora supporta l'accesso all' CloudWatch `FilterLogEvents` azione.	30 agosto 2022
AmazonDevOpsGuruReadOnlyAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruReadOnlyAccess` gestita ora supporta l'accesso in sola lettura all'azione CloudWatch `FilterLogEvents` .	30 agosto 2022
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora supporta le azioni di CloudWatch registro e. `FilterLogEvents` `DescribeLogGroups` `DescribeLogStreams`	12 luglio 2022
Politiche basate sull'identità per DevOps Guru: nuova politica gestita.	La `AmazonDevOpsGuruConsoleFullAccess` politica è stata aggiunta.	16 dicembre 2021

Modifica	Descrizione	Data
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora supporta le azioni Performance Insights `DescribeMetricsKeys` e Amazon `DescribeDBInstances` RDS.	1° dicembre 2021
AmazonDevOpsGuruReadOnlyAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruReadOnlyAccess` gestita ora supporta l'accesso in sola lettura alle azioni di Amazon `DescribeDBInstances` RDS.	1° dicembre 2021
AmazonDevOpsGuruFullAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruFullAccess` gestita ora supporta l'accesso alle `DescribeDBInstances` azioni di Amazon RDS.	1° dicembre 2021

Modifica	Descrizione	Data
Politiche basate sull'identità per Amazon Guru DevOps— Aggiunta una nuova policy.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora supporta l'accesso alle azioni di Amazon RDS e Performance Insights. `DescribeDBInstances` `GetResourceMetrics` La policy `AmazonDevOpsGuruOrganizationsAccess` gestita fornisce l'accesso a DevOps Guru all'interno di un'organizzazione.	16 novembre 2021
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato ai servizi ora supporta AWS Organizations.	4 novembre 2021
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato ai servizi ora contiene nuove condizioni sulle azioni e. `ssm:CreateOpsItem` `ssm:AddTagsToResource`	11 ottobre 2021

Modifica	Descrizione	Data
Autorizzazioni di ruolo collegate al servizio per Guru DevOps: aggiorna a una policy esistente.	Il ruolo `AWSServiceRoleForDevOpsGuru` collegato al servizio ora contiene nuove condizioni sulle azioni e. `ssm:CreateOpsItem` `ssm:AddTagsToResource`	14 giugno 2021
AmazonDevOpsGuruReadOnlyAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruReadOnlyAccess` gestita ora consente l'accesso in sola lettura alle azioni AWS Identity and Access Management `GetRole` e alle azioni Guru. DevOps `DescribeFeedback`	14 giugno 2021
AmazonDevOpsGuruReadOnlyAccess: aggiornamento a una policy esistente	La policy `AmazonDevOpsGuruReadOnlyAccess` gestita ora consente l'accesso in sola lettura al Guru e alle azioni. DevOps `GetCostEstimation` `StartCostEstimation`	27 aprile 2021
AmazonDevOpsGuruServiceRolePolicy: aggiorna a una policy esistente.	Il `AWSServiceRoleForDevOpsGuru` ruolo ora consente l'accesso alle azioni AWS Systems Manager `AddTagsToResource` e alle azioni di Auto `DescribeAutoScalingGroups` Scaling di Amazon EC2.	27 aprile 2021

Modifica	Descrizione	Data
DevOpsGuru ha iniziato a tracciare le modifiche	DevOpsGuru ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	10 dicembre 2020

Come funziona Amazon DevOps Guru con IAM

Prima di utilizzare IAM per gestire l'accesso a DevOps Guru, scopri quali funzionalità IAM sono disponibili per l'uso con DevOps Guru.

Funzionalità IAM che puoi usare con Amazon DevOps Guru

Funzionalità IAM	DevOpsSupporto Guru
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
☻Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione generale di come DevOps Guru e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Guru DevOps

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per Guru DevOps

Per visualizzare esempi di politiche basate sull'identità di DevOps Guru, vedi. Politiche basate sull'identità per Amazon Guru DevOps

Politiche basate sulle risorse all'interno di Guru DevOps

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. AWS servizi

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per DevOps Guru

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni DevOps Guru, consulta Azioni definite da Amazon DevOps Guru nel Service Authorization Reference.

Le azioni politiche in DevOps Guru utilizzano il seguente prefisso prima dell'azione:

```
aws
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

```
      "aws:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di DevOps Guru, consulta. Politiche basate sull'identità per Amazon Guru DevOps

Risorse politiche per Guru DevOps

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse DevOps Guru e dei relativi ARN, consulta Risorse definite da Amazon DevOps Guru nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon DevOps Guru.

Per visualizzare esempi di politiche basate sull'identità di DevOps Guru, consulta. Politiche basate sull'identità per Amazon Guru DevOps

Chiavi relative alle condizioni delle policy per Guru DevOps

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione DevOps Guru, consulta Condition keys for Amazon DevOps Guru nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon DevOps Guru.

Per visualizzare esempi di politiche basate sull'identità di DevOps Guru, consulta. Politiche basate sull'identità per Amazon Guru DevOps

Liste di controllo degli accessi (ACL) in Guru DevOps

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Controllo degli accessi basato sugli attributi (ABAC) con Guru DevOps

Supporta ABAC (tag nelle policy)	No

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con DevOps Guru

Supporta le credenziali temporanee	Sì

Alcune AWS servizi non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che AWS servizi funzionano con credenziali temporanee, consulta la sezione relativa alla AWS servizi compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente

e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Guru DevOps

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an AWS servizio, in combinazione con la richiesta AWS servizio per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri AWS servizi o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per DevOps Guru

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di DevOps Guru. Modifica i ruoli di servizio solo quando DevOps Guru fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Guru DevOps

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. AWS servizio Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Politiche basate sull'identità per Amazon Guru DevOps

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse Guru. DevOps Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o l' AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da DevOps Guru, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon DevOps Guru nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Guru DevOps
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Policy AWS gestite (predefinite) per DevOps Guru

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare DevOps le risorse Guru nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico AWS servizio, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Guru DevOps

Per accedere alla console Amazon DevOps Guru, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse DevOps Guru presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console DevOps Guru, collega anche il DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` o la policy `AmazonDevOpsGuruFullAccess` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Policy AWS gestite (predefinite) per DevOps Guru

AWS affronta molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da. AWS Queste policy AWS gestite concedono le autorizzazioni necessarie per i casi d'uso comuni, in modo da evitare di dover verificare quali autorizzazioni sono necessarie. Per ulteriori informazioni, consulta Policy gestite AWS nella Guida per gli utenti di IAM.

Per creare e gestire i ruoli del servizio DevOps Guru, devi anche allegare la policy -managed denominata AWS. `IAMFullAccess`

Puoi anche creare le tue policy IAM personalizzate per consentire le autorizzazioni per le azioni e le risorse di DevOps Guru. Puoi collegare queste policy personalizzate agli utenti o ai gruppi che richiedono le autorizzazioni.

Le seguenti politiche AWS gestite, che puoi allegare agli utenti del tuo account, sono specifiche di Guru. DevOps

Argomenti

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess`— Fornisce l'accesso completo a DevOps Guru, incluse le autorizzazioni per creare argomenti Amazon SNS, accedere ai parametri di CloudWatch Amazon e agli stack di accesso. AWS CloudFormation Applicalo solo agli utenti di livello amministrativo a cui desideri concedere il pieno controllo su Guru. DevOps

La `AmazonDevOpsGuruFullAccess` politica contiene la seguente dichiarazione.

```
{
    "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`— Fornisce l'accesso completo a DevOps Guru, incluse le autorizzazioni per creare argomenti Amazon SNS, accedere ai parametri di CloudWatch Amazon e agli stack di accesso. AWS CloudFormation Questa policy offre ulteriori autorizzazioni di analisi delle prestazioni che consentono di visualizzare analisi dettagliate relative alle istanze database di Amazon RDS Aurora anomale nella console. Applicala solo agli utenti di livello amministrativo a cui desideri concedere il pieno controllo su Guru. DevOps

La `AmazonDevOpsGuruConsoleFullAccess` politica contiene la seguente dichiarazione.

```
{
    "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`— Garantisce l'accesso in sola lettura a DevOps Guru e alle risorse correlate in altri servizi. AWS Applica questa politica agli utenti a cui desideri concedere la possibilità di visualizzare le informazioni, ma non apportare aggiornamenti al limite di copertura dell'analisi di DevOps Guru, agli argomenti di Amazon SNS o all'integrazione di Systems Manager. OpsCenter

La `AmazonDevOpsGuruReadOnlyAccess` policy contiene la seguente dichiarazione.

```
{
"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`— Fornisce agli amministratori dell'organizzazione l'accesso alla visualizzazione multi-account DevOps Guru all'interno di un'organizzazione. Applica questa politica agli utenti a livello di amministratore della tua organizzazione ai quali desideri concedere l'accesso completo a Guru all'interno di un'organizzazione. DevOps Puoi applicare questa politica nell'account di gestione e nell'account amministratore delegato della tua organizzazione per Guru. DevOps Puoi applicare `AmazonDevOpsGuruReadOnlyAccess` o `AmazonDevOpsGuruFullAccess` aggiungere questa politica per fornire l'accesso completo o di sola lettura a Guru. DevOps

La `AmazonDevOpsGuruOrganizationsAccess` politica contiene la seguente dichiarazione.

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

Utilizzo di ruoli collegati ai servizi per Guru DevOps

Amazon DevOps Guru utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Guru. DevOps I ruoli collegati ai servizi sono predefiniti da DevOps Guru e includono tutte le autorizzazioni richieste dal servizio per chiamare AWS CloudTrail Amazon CloudWatch AWS CodeDeploy e AWS X-Ray AWS Organizations per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di DevOps Guru perché non è necessario aggiungere manualmente le autorizzazioni necessarie. DevOpsGuru definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Guru può assumerne i ruoli. DevOps Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questo protegge le tue risorse DevOps Guru perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Autorizzazioni di ruolo collegate al servizio per Guru DevOps

DevOpsGuru utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForDevOpsGuru` Questa è una politica AWS gestita con autorizzazioni specifiche che DevOps Guru deve eseguire nel tuo account.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForDevOpsGuru` considera attendibile il seguente servizio:

- `devops-guru.amazonaws.com`

La politica di autorizzazione dei ruoli `AmazonDevOpsGuruServiceRolePolicy` consente a DevOps Guru di completare le seguenti azioni sulle risorse specificate.

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

Creazione di un ruolo collegato al servizio per Guru DevOps

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei una panoramica sulla AWS Management Console, la o l' AWS API AWS CLI, DevOps Guru crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nel tuo account se hai completato un'azione in un altro servizio che utilizza le funzionalità supportate da questo ruolo; ad esempio, può apparire se hai aggiunto DevOps Guru a un repository di. AWS CodeCommit

Modifica di un ruolo collegato al servizio per Guru DevOps

DevOpsGuru non consente di modificare il ruolo collegato al servizio. `AWSServiceRoleForDevOpsGuru` Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne

la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Guru DevOps

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario dissociarsi da tutti i repository prima di poterlo eliminare manualmente.

> **Note**
>
> Se il servizio DevOps Guru utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al `AWSServiceRoleForDevOpsGuru` servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Riferimento alle autorizzazioni di Amazon DevOps Guru

Puoi utilizzare le chiavi di condizione AWS-wide nelle tue politiche DevOps Guru per esprimere condizioni. Per un elenco, consulta IAM JSON Policy Elements Reference nella IAM User Guide.

Puoi specificare le operazioni nel campo `Action` della policy. Per specificare un'operazione, utilizza il prefisso `devops-guru:` seguito dal nome dell'operazione API (ad esempio, `devops-guru:SearchInsights` and `devops-guru:ListAnomalies`). Per specificare più operazioni in una sola istruzione, separa ciascuna di esse con una virgola (ad esempio, `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

Utilizzo di caratteri jolly

Specifichi un Amazon Resource Name (ARN), con o senza un carattere jolly (*), come valore della risorsa nel campo della policy. `Resource` È possibile utilizzare un carattere jolly per specificare più

operazioni o risorse. Ad esempio, `devops-guru:*` specifica tutte le azioni DevOps Guru e `devops-guru:List*` specifica tutte le azioni DevOps Guru che iniziano con la parola. `List` L'esempio seguente si riferisce a tutti gli approfondimenti con un identificatore univoco universale (UUID) che inizia con. `12345`

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

È possibile utilizzare la tabella seguente come riferimento quando si impostano Autenticazione con identità e si scrivono politiche di autorizzazione da allegare a un'identità IAM (politiche basate sull'identità).

DevOpsOperazioni dell'API Guru e autorizzazioni richieste per le azioni

`AddNotificationChannel`

Operazione: `devops-guru:AddNotificationChannel`

Necessario per aggiungere un canale di notifica da DevOps Guru. Un canale di notifica viene utilizzato per avvisarti quando DevOps Guru genera un'analisi contenente informazioni su come migliorare le tue operazioni.

Risorsa: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Necessario per rimuovere un canale di notifica da DevOps Guru. Un canale di notifica viene utilizzato per avvisarti quando DevOps Guru genera un'analisi contenente informazioni su come migliorare le tue operazioni.

Risorsa: *

`ListNotificationChannels`

Operazione: `devops-guru:ListNotificationChannels`

Necessario per restituire un elenco di canali di notifica configurati per DevOps Guru. Ogni canale di notifica viene utilizzato per avvisarti quando DevOps Guru genera un'analisi contenente informazioni su come migliorare le tue operazioni. L'unico tipo di notifica supportato è Amazon Simple Notification Service.

Risorsa: *

`UpdateResourceCollectionFilter`

Operazione: `devops-guru:UpdateResourceCollectionFilter`

Necessario per aggiornare l'elenco degli AWS CloudFormation stack utilizzati per specificare quali AWS risorse del tuo account vengono analizzate da DevOps Guru. L'analisi genera approfondimenti che includono consigli, metriche operative ed eventi operativi che puoi utilizzare per migliorare le prestazioni delle tue operazioni. Questo metodo crea anche i ruoli IAM necessari per l'utilizzo CodeGuru OpsAdvisor.

Risorsa: *

`GetResourceCollectionFilter`

Operazione: `devops-guru:GetResourceCollectionFilter`

Obbligatorio per restituire l'elenco degli AWS CloudFormation stack utilizzati per specificare quali AWS risorse del tuo account vengono analizzate da DevOps Guru. L'analisi genera approfondimenti che includono consigli, metriche operative ed eventi operativi che puoi utilizzare per migliorare le prestazioni delle tue operazioni.

Risorsa: *

`ListInsights`

Operazione: `devops-guru:ListInsights`

Necessario per restituire un elenco di informazioni dettagliate nel tuo AWS account. Puoi specificare quali approfondimenti vengono restituiti in base all'ora di inizio, allo stato (`ongoingoany`) e al tipo (`reactiveopredictive`).

Risorsa: *

`DescribeInsight`

Operazione: `devops-guru:DescribeInsight`

Necessario per restituire i dettagli su un'analisi specificata utilizzando il relativo ID.

Risorsa: *

`SearchInsights`

Operazione: `devops-guru:SearchInsights`

Necessario per restituire un elenco di approfondimenti nel tuo AWS account. Puoi specificare quali approfondimenti vengono restituiti in base all'ora di inizio, ai filtri e al tipo (`reactiveopredictive`).

Risorsa: *

`ListAnomalies`

Operazione: `devops-guru:ListAnomalies`

Obbligatorio per restituire un elenco delle anomalie che appartengono a un'analisi specificata utilizzando il relativo ID.

Risorsa: *

`DescribeAnomaly`

Operazione: `devops-guru:DescribeAnomaly`

Obbligatorio per restituire i dettagli su un'anomalia specificata utilizzando il relativo ID.

Risorsa: *

`ListEvents`

Operazione: `devops-guru:ListEvents`

Obbligatorio per restituire un elenco degli eventi emessi dalle risorse valutate da Guru. DevOps È possibile utilizzare i filtri per specificare quali eventi vengono restituiti.

Risorsa: *

`ListRecommendations`

Operazione: `devops-guru:ListRecommendations`

Necessario per restituire un elenco dei consigli di uno specifico approfondimento. Ogni raccomandazione include un elenco di metriche e un elenco di eventi correlati ai consigli.

Risorsa: *

`DescribeAccountHealth`

Operazione: `devops-guru:DescribeAccountHealth`

Necessario per restituire il numero di approfondimenti reattivi aperti, il numero di approfondimenti predittivi aperti e il numero di metriche analizzate nel tuo account. AWS Usa questi numeri per valutare lo stato delle operazioni del tuo account. AWS

Risorsa: *

`DescribeAccountOverview`

Operazione: `devops-guru:DescribeAccountOverview`

Necessario per restituire quanto segue che si è verificato in un intervallo di tempo: il numero di approfondimenti reattivi aperti che sono stati creati, il numero di approfondimenti predittivi aperti che sono stati creati e il tempo medio di recupero (MTTR) per tutti gli approfondimenti reattivi che sono stati chiusi.

Risorsa: *

`DescribeResourceCollectionHealthOverview`

Operazione: `devops-guru:DescribeResourceCollectionHealthOverview`

Necessario per restituire il numero di approfondimenti predittivi aperti, approfondimenti reattivi aperti e il tempo medio di recupero (MTTR) per tutti gli approfondimenti per ogni stack specificato in Guru. AWS CloudFormation DevOps

Risorsa: *

`DescribeIntegratedService`

Operazione: `devops-guru:DescribeIntegratedService`

Necessario per restituire lo stato di integrazione dei servizi che possono essere integrati con Guru. DevOps L'unico servizio che può essere integrato con DevOps Guru è quello AWS Systems Manager che può essere utilizzato per creare una visione OpsItem per ogni intuizione generata.

Risorsa: *

`UpdateIntegratedServiceConfig`

Operazione: `devops-guru:UpdateIntegratedServiceConfig`

Necessario per abilitare o disabilitare l'integrazione con un servizio che può essere integrato con DevOps Guru. L'unico servizio che può essere integrato con DevOps Guru è Systems Manager, che può essere utilizzato per creare una visione OpsItem per ogni analisi generata.

Risorsa: *

Autorizzazioni per argomenti di Amazon SNS

Utilizza le informazioni in questo argomento solo se desideri configurare Amazon DevOps Guru per inviare notifiche agli argomenti Amazon SNS di proprietà di AWS un altro account.

DevOps DevOpsAffinché Guru invii notifiche a un argomento Amazon SNS di proprietà di un altro account, devi allegare all'argomento Amazon SNS una policy che conceda a Guru le autorizzazioni per inviargli notifiche. Se configuri DevOps Guru per inviare notifiche agli argomenti di Amazon SNS di proprietà dello stesso account che usi DevOps per Guru, DevOps Guru aggiunge una policy agli argomenti per te.

Dopo aver allegato una policy per configurare le autorizzazioni per un argomento Amazon SNS in un altro account, puoi aggiungere l'argomento Amazon SNS in Guru. DevOps Puoi anche aggiornare la tua policy di Amazon SNS con un canale di notifica per renderla più sicura.

> **Note**
>
> DevOpsAttualmente Guru supporta solo l'accesso tra più account nella stessa regione.

Argomenti

Configurazione delle autorizzazioni per un argomento di Amazon SNS in un altro account

Aggiungere autorizzazioni come ruolo IAM

Per utilizzare un argomento Amazon SNS da un altro account dopo aver effettuato l'accesso con un ruolo IAM, devi allegare una policy all'argomento Amazon SNS che desideri utilizzare. Per allegare una policy a un argomento Amazon SNS da un altro account mentre utilizzi un ruolo IAM, devi disporre delle seguenti autorizzazioni per quella risorsa dell'account come parte del tuo ruolo IAM:

- sns: CreateTopic
- sms: GetTopicAttributes
- sms: SetTopicAttributes

- sns:Publish

Allega la seguente policy all'argomento di Amazon SNS che desideri utilizzare. Per la `Resource` chiave, *`topic-owner-account-id`*è l'ID dell'account del proprietario dell'argomento, *`topic-sender-account-id`*è l'ID dell'account dell'utente che ha configurato DevOps Guru e *`devops-guru-role`*il ruolo IAM del singolo utente coinvolto. È necessario sostituire *`region-id`* con valori appropriati (ad esempio,`us-west-2`) e. *`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"]
            }
        }
    ]
}
```

Aggiungere autorizzazioni come utente IAM

Per utilizzare un argomento Amazon SNS da un altro account come utente IAM, allega la seguente policy all'argomento Amazon SNS che desideri utilizzare. La `Resource` chiave *`topic-owner-`*

*account-id*è l'ID dell'account del proprietario dell'argomento, *topic-sender-account-id*l'ID dell'account dell'utente che ha configurato DevOps Guru e *devops-guru-user-name*il singolo utente IAM coinvolto. È necessario sostituire i valori appropriati per *region-id* (ad esempio,) e. `us-west-2` *my-topic-name*

> **Note**
>
> Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

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

```
}
```

Aggiungere un argomento Amazon SNS da un altro account

Dopo aver configurato le autorizzazioni per un argomento Amazon SNS in un altro account, puoi aggiungere quell'argomento Amazon SNS alle DevOps impostazioni di notifica di Amazon SNS. Puoi aggiungere l'argomento Amazon SNS utilizzando la console AWS CLI o la console DevOps Guru.

- Quando si utilizza la console, è necessario selezionare l'opzione Usa un argomento SNS ARN per specificare un argomento esistente in modo da utilizzare un argomento di un altro account.
- Quando si utilizza l' AWS CLI operazione add-notification-channel, è necessario specificare l'elemento `TopicArn` all'interno dell'`NotificationChannelConfig`oggetto.

Aggiungi un argomento Amazon SNS da un altro account utilizzando la console

1. Apri la console Amazon DevOps Guru all'indirizzo https://console.aws.amazon.com/devops-guru/.
2. Apri il pannello di navigazione, quindi scegli Impostazioni.
3. Vai alla sezione Notifiche e scegli Modifica.
4. Scegli Aggiungi argomento SNS.
5. Scegli Usa un argomento SNS ARN per specificare un argomento esistente.
6. Inserisci l'ARN dell'argomento Amazon SNS che desideri utilizzare. Dovresti aver già configurato le autorizzazioni per questo argomento allegandovi una policy.
7. (Facoltativo) Scegliete Configurazione delle notifiche per modificare le impostazioni della frequenza delle notifiche.
8. Selezionare Salva.

Dopo aver aggiunto l'argomento Amazon SNS alle impostazioni di notifica, DevOps Guru lo utilizza per informarti di eventi importanti, ad esempio quando viene creata una nuova analisi.

Aggiornamento della policy di Amazon SNS con un canale di notifica (consigliato)

Dopo aver aggiunto un argomento, ti consigliamo di rendere più sicura la tua politica specificando le autorizzazioni solo per il canale di notifica DevOps Guru che contiene l'argomento.

Aggiorna la policy tematica di Amazon SNS con un canale di notifica (consigliato)

1. Esegui il AWS CLI comando `list-notification-channels` DevOps Guru nell'account da cui desideri inviare le notifiche.

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

2. Nella `list-notification-channels` risposta, prendi nota dell'ID del canale che contiene l'ARN del tuo argomento Amazon SNS. L'ID del canale è un guid.

   Ad esempio, nella risposta seguente, l'ID del canale per l'argomento con l'ARN `arn:aws:sns:`*region-id*`:`*111122223333*`:`*topic-name* è *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. Vai alla policy che hai creato in un altro account utilizzando l'ID del proprietario dell'argomento inthe section called “Configurazione delle autorizzazioni per un argomento di Amazon SNS in un altro account”. Nella `Condition` dichiarazione della politica, aggiungi la riga che specifica il`SourceArn`. L'ARN contiene il tuo ID regionale (ad esempio,`us-east-1`), il numero di AWS account del mittente dell'argomento e l'ID del canale di cui hai preso nota.

   La tua `Condition` dichiarazione aggiornata è simile alla seguente.

```
"Condition" : {
  "StringEquals" : {
```

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

Se `AddNotificationChannel` non riesci ad aggiungere il tuo argomento SNS, verifica che la tua policy IAM disponga delle seguenti autorizzazioni.

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

Autorizzazioni per argomenti AWS KMS Amazon SNS crittografati

L'argomento Amazon SNS specificato potrebbe essere crittografato da. AWS Key Management Service Per consentire a DevOps Guru di lavorare con argomenti crittografati, devi prima creare una dichiarazione AWS KMS key e quindi aggiungere la seguente dichiarazione alla politica della chiave KMS. Per ulteriori informazioni, consulta Crittografia dei messaggi pubblicati su Amazon SNS con AWS KMS, Key identifiers KeyId () nella User Guide e Data encryption AWS KMS nella 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**
>
> DevOpsAttualmente Guru supporta argomenti crittografati da utilizzare all'interno di un singolo account. Al momento non è supportato l'utilizzo di un argomento crittografato su più account.

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon DevOps Guru

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con DevOps Guru e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Guru DevOps
- Voglio fornire agli utenti l'accesso programmatico
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse DevOps Guru

Non sono autorizzato a eseguire un'azione in Guru DevOps

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su una *my-example-widget* risorsa fittizia ma non dispone delle autorizzazioni fittizie`aws:GetWidget`.

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

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-widget* utilizzando l'operazione `aws:GetWidget`.

Voglio fornire agli utenti l'accesso programmatico

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfa ccia che desideri utilizzare. • Per la AWS CLI, consulta Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface • Per AWS SDK, strumenti e AWS API, consulta l'autenticazione IAM Identity Center nella Guida di riferimento agli AWS SDK e agli strumenti.
IAM	Utilizza credenziali temporane e per firmare le richieste	Segui le istruzioni in Uso delle credenziali temporanee con

Quale utente necessita dell'accesso programmatico?	Per	Come
	programmatiche agli SDK o alle API AWS CLI. AWS AWS	AWS risorse nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	Segui le istruzioni per l'interfaccia che desideri utilizzare. • Per la AWS CLI, consulta Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface • Per gli AWS SDK e gli strumenti, consulta Autenticazione tramite credenziali a lungo termine nella Guida di riferimento agli SDK e agli AWS strumenti. • Per le AWS API, consulta Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a DevOps Guru.

Alcuni AWS servizi consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in DevOps Guru. Tuttavia, l'azione richiede che il servizio

disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie risorse DevOps Guru

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se DevOps Guru supporta queste funzionalità, consulta. Come funziona Amazon DevOps Guru con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Guru della registrazione e del monitoraggio DevOps

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di DevOps Guru e delle altre soluzioni AWS. AWS fornisce i seguenti strumenti di monitoraggio per monitorare DevOps Guru, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Argomenti

Monitoring DevOps Guru con Amazon CloudWatch

Puoi monitorare DevOps Guru utilizzando CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Per DevOps Guru, puoi tenere traccia delle metriche per ottenere informazioni dettagliate e delle metriche relative all'utilizzo DevOps di Guru. Potresti voler controllare il gran numero di risultati creati per aiutarti `Insights` a determinare se le tue soluzioni operative presentano un comportamento

anomalo. Oppure potreste voler controllare l'utilizzo di DevOps Guru per aiutarvi a tenere traccia dei costi.

Il servizio DevOps Guru riporta le seguenti metriche nel namespace. `AWS/DevOps-Guru`

Argomenti

Metriche Insight

Puoi utilizzarla CloudWatch per tracciare una metrica per mostrarti quante informazioni vengono create nel tuo AWS account. Puoi specificare la `Type` dimensione da tracciare `proactive` o gli `reactive` approfondimenti. Non specificate una dimensione se desiderate tenere traccia di tutti gli approfondimenti.

Metriche

Parametro	Descrizione
`Insight`	Il numero di approfondimenti creati in un AWS account. Dimensioni valide: `Type` Statistiche valide: conteggio dei campioni, somma Unità: numero

La seguente dimensione è supportata per la `Insight` metrica DevOps Guru.

Dimensioni

Dimensione	Descrizione
`Type`	Questo è il tipo di intuizione. Non specificare una dimensione per la `Insights` metrica se desideri tenere traccia di tutti gli approfondimenti. I valori validi sono:`proactive` ,`reactive`.

DevOpsMetriche di utilizzo di Guru

Puoi utilizzarlo CloudWatch per monitorare l'utilizzo di Amazon DevOps Guru.

Metriche

Parametro	Descrizione
`CallCount`	Il numero di chiamate effettuate con uno dei seguenti metodi DevOps Guru. • `ListInsights` • `ListAnomaliesForInsight` • `ListRecommendations` • `ListEvents` • `SearchInsights` • `DescribeInsight` • `DescribeAnomaly` Dimensioni valide:`Service`,,`Class`, `Type` `Resource` Statistiche valide: conteggio dei campioni, somma Unità: numero

Le seguenti dimensioni sono supportate per le metriche di utilizzo di DevOps Guru.

Dimensioni

Dimensione	Descrizione

Dimensione	Descrizione
`Service`	Questo è il nome del servizio AWS che contiene la risorsa. Ad esempio, per DevOps Guru, questo valore è`DevOps-Guru` .
`Class`	Questa è la classe della risorsa che viene tracciata. DevOpsGuru usa questa dimensione con il valore. `None`
`Type`	Questo è il tipo di risorsa che viene tracciata. DevOpsGuru usa questa dimensione con il valore. `API`
`Resource`	Questo è il nome dell'operazione DevOps Guru. I valori validi sono:`ListInsights` ,`ListAnomaliesForInsight` ,`ListRecommendations` ,`ListEvents` ,, `SearchInsights` `DescribeInsight` ,`DescribeAnomaly` .

Registrazione delle chiamate API Amazon DevOps Guru con AWS CloudTrail

Amazon DevOps Guru è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in DevOps Guru. CloudTrail acquisisce le chiamate API per DevOps Guru come eventi. Le chiamate acquisite includono chiamate dalla console DevOps Guru e chiamate in codice alle operazioni dell'API DevOps Guru. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Guru. DevOps Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata fatta a DevOps Guru, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

DevOpsInformazioni sul guru in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in DevOps Guru, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli

eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per DevOps Guru, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

DevOpsGuru supporta la registrazione di tutte le sue azioni come eventi nei CloudTrail file di registro. Per ulteriori informazioni, consulta Actions in the DevOpsGuru API Reference.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Comprendere le voci dei file di log di DevOps Guru

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di

registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`UpdateResourceCollection`azione.


```
{
  "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"
}
```

DevOpsEndpoint VPC Guru e interfaccia ()AWS PrivateLink

Puoi usare gli endpoint VPC quando chiami le API di Amazon DevOps Guru. Quando utilizzi gli endpoint VPC, le tue chiamate API sono più sicure perché sono contenute nel tuo VPC e non accedono a Internet. Per ulteriori informazioni, consulta Azioni nell'Amazon DevOps Guru API Reference.

Stabilisci una connessione privata tra il tuo VPC e DevOps Guru creando un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere in modo privato alle API DevOps Guru senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect. AWS PrivateLink Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare DevOps con le API Guru. Il traffico tra il tuo VPC e DevOps Guru non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più interfacce di rete elastiche nelle tue sottoreti.

Per ulteriori informazioni, consulta Interface VPC endpoints (AWS PrivateLink) nella Amazon VPC User Guide.

Considerazioni sugli endpoint DevOps VPC Guru

Prima di configurare un endpoint VPC di interfaccia per DevOps Guru, assicurati di esaminare le proprietà e le limitazioni degli endpoint dell'interfaccia nella Amazon VPC User Guide.

DevOpsGuru supporta le chiamate a tutte le sue azioni API dal tuo VPC.

Creazione di un endpoint VPC di interfaccia per Guru DevOps

Puoi creare un endpoint VPC per il servizio DevOps Guru utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint dell'interfaccia nella Guida per l'utente di Amazon VPC.

Crea un endpoint VPC per DevOps Guru utilizzando il seguente nome di servizio:

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

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a DevOps Guru utilizzando il nome DNS predefinito per la regione, ad esempio. `devops-guru.us-east-1.amazonaws.com`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint dell'interfaccia in Guida per l'utente di Amazon VPC.

Creazione di una policy per gli endpoint VPC per Guru DevOps

Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso a Guru. DevOps La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

Esempio: policy degli endpoint VPC per le azioni Guru DevOps

Di seguito è riportato un esempio di policy sugli endpoint per Guru. DevOps Se associata a un endpoint, questa policy garantisce l'accesso alle azioni DevOps Guru elencate a tutti i responsabili su tutte le risorse.

```
{
   "Statement":[
      {
         "Principal":"*",
```

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

Sicurezza dell'infrastruttura in Guru DevOps

In quanto servizio gestito, Amazon DevOps Guru è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere a DevOps Guru attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Resilienza in Amazon DevOps Guru

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. DevOpsGuru opera in più zone di disponibilità e archivia dati e metadati sugli artefatti in Amazon S3 e Amazon DynamoDB. I dati crittografati vengono archiviati in modo ridondante su più strutture e più dispositivi in ogni struttura, il che li rende altamente disponibili e altamente durevoli.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta AWS Global Infrastructure.

Quote e limiti per AmazonDevOpsGuru

La seguente tabella elenca la quota corrente in AmazonDevOpsGuru. Questa quota è per ogni persona supportataAWSRegione per ciascunaAWSconto.

Notifiche

Numero massimo di argomenti di Amazon Simple Notification Service che possono essere specificati in una volta	2

Stack AWS CloudFormation

Numero massimo di stack AWS CloudFormation che è possibile specificare	1000

DevOpsLimiti di monitoraggio delle risorse di Guru

Descrizione delle risorse	Limite	Può essere aumentata
Limite predefinito per il monitoraggio delle code di Amazon Simple Queue Service (Amazon SQS)	100*	Sì**

*Per nuoviDevOpsAccount Guru creati il 29 giugno 2023 o successivamente e per account esistenti che erano attivi alla stessa data e con meno di 100 code Amazon SQS.

**Per richiedere una modifica di questo limite, contattaAWS Supportalhttps://aws.amazon.com/contact-us. Puoi richiedere un limite di monitoraggio delle code Amazon SQS di 100, 500, 1.000, 5.000 o 10.000.

DevOpsQuote Guru per la creazione, l'implementazione e la gestione di un'API

Le seguenti quote fisse si applicano alla creazione, all'implementazione e alla gestione di un'API inDevOpsGuru, usando ilAWS CLI, la console API Gateway o l'API REST di API Gateway e i relativi SDK.

Per un elenco di tuttiDevOpsAPI Guru, vediAmazonDevOpsAzioni Guru.

Quota predefinita	Può essere aumentata	
20 richieste ogni 1 secondo per account	Sì	

AmazonDevOpsStoria dei documenti Guru

La tabella seguente descrive la documentazione per questa versione diDevOpsGuru.

- Versione API: ultima
- Ultimo aggiornamento della documentazione:9 agosto 2023

Modifica	Descrizione	Data
Aggiornamenti gestiti delle policy	Gli abbonamenti Amazon SNS e l'accesso all'elenco degli abbonamenti sono stati aggiunti al`AmazonDevOpsGuruConsoleFullAccess` politica. L'accesso alla lista di sottoscrizioni è stato aggiunto anche al`AmazonDevOpsGuruReadOnlyAccess` politica. Per ulteriori informazioni, vederePolitiche basate sull'identità per AmazonDevOpsGuru.	9 agosto 2023
Chiavi di crittografia gestite dal cliente	DevOpsGuru ora supporta la crittografia con chiavi gestite dal cliente utilizzandoAWS KMS. Per ulteriori informazioni, vedereProtezione dei dati inDevOpsGuru.	5 luglio 2023
DevOpsGuru for RDS supporta RDS PostgreSQL	DevOpsGuru for RDS è in grado di rilevare problemi di prestazioni e altre informazioni nei database PostgreSQL. Per ulteriori informazioni,	30 marzo 2023

	vedereVantaggi diDevOpsGuru per RDS.	
DevOpsGuru for RDS supporta approfondimenti proattivi	DevOpsGuru for RDS pubblica approfondimenti proattivi con consigli per aiutarti a risolvere i problemi nei tuoi database Aurora prima che diventino problemi più gravi. Per ulteriori informazioni, vedereGestione delle anomalie inDevOpsGuru per RDS.	28 febbraio 2023
Pagina delle risorse analizzate	Una nuova pagina nelDevOps La console Guru elenca le risorse del tuo account che vengono analizzate daDevOpsGuru. Per ulteriori informazioni, vedereVisualizzazione delle risorse analizzate daDevOpsGuru.	20 ottobre 2022
Nuove impostazioni di configurazione delle notifiche	Ora puoi scegliere se ricevere tutte le notifiche o ricevere solo notifiche per determinati livelli ed eventi. Per ulteriori informazioni, vedereAggiornamento delle configurazioni di notifica di Amazon Amazon SNS.	30 settembre 2022

Analisi delle anomalie dei log aggiunta alle policy gestite	AWSpolitiche gestite perDevOpsGuru è stato aggiornato nella console IAM per supportare l'accesso aCloudWatchazione`FilterLogEvents` . Per ulteriori informazioni, vedereDevOpsGuru si aggiorna aAWSpolitiche gestite e ruolo legato ai servizi.	30 agosto 2022
Aggiunta l'analisi delle anomalie dei log	È possibile visualizzare informazioni dettagliate sui gruppi di log relativi agli approfondimenti nelDevOps Consolle Guru. È disponibile anche un ruolo esteso legato ai servizi per descriveCloudWatchregistri e flussi. Per ulteriori informazioni, vedereComprendere gli approfondimenti inDevOpsConsolle GurueDevOpsGuru si aggiorna aAWSpolitiche gestite e ruolo legato ai servizi.	12 luglio 2022
CodeGuruIntegrazione con Profiler	DevOpsGuru ora si integra con AmazonCodeGuruProfiler con unEventBridgeregola gestita. Ogni evento in entrata daCodeGuruProfiler è un rapporto proattivo sulle anomalie. Per ulteriori informazioni, vedereIntegrazione conCodeGuruProfiler.	7 marzo 2022

Aggiornamenti dei ruoli collegati al servizio e delle policy gestite	Policy estese disponibili nella console IAM. Le modifiche consentonoDevOpsGuru supporterà una migliore integrazione con Amazon Relational Database Service (Amazon RDS). Per ulteriori informazioni, vedereUtilizzo di ruoli collegati ai servizieAWSpolitiche gestite (predefinite) perDevOpsGuru.	21 dicembre 2021
Aggiunta una nuova politica gestita	La`AmazonDevOpsGuruConsoleFullAccess` la politica è stata aggiunta. Per ulteriori informazioni, vederePolitiche basate sull'identità per AmazonDevOpsGuru.	6 dicembre 2021
Supporto per definire la tua applicazione conAWStag	Ora puoi usareAWStag per identificare le risorse desiderateDevOpsGuru per analizzare, identificare le risorse nelle tue applicazioni e filtrare le informazioni nella console. Per ulteriori informazioni, vedereUsa i tag per identificare le risorse nelle tue applicazioni.	1° dicembre 2021

Aggiornamenti dei ruoli collegati al servizio e delle policy gestite	Policy estese disponibili nella console IAM. Le modifiche consentonoDevOpsGuru supporterà una migliore integrazione con Amazon Relational Database Service (Amazon RDS). Per ulteriori informazioni, vedereUtilizzo di ruoli collegati ai servizieAWSpolitiche gestite (predefinite) perDevOpsGuru.	1° dicembre 2021
Supporto Amazon RDS	DevOpsGuru ora fornisce analisi e approfondimenti completi per le risorse di Amazon Relational Database Service (Amazon RDS) nella tua applicazione. Per ulteriori informazioni, vedereGestione delle anomalie inDevOpsGuru per Amazon RDS.	1° dicembre 2021
AmazonEventBridgeintegrazione	DevOpsGuru ora si integra conEventBridgeper informarti di determinati eventi relativi al tuoDevOpsApprofondimenti dei guru. Per ulteriori informazioni, consulta la pagina relativa al funzionamento di EventBridge.	18 novembre 2021

AWSpolicy gestita aggiunta	NuovoAWSpolicy gestita aggiunta. La`AmazonDevOpsGuruOrganizationsAccess` la politica fornisce l'accesso aDevOpsGuru all'interno di un'organizzazione. Per ulteriori informazioni, vederepolitiche basate sull'identità.	16 novembre 2021
Aggiornamento della politica sui ruoli collegata al servizio	Policy estesa disponibile nella console IAM. La modifica consenteDevOpsGuru per supportare la visualizzazione di più account. Per ulteriori informazioni, vedereUtilizzo di ruoli collegati ai servizi.	4 novembre 2021
Supporto per più account	Ora puoi visualizzare approfondimenti e metriche su più account della tua organizzazione. Per ulteriori informazioni, vedereChe cos'è AmazonDevOpsGuru.	4 novembre 2021
Versione di disponibilità generale	AmazonDevOpsGuru è ora disponibile a tutti (GA).	4 maggio 2021
Nuovo argomento	È ora possibile generare una stima dei costi mensili perDevOpsGuru per analizzare le tue risorse. Per ulteriori informazioni, vedereValuta la tua AmazonDevOpsCosti Guru.	27 aprile 2021

Supporto per VPC Endpoint	Ora puoi utilizzare gli endpoint VPC per migliorare la sicurezza dell'analisi delle risorse e della generazione di informazioni. Per ulteriori informazioni, vedereDevOpsEndpoint VPC Guru e interfaccia (AWS PrivateLink).	15 aprile 2021
Nuovo argomento	Un nuovo argomento su come monitorareDevOpsGuru con AmazonCloudWatchè stato aggiunto. Per ulteriori informazioni, vedereMonitoraggioDevOpsGuru con AmazonCloudWatch.	11 dicembre 2020
Versione di anteprima	Questa è la versione di anteprima diAmazonDevOpsGuida per l'utente di Guru.	1° dicembre 2020

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.