aws

Panduan Pengguna

Amazon DevOps Guru

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

Amazon DevOps Guru: Panduan Pengguna

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

..... viii
Apa itu Amazon DevOps Guru? 1
Bagaimana DevOps Guru bekerja? 1
Alur kerja DevOps Guru tingkat tinggi 2
Alur kerja DevOps Guru terperinci 3
Bagaimana saya memulainya? 5
Bagaimana cara saya berhenti dikenakan biaya DevOps Guru? 5
Konsep 6
Anomali 6
Wawasan 6
Metrik dan peristiwa operasional 7
Grup log dan anomali log 7
Rekomendasi 7
Cakupan 8
Daftar cakupan layanan 10
Amazon DevOps Guru berakhir dukungan 12
Gambaran umum 12
Status layanan hingga 30 September 2027 12
Apa yang terjadi pada sumber daya Anda setelah 30 September 2027 12
Apa artinya ini bagi Anda 13
Memilih jalur migrasi yang tepat 13
Solusi alternatif 14
Amazon CloudWatch 14
DevOps Agen Amazon 14
Langkah migrasi 14
Migrasikan infrastruktur sebagai kode dan penggunaan CLI 14
Migrasikan integrasi API 15
Langkah-langkah offboarding: Ekspor data Anda 15
Hapus sumber daya Amazon DevOps Guru Anda 15
Pertanyaan umum 16
Sumber daya tambahan 16
Transisi dari Amazon DevOps Guru ke Amazon CloudWatch dan Amazon DevOps Agen 17
Bagaimana DevOps Guru dan penggantinya berbeda 18
Bagaimana transisi bekerja 18

Bagaimana kami mendukung Anda melalui transisi 19
Siapa yang perlu bertindak, dan kapan 19
Apa yang berubah sekilas 20
Deteksi anomali metrik dan peringatan 21
Deteksi anomali log 22
Deteksi anomali database 22
Investigasi dan analisis akar penyebab 23
Wawasan proaktif 24
Infrastruktur sebagai kode dan penggunaan CLI 24
Integrasi API 25
Ekspor data Anda 26
Hapus DevOps Sumber daya Guru 26
Garis waktu dan dukungan 27
Daftar periksa transisi 27
Pertanyaan umum 28
Sumber daya terkait 28
Penyiapan 30
Mendaftar untuk AWS 30
Mendaftar untuk Akun AWS 30
Tentukan cakupan untuk DevOps Guru 31
Mengidentifikasi topik notifikasi Anda 32
Izin ditambahkan ke topik Anda 32
Memperkirakan biaya Anda 34
Memulai 37
Langkah 1: Siapkan 37
Langkah 2: Aktifkan DevOps Guru 37
Memantau akun di seluruh organisasi 37
Pantau akun Anda saat ini 39
Langkah 3: Tentukan DevOps Cakupan sumber daya Guru 40
Mengaktifkan AWS layanan untuk analisis DevOps Guru 43
Bekerja dengan wawasan 44
Melihat wawasan 44
Memahami wawasan di konsol DevOps Guru 45
Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan 48
Memahami keparahan wawasan 49
Database pemantauan 50

Basis data relasional ... 50
Memantau operasi basis data di Amazon RDS ... 50
Memantau operasi database di Amazon Redshift ... 52
Bekerja dengan anomali di DevOps Guru untuk RDS ... 53
Database non-relasional ... 73
Memantau operasi database di Amazon DynamoDB ... 73
Memantau operasi database di Amazon ElastiCache ... 74
Integrasi dengan Profiler CodeGuru ... 75
Mendefinisikan aplikasi menggunakan sumber daya AWS ... 76
Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi Anda ... 77
Apa itu tag? ... 78
Mendefinisikan aplikasi menggunakan tag ... 78
Menggunakan tag dengan DevOps Guru ... 79
Menambahkan tag ke sumber daya ... 80
Menggunakan tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda ... 81
Memilih tumpukan untuk dianalisis ... 81
Bekerja dengan EventBridge ... 83
Acara untuk DevOps Guru ... 83
DevOps Acara Terbuka Guru New Insight ... 83
Pola peristiwa sampel khusus untuk Insight baru dengan tingkat keparahan tinggi ... 85
Memperbarui pengaturan ... 86
Memperbarui akun manajemen Anda ... 86
Memperbarui cakupan AWS analisis Anda ... 86
Memperbarui notifikasi ... 87
Arahkan ke pengaturan notifikasi di konsol DevOps Guru ... 88
Menambahkan topik notifikasi Amazon SNS ... 88
Menghapus topik notifikasi Amazon SNS ... 89
Memperbarui konfigurasi notifikasi Amazon SNS ... 89
Izin ditambahkan ke topik Anda ... 90
Memfilter notifikasi ... 91
Memfilter notifikasi dengan kebijakan filter langganan Amazon SNS ... 91
Contoh notifikasi Amazon SNS yang difilter ... 92
Memperbarui integrasi Systems Manager ... 93
Memperbarui deteksi anomali log ... 94
Memperbarui enkripsi ... 94

Melihat notifikasi 96
Wawasan baru 96
Wawasan tertutup 97
Asosiasi baru 99
Rekomendasi baru 100
Tingkat keparahan ditingkatkan 101
Kegagalan validasi sumber daya 102
Melihat sumber daya yang dianalisis 104
Memperbarui cakupan AWS analisis Anda 104
Menghapus tampilan sumber daya yang dianalisis untuk pengguna 106
Praktik terbaik 108
Keamanan 109
Perlindungan Data 110
Enkripsi data 111
Bagaimana DevOps Guru menggunakan hibah di AWS KMS 112
Memantau kunci enkripsi Anda di DevOps Guru 113
Membuat kunci yang dikelola pelanggan 113
Privasi lalu lintas 115
Identity and Access Management 115
Audiens 116
Mengautentikasi dengan Identitas 116
Mengelola Akses menggunakan Kebijakan 118
Pembaruan Kebijakan 119
Bagaimana Amazon DevOps Guru bekerja dengan IAM 124
Identity-based kebijakan 130
Menggunakan peran tertaut layanan 141
DevOps Referensi izin Guru 147
Izin untuk topik Amazon SNS 152
Izin untuk topik Amazon SNS terenkripsi 156
Pemecahan Masalah 156
Pemantauan DevOps Guru 161
Pemantauan CloudWatch dengan 161
Pencatatan DevOps Panggilan API Guru dengan AWS CloudTrail 164
Titik akhir VPC (AWS PrivateLink) 167
Pertimbangan untuk DevOps Titik akhir Guru VPC 167
Membuat titik akhir antarmuka VPC untuk DevOps Guru 168

Membuat kebijakan titik akhir VPC untuk DevOps Guru 168
Keamanan Infrastruktur 169
Ketahanan 169
Kuota dan batas 170
Notifikasi 170
CloudFormation tumpukan 170
DevOpsBatas pemantauan sumber daya Guru 170
DevOpsKuota Guru untuk membuat, menerapkan, dan mengelola API 171
Riwayat dokumen 172
AWS Glosarium 180

Pemberitahuan akhir dukungan: Amazon DevOps Guru akan berhenti menerima pelanggan baru pada 29 Oktober 2026. Pelanggan saat ini tidak akan terpengaruh dan dapat terus menggunakan Amazon DevOps Guru hingga 30 September 2027. Setelah 30 September 2027 Anda tidak akan lagi dapat mengakses Amazon DevOps Guru. Untuk informasi selengkapnya, lihat Amazon DevOps Guru berakhir dukungan.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

Apa itu Amazon DevOps Guru?

Selamat datang di panduan pengguna Amazon DevOps Guru.

DevOpsGuru adalah layanan operasi yang dikelola sepenuhnya yang memudahkan pengembang dan operator untuk meningkatkan kinerja dan ketersediaan aplikasi mereka. DevOpsGuru memungkinkan Anda melepaskan tugas administratif yang terkait dengan mengidentifikasi masalah operasional sehingga Anda dapat dengan cepat menerapkan rekomendasi untuk meningkatkan aplikasi Anda. DevOpsGuru menciptakan wawasan reaktif yang dapat Anda gunakan untuk meningkatkan aplikasi Anda sekarang. Ini juga menciptakan wawasan proaktif untuk membantu Anda menghindari masalah operasional yang mungkin memengaruhi aplikasi Anda di masa mendatang.

DevOpsGuru menerapkan pembelajaran mesin untuk menganalisis data operasional Anda dan metrik aplikasi dan peristiwa untuk mengidentifikasi perilaku yang menyimpang dari pola operasi normal. Anda diberitahu ketika DevOps Guru mendeteksi masalah operasional atau risiko. Untuk setiap masalah, DevOps Guru menyajikan rekomendasi cerdas untuk mengatasi masalah operasional saat ini dan yang diprediksi di masa depan.

Untuk memulai, lihat Bagaimana cara memulai dengan DevOps Guru?

Bagaimana DevOps Guru bekerja?

Alur kerja DevOps Guru dimulai saat Anda mengonfigurasi cakupan dan notifikasi. Setelah Anda mengatur DevOps Guru, itu mulai menganalisis data operasional Anda. Ketika mendeteksi perilaku anomali, ia menciptakan wawasan yang berisi rekomendasi dan daftar metrik, grup log, dan peristiwa yang terkait dengan masalah tersebut. Untuk setiap wawasan, DevOps Guru memberi tahu Anda. Jika Anda mengaktifkan AWS Systems Manager OpsCenter, sebuah OpsItem dibuat sehingga Anda dapat menggunakan Manajer Sistem OpsCenter untuk melacak dan mengelola pengalamatan wawasan Anda. Setiap wawasan berisi rekomendasi, metrik, grup log, dan peristiwa yang terkait dengan perilaku anomali. Gunakan informasi dalam wawasan untuk membantu Anda memahami dan mengatasi perilaku anomali.

Lihat Alur kerja DevOps Guru tingkat tinggi untuk detail lebih lanjut tentang tiga langkah alur kerja tingkat tinggi. Lihat Alur kerja DevOps Guru terperinci untuk mempelajari alur kerja DevOps Guru yang lebih rinci, termasuk bagaimana cara berinteraksi dengan AWS layanan lain.

Topik

- Alur kerja DevOps Guru tingkat tinggi

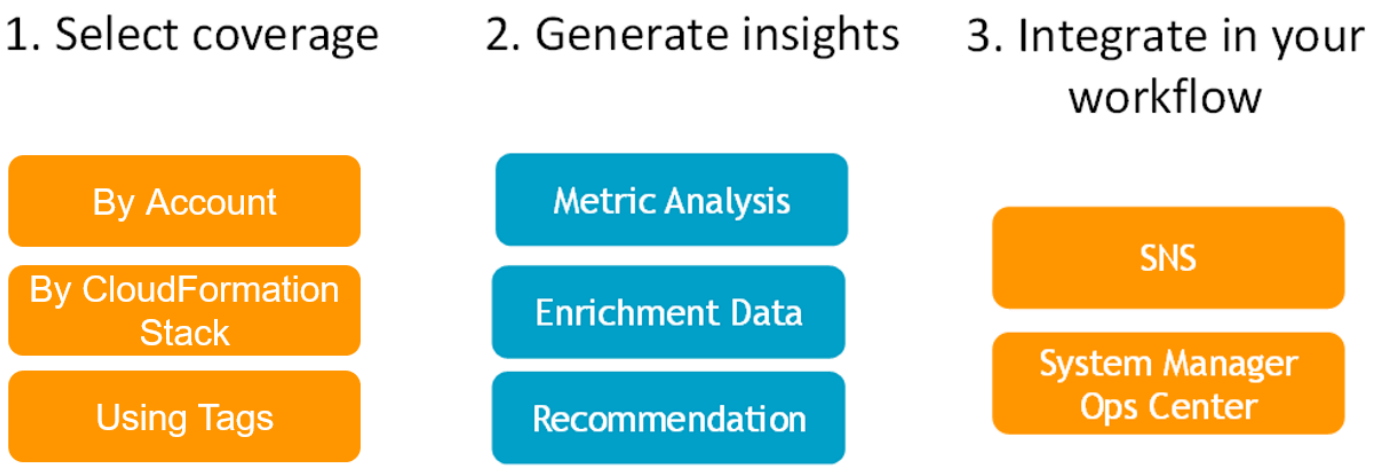
- Alur kerja DevOps Guru terperinci

Alur kerja DevOps Guru tingkat tinggi

Alur kerja Amazon DevOps Guru dapat dipecah menjadi tiga langkah tingkat tinggi.

1. T DevOps entukan cakupan Guru dengan memberi tahu AWS sumber daya mana di AWS akun Anda yang ingin Anda analisis.
2. DevOpsGuru mulai menganalisis CloudWatch metrik Amazon AWS CloudTrail, dan data operasional lainnya untuk mengidentifikasi masalah yang dapat Anda perbaiki untuk meningkatkan operasi Anda.
3. DevOpsGuru memastikan bahwa Anda tahu tentang wawasan dan informasi penting dengan mengirimkan pemberitahuan untuk setiap acara DevOps Guru yang penting.

Anda juga dapat mengonfigurasi DevOps Guru untuk membuat OpsItem in AWS Systems Manager OpsCenter untuk membantu Anda melacak wawasan Anda. Diagram berikut menunjukkan alur kerja tingkat tinggi ini.



1. Pada langkah pertama, Anda memilih cakupan Anda dengan menentukan AWS sumber daya mana di AWS akun Anda yang dianalisis. DevOpsGuru dapat mencakup, atau menganalisis, semua sumber daya dalam AWS akun, atau Anda dapat menggunakan tumpu AWS CloudFormation kan atau AWS tag untuk menentukan subset sumber daya di akun Anda untuk dianalisis. Pastikan bahwa sumber daya yang Anda tentukan membentuk aplikasi, beban kerja, dan layanan mikro yang penting untuk bisnis Anda. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

2. Pada langkah kedua, DevOps Guru menganalisis sumber daya untuk menghasilkan wawasan. Ini adalah proses yang berkelanjutan. Anda dapat melihat wawasan dan melihat rekomendasi dan informasi terkait yang dikandungnya di konsol DevOps Guru. DevOps Guru menganalisis data berikut untuk menemukan masalah dan membuat wawasan.
   - CloudWatch Metrik Amazon individual yang dipancarkan oleh AWS sumber daya Anda. Ketika masalah diidentifikasi, DevOps Guru mengumpulkan metrik tersebut bersama-sama.
   - Login anomali dari CloudWatch grup log Amazon. Jika Anda mengaktifkan deteksi anomali log, DevOps Guru menampilkan anomali log terkait saat terjadi masalah.
   - DevOpsGuru menarik data pengayaan dari log AWS CloudTrail manajemen untuk menemukan peristiwa yang terkait dengan metrik yang dikumpulkan. Peristiwa dapat berupa peristiwa penyebaran sumber daya dan perubahan konfigurasi.
   - Jika Anda menggunakan AWS CodeDeploy, DevOps Guru menganalisis peristiwa penerapan untuk membantu menghasilkan wawasan. Peristiwa untuk semua jenis pener CodeDeploy apan (server lokal, server Amazon EC2, Lambda, atau Amazon EC2) dianalisis.
   - Ketika DevOps Guru menemukan pola tertentu, itu menghasilkan satu atau lebih rekomendasi untuk membantu mengurangi atau memperbaiki masalah yang diidentifikasi. Rekomendasi dikumpulkan dalam satu wawasan. Wawasan juga berisi daftar metrik dan peristiwa yang terkait dengan masalah tersebut. Anda menggunakan data wawasan untuk mengatasi dan memahami masalah yang diidentifikasi.
3. Pada langkah ketiga, DevOps Guru mengintegrasikan pemberitahuan wawasan ke dalam alur kerja Anda untuk membantu Anda mengelola masalah dan mengatasinya dengan cepat.
   - Wawasan yang dihasilkan di AWS akun Anda dipublikasikan ke topik Amazon Simple Notification Service (Amazon SNS) yang dipilih selama pengaturan DevOps Guru. Ini adalah bagaimana Anda diberitahu segera setelah wawasan dibuat. Untuk informasi selengkapnya, lihat Memperbarui notifikasi Anda di DevOps Guru.
   - Jika Anda mengaktifkan AWS Systems Manager selama pengaturan DevOps Guru, setiap wawasan membuat yang sesuai OpsItem untuk membantu Anda melacak dan mengelola masalah yang ditemukan. Untuk informasi selengkapnya, lihat Memperbarui AWS Systems Manager integrasi di DevOps Guru.

Alur kerja DevOps Guru terperinci

Alu DevOps r kerja Guru terintegrasi dengan beberapa AWS layanan, termasuk Amazon CloudWatch, AWS CloudTrail, Amazon Simple Notification Service, dan AWS Systems Manager.

Diagram berikut menunjukkan alur kerja terperinci yang mencakup cara kerjanya dengan AWS layanan lain.

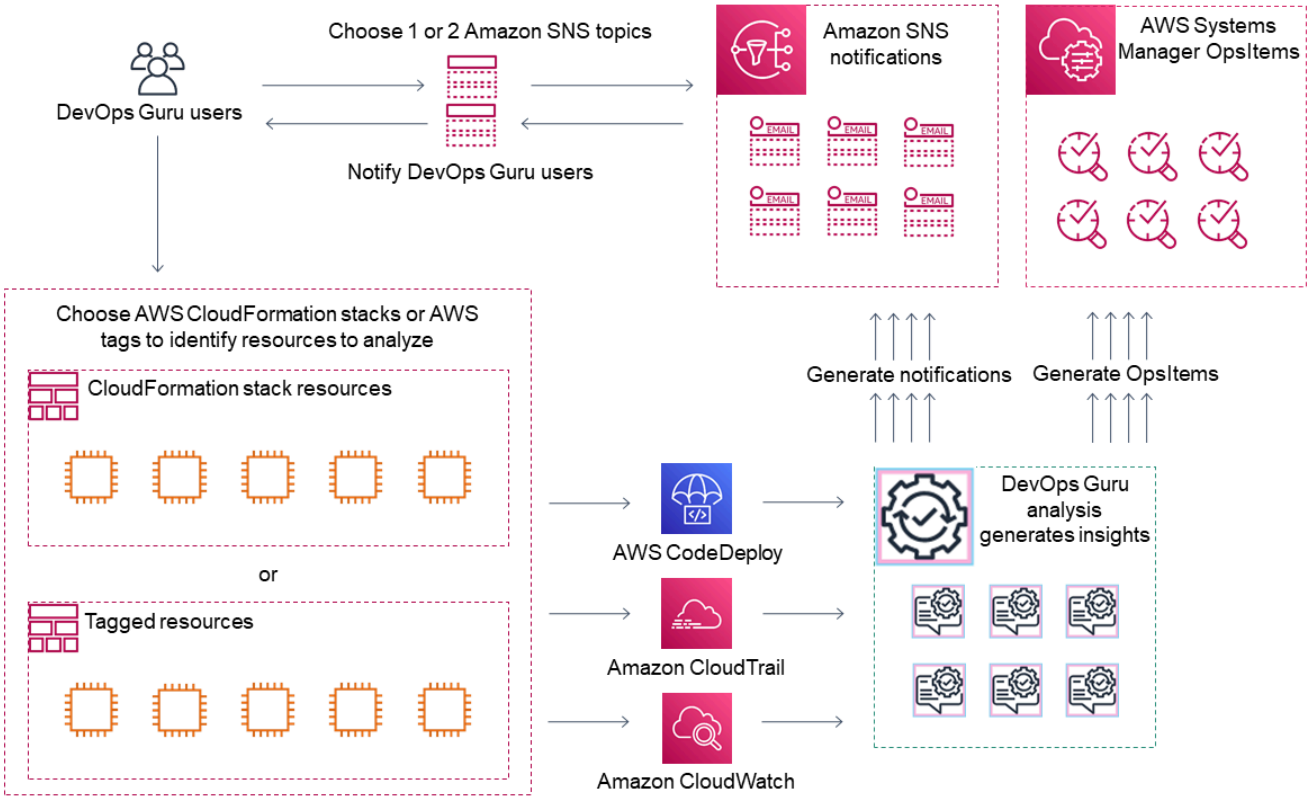


Diagram ini menunjukkan skenario di mana cakupan DevOps Guru ditentukan oleh AWS sumber daya yang ditentukan dalam tumpu AWS CloudFormation kan atau menggunakan AWS tag. Jika tidak ada tumpukan atau tag yang dipilih, cakupan DevOps Guru menganalisis semua AWS sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Mendefinisikan aplikasi menggunakan sumber daya AWS dan Tentukan cakupan untuk DevOps Guru.

1. Selama penyiapan, Anda menentukan satu atau dua topik Amazon SNS yang digunakan untuk memberi tahu Anda tentang peristiwa DevOps Guru penting, seperti saat wawasan dibuat. Selanjutnya, Anda dapat menentukan tum AWS CloudFormation pukan yang menentukan sumber daya yang ingin Anda analisis. Anda juga dapat mengaktifkan Manajer Sistem untuk menghasilkan wawasan OpsItem untuk setiap wawasan untuk membantu Anda mengelola wawasan Anda.
2. Setelah DevOps Guru dikonfigurasi, ia mulai menganalisis CloudWatch metrik, grup log, dan peristiwa yang dipancarkan dari sumber daya dan AWS CloudTrail data Anda yang terkait dengan CloudWatch metrik. Jika operasi Anda mencakup pener CodeDeploy apan, DevOps Guru juga menganalisis peristiwa penerapan.

DevOpsGuru menciptakan wawasan ketika mengidentifikasi perilaku yang tidak biasa dan anomali dalam data yang dianalisis. Setiap wawasan berisi satu atau lebih rekomendasi, daftar metrik yang digunakan untuk menghasilkan wawasan, daftar grup log terkait, dan daftar peristiwa yang digunakan untuk menghasilkan wawasan. Gunakan informasi ini untuk mengatasi masalah yang diidentifikasi.

3. Setelah setiap wawasan dibuat, DevOps Guru mengirimkan pemberitahuan menggunakan topik atau topik Amazon SNS yang ditentukan selama DevOps pengaturan Guru. Jika Anda mengaktifkan DevOps Guru untuk menghasilkan OpsItem di Manajer Sistem OpsCenter, maka setiap wawasan juga memicu Manajer Sistem baruOpsItem. Anda dapat menggunakan Manajer Sistem untuk mengelola wawasan Anda OpsItems.

Bagaimana cara memulai dengan DevOps Guru?

Kami menyarankan agar Anda menyelesaikan langkah berikut:

1. Pelajari lebih DevOps lanjut tentang Guru dengan membaca informasi diDevOpsKonsep guru.
2. Siapkan AWS akun Anda, pengguna AWS CLI, dan administratif dengan mengikuti langkah-langkah diMenyiapkan Amazon DevOps Guru.
3. Gunakan DevOps Guru, ikuti instruksi diMemulai dengan DevOps Guru.

Bagaimana cara saya berhenti dikenakan biaya DevOps Guru?

Untuk menonaktifkan Amazon DevOps Guru sehingga berhenti menimbulkan biaya dari menganalisis sumber daya di AWS akun dan Wilayah Anda, perbarui pengaturan cakupan Anda sehingga tidak menganalisis sumber daya. Untuk melakukan ini, ikuti langkah-langkah di Memperbarui cakupan AWS analisis Anda di DevOps Guru dan pilih Tidak ada di langkah 4. Anda harus melakukan ini untuk setiap AWS akun dan Wilayah tempat DevOps Guru menganalisis sumber daya.

> **Note**
>
> Jika Anda memperbarui cakupan Anda untuk berhenti menganalisis sumber daya, Anda mungkin terus dikenakan biaya kecil jika Anda meninjau wawasan yang ada yang dihasilkan oleh DevOps Guru di masa lalu. Biaya ini terkait dengan panggilan API yang digunakan untuk mengambil dan menampilkan informasi wawasan. Untuk informasi selengkapnya, lihat harga Amazon DevOps Guru.

DevOpsKonsep guru

Konsep-konsep berikut ini penting untuk memahami cara kerja Amazon DevOps Guru.

Topik

- Anomali
- Wawasan
- Metrik dan peristiwa operasional
- Grup log dan anomali log
- Rekomendasi

Anomali

Anomali mewakili satu atau lebih metrik terkait yang terdeteksi oleh DevOps Guru yang tidak terduga atau tidak biasa. DevOpsGuru menghasilkan anomali dengan menggunakan pembelajaran mesin untuk menganalisis metrik dan data operasional yang terkait dengan sumber daya Anda. AWS Anda menentukan AWS sumber daya yang ingin dianalisis saat menyiapkan Amazon DevOps Guru. Untuk informasi selengkapnya, lihat Menyiapkan Amazon DevOps Guru.

Wawasan

Wawasan adalah kumpulan anomali yang dibuat selama analisis AWS sumber daya yang Anda tentukan saat Anda mengatur DevOps Guru. Setiap wawasan berisi pengamatan, rekomendasi, dan data analitis yang dapat Anda gunakan untuk meningkatkan kinerja operasional Anda. Ada dua jenis wawasan:

- Reaktif: Wawasan reaktif mengidentifikasi perilaku anomali saat terjadi. Ini berisi anomali dengan rekomendasi, metrik terkait, dan peristiwa untuk membantu Anda memahami dan mengatasi masalah sekarang.
- Proaktif: Wawasan proaktif memberi tahu Anda tentang perilaku anomali sebelum itu terjadi. Ini berisi anomali dengan rekomendasi untuk membantu Anda mengatasi masalah sebelum diprediksi terjadi.

Metrik dan peristiwa operasional

Anomali yang membentuk wawasan dihasilkan dengan menganalisis metrik yang dikembalikan oleh Amazon CloudWatch dan peristiwa operasional yang dipancarkan oleh sumber daya Anda. AWS Anda dapat melihat metrik dan peristiwa operasional yang menciptakan wawasan untuk membantu Anda lebih memahami masalah dalam aplikasi Anda.

Grup log dan anomali log

Saat Anda mengaktifkan deteksi anomali log, grup log yang relevan akan ditampilkan di halaman wawasan DevOps Guru di konsol DevOps Guru. Grup log memberi tahu Anda tentang informasi diagnostik penting tentang kinerja sumber daya dan diakses.

Anomali log mewakili sekelompok peristiwa log anomali serupa yang ditemukan dalam grup log. Contoh peristiwa log anomali yang dapat ditampilkan di DevOps Guru termasuk anomali kata kunci, anomali format, anomali kode HTTP, dan banyak lagi.

Anda dapat menggunakan anomali log untuk mendiagnosis akar penyebab masalah operasional. DevOpsGuru juga mereferensikan baris log dalam rekomendasi wawasan untuk memberikan lebih banyak konteks untuk solusi yang direkomendasikan.

> **Note**
>
> DevOpsGuru bekerja dengan Amazon CloudWatch untuk mengaktifkan deteksi anomali log. Saat Anda mengaktifkan deteksi anomali log, DevOps Guru menambahkan tag ke grup CloudWatch log Anda. Saat Anda mematikan deteksi anomali log, DevOps Guru menghapus tag dari grup CloudWatch log Anda.
> Selain itu, administrator harus memastikan bahwa hanya pengguna dengan izin untuk melihat log yang memiliki izin untuk melihat CloudWatch log anomali. CloudWatch Kami menyarankan Anda menggunakan kebijakan IAM untuk mengizinkan atau menolak akses ke `ListAnomalousLogs` operasi. Untuk informasi selengkapnya, lihat Identity and Access Management for DevOps Guru.

Rekomendasi

Setiap wawasan memberikan rekomendasi dengan saran untuk membantu Anda meningkatkan kinerja aplikasi Anda. Rekomendasi tersebut meliputi:

- Deskripsi tindakan rekomendasi untuk mengatasi anomali yang terdiri dari wawasan.
- Daftar metrik yang dianalisis di mana DevOps Guru menemukan perilaku anomali. Setiap metrik menyertakan nama CloudFormation tumpukan yang menghasilkan sumber daya yang terkait dengan metrik, nama sumber daya, dan nama AWS layanan yang terkait dengan sumber daya.
- Daftar peristiwa yang terkait dengan metrik anomali yang terkait dengan wawasan. Setiap peristiwa terkait berisi nama CloudFormation tumpukan yang menghasilkan sumber daya yang terkait dengan acara, nama sumber daya yang menghasilkan acara, dan nama AWS layanan yang terkait dengan acara tersebut.
- Daftar grup log yang terkait dengan perilaku anomali yang terkait dengan wawasan. Setiap grup log berisi pesan log sampel, informasi tentang jenis anomali log yang dilaporkan, waktu anomali log terjadi, dan tautan untuk melihat baris log. CloudWatch

DevOpsCakupan Guru

DevOpsGuru menangani dan menciptakan wawasan untuk sejumlah AWS layanan yang berbeda. Untuk setiap layanan yang dibuat oleh DevOps Guru, DevOps Guru menampilkan berbagai metrik yang dianalisis dan wawasan yang dihasilkan.

Contoh kasus penggunaan untuk wawasan reaktif:

Nama Layanan	Kasus Penggunaan	Contoh	Metrik-metrik
AWS Lambda	Mendeteksi anomali latensi atau durasi untuk fungsi Lambda yang disebabkan oleh berbagai akar penyebab seperti start dingin, peningkatan permintaan, pelambatan hilir, atau penerapan kode. Merekomendasikan cara untuk mengurangi dengan cepat.	Penyebaran kode: Amazon API Gateway latensi dipengaruhi oleh peningkatan latensi Lambda setelah penerapan kode Lambda baru-baru ini. Pelambatan hilir: operator mengurangi kapasitas pada unit baca untuk DynamoDB, menyebabkan peningkatan	Durasi Trotel

Nama Layanan	Kasus Penggunaan	Contoh	Metrik-metrik
		percobaan ulang. Ini menghasilkan pelambatan. Mulai dingin: fungsi Lambda kurang disediaka n, jadi Lambda membutuhkan waktu lebih lama saat permintaan dibuat.	

Contoh kasus penggunaan untuk wawasan proaktif:

Nama Layanan	Kasus Penggunaan	Metrik-metrik
Amazon DynamoDB	Kapasitas konsumsi baca tabel DynamoDB berisiko mencapai batas tabel. Tindakan yang disarankan: jika Anda menggunakan mode kapasitas yang disediakan, gunakan penskalaan otomatis untuk secara aktif mengelola kapasitas throughput untuk tabel atau membeli kapasitas cadangan terlebih dahulu untuk tabel. Beralih ke mode kapasitas sesuai permintaa n untuk membayar per permintaan baca, hanya membayar untuk apa yang digunakan. Waktu deteksi: 6 hari	ConsumedReadCapacityUnits

Daftar cakupan layanan

Untuk beberapa layanan, DevOps Guru menciptakan wawasan reaktif. Wawasan reaktif mengidentifikasi perilaku anomali saat terjadi. Ini berisi anomali dengan rekomendasi, metrik terkait, dan peristiwa untuk membantu Anda memahami dan mengatasi masalah sekarang.

Untuk beberapa layanan, DevOps Guru menciptakan wawasan proaktif. Wawasan proaktif memberi tahu Anda tentang perilaku anomali sebelum itu terjadi. Ini berisi anomali dengan rekomendasi untuk membantu Anda mengatasi masalah sebelum diprediksi terjadi.

DevOpsGuru menciptakan wawasan reaktif untuk layanan seperti berikut:

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

> **Note**
>
> DevOpsPemantauan Guru berada pada tingkat grup Auto Scaling, dan tidak pada satu tingkat instans.

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

- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru menciptakan wawasan proaktif untuk layanan seperti berikut:

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

Amazon DevOps Guru berakhir dukungan

Gambaran umum

Setelah mempertimbangkan dengan cermat, kami memutuskan untuk mengakhiri dukungan untuk Amazon DevOps Guru, efektif 30 September 2027. Amazon DevOps Guru tidak akan lagi menerima pelanggan baru mulai 29 Oktober 2026. Sebagai pelanggan lama dengan akun yang mendaftar untuk layanan sebelum 29 Oktober 2026, Anda dapat terus menggunakan fitur Amazon DevOps Guru. Setelah 30 September 2027, Anda tidak akan dapat lagi menggunakan Amazon DevOps Guru.

Kami menyarankan agar pelanggan memindahkan kebutuhan peringatan dan deteksi anomali mereka ke Amazon CloudWatch, dan, untuk penyelidikan AI-assisted operasional dan pengayaan wawasan, jelajahi Agen Amazon. DevOps Lihat Solusi alternatif untuk detail.

Status layanan hingga 30 September 2027

Hingga 30 September 2027, pelanggan Amazon DevOps Guru yang ada dapat terus menggunakan layanan secara normal. Selama periode ini, AWS akan:

1. Berikan patch keamanan dan perbaikan bug kritis
2. Menjaga ketersediaan dan kinerja layanan
3. Terus menawarkan dukungan melalui saluran AWS Dukungan
4. Tidak menambahkan fitur baru ke layanan

Apa yang terjadi pada sumber daya Anda setelah 30 September 2027

Setelah 30 September 2027:

- Anda tidak akan lagi dapat mengakses konsol Amazon DevOps Guru.
- Oper DevOps asi Amazon Guru API tidak lagi tersedia. Aplikasi, skrip, atau pipeline apa pun yang memanggil API Amazon DevOps Guru perlu diperbarui sebelum tanggal ini. Lihat Apa artinya ini bagi Anda.
- Jenis sumber daya Amazon DevOps Guru akan ditarik, dan AWS CloudFormation operasi AWS CLI yang membuat atau memperbarui jenis sumber daya tersebut akan gagal. Lihat Migrasikan infrastruktur sebagai kode dan penggunaan CLI.

- Wawasan yang sebelumnya dihasilkan oleh Amazon DevOps Guru tidak akan dapat diambil lagi.

Apa artinya ini bagi Anda

Dampak dari perubahan ini tergantung pada cara Anda menggunakan Amazon DevOps Guru. Karena Amazon DevOps Guru adalah alat pemantauan, kerugian tidak mengganggu beban kerja yang sedang berjalan. Pelanggan yang telah membangun otomatisasi, infrastruktur sebagai kode, atau perkakas hilir di atas Amazon DevOps Guru perlu mengambil tindakan sebelum 30 September 2027 untuk menghindari dampak apa pun.

Jika Anda mendeklarasikan sumber daya Amazon DevOps Guru di infrastruktur sebagai kode (AWS CloudFormation, AWS CDK, Terraform) atau CLI. AWS Template dan tumpukan yang mer `AWS::DevOpsGuru::ResourceCollection` ef `AWS::DevOpsGuru::NotificationChannel` erensikan atau akan gagal dibuat atau diperbarui setelah jenis sumber daya ditarik. Karena satu sumber daya yang gagal dapat memblokir seluruh operasi tumpukan, ini adalah dampak tingkat keparahan tertinggi. Hapus sumber daya ini dari template Anda sebelum dukungan berakhir. Lihat Migrasikan infrastruktur sebagai kode dan penggunaan CLI.

Jika Anda memanggil API Amazon DevOps Guru dari perkakas Anda sendiri. Jika Anda menarik wawasan ke dalam alat pengembang internal, dasbor, atau sistem tiket melalui Amazon DevOps Guru API, integrasi tersebut akan berhenti mengembalikan data setelah dukungan berakhir. Perbarui mereka untuk mendapatkan sinyal yang setara dari Amazon CloudWatch. Lihat Migrasikan integrasi API.

Memilih jalur migrasi yang tepat

Gunakan panduan berikut untuk memutuskan ke mana harus pindah setiap cara Anda menggunakan Amazon DevOps Guru hari ini.

- Anda menggunakan Amazon DevOps Guru terutama untuk deteksi anomali dan memperingatkan metrik. Pindah ke Amazon CloudWatch. Lihat Amazon CloudWatch.
- Anda menggunakan Amazon DevOps Guru untuk memperkaya, menghubungkan, atau menyelidiki masalah operasional. Jelajahi DevOps Agen Amazon. Lihat DevOps Agen Amazon.

Solusi alternatif

Kami telah mengidentifikasi alternatif berikut untuk Amazon DevOps Guru yang dapat membantu Anda menjaga visibilitas operasional dan deteksi anomali.

Amazon CloudWatch

Terbaik untuk: Pelanggan yang menggunakan Amazon DevOps Guru untuk deteksi anomali metrik dan peringatan operasional.

Amazon CloudWatch menyediakan pemantauan metrik, alarm, dan deteksi anomali di seluruh AWS sumber daya dan aplikasi Anda.

Manfaat utama:

1. Deteksi anomali asli pada CloudWatch metrik, dengan alarm yang memberi tahu Anda ketika metrik menyimpang dari pola yang diharapkan.
2. Cakupan AWS layanan dan metrik khusus pihak pertama yang luas.
3. Terintegrasi dengan rangkaian CloudWatch observabilitas yang lebih luas (metrik, log, dasbor).

Pelajari lebih lanjut: CloudWatch Dokumentasi Amazon.

DevOps Agen Amazon

Terbaik untuk: Pelanggan yang mengandalkan Amazon DevOps Guru untuk memperkaya, menghubungkan, dan menyelidiki masalah operasional.

Pelajari lebih lanjut: Dokumentasi DevOps Agen Amazon.

Langkah migrasi

Bagian berikut menjelaskan cara memigrasi infrastruktur Anda sebagai kode, penggunaan CLI, dan integrasi API dari Amazon DevOps Guru sebelum 30 September 2027.

Migrasikan infrastruktur sebagai kode dan penggunaan CLI

Jika Anda mendeklarasikan sumber daya Amazon DevOps Guru di AWS CloudFormation, AWS CDK, Terraform, atau membuatnya melalui AWS CLI, hapus sumber daya tersebut sebelum 30 September 2027 untuk menghindari operasi tumpukan yang gagal.

Amazon DevOps Guru mengekspos jenis sumber daya berikut:

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

1. Inventarisasi templat dan tumpukan yang mereferensikan jenis sumber daya sebelumnya.
2. Siapkan CloudWatch konfigurasi Amazon yang setara (misalnya, alarm dan notifikasi yang menggantikan saluran notifikasi Amazon DevOps Guru Anda).
3. Hapus sumber daya Amazon DevOps Guru dari templat Anda dan terapkan perubahan sehingga sumber daya tidak lagi dikelola oleh tumpukan Anda.

Migrasikan integrasi API

Jika perkakas Anda memanggil API Amazon DevOps Guru, perbarui ke sumber sinyal yang setara dari Amazon CloudWatch sebelum dukungan berakhir.

Langkah-langkah offboarding: Ekspor data Anda

W DevOps awasan Amazon Guru tidak dapat diambil setelah 30 September 2027. Jika Anda ingin menyimpan catatan wawasan Anda, ekspor sebelum tanggal tersebut. Ada dua cara untuk melakukan ini, dan kami menyarankan sebagian besar pelanggan menggunakan keduanya: saluran notifikasi Amazon SNS untuk menangkap wawasan mulai sekarang hingga akhir dukungan, dan API Amazon DevOps Guru untuk mengekspor wawasan yang telah Anda kumpulkan.

Hapus sumber daya Amazon DevOps Guru Anda

Untuk menghentikan analisis dan menghentikan biaya sebelum dukungan berakhir, setel cakupan analisis Anda ke Tidak ada untuk setiap akun dan Wilayah tempat Amazon DevOps Guru diaktifkan. Di konsol, pilih Peng aturan, lalu cakupan analisis DevOps Guru, lalu Kel ola, lalu Tidak Ada. Anda juga dapat memanggil `UpdateResourceCollection` untuk menghapus tum CloudFormation pukan atau tag yang menentukan batas cakupan Anda. Selesaikan ekspor data Anda sebelum Anda melakukan ini.

Untuk menghapus saluran notifikasi, hubungi `RemoveNotificationChannel` atau hapus dari Pengaturan di konsol. Menghapus saluran tidak menghapus topik Amazon SNS atau apa pun yang telah Anda arsipkan melaluinya.

Jika Anda mendeklarasikan sumber daya Amazon DevOps Guru di infrastruktur sebagai kode, hapus sumber daya tersebut dari template Anda daripada menghapusnya di luar band, sehingga tumpukan dan templat Anda tetap sesuai kesepakatan. Lihat Migrasikan infrastruktur sebagai kode dan penggunaan CLI.

Pertanyaan umum

Akankah aplikasi atau database saya berhenti bekerja setelah 30 September 2027?

> Tidak. Amazon DevOps Guru adalah layanan pemantauan: ia mengamati sumber daya yang Anda jalankan, tidak meng-host mereka. Setelah dukungan berakhir, Anda kehilangan visibilitas dan rekomendasi Amazon DevOps Guru, tetapi aplikasi, database, dan infrastruktur Anda terus berjalan.

Apa yang terjadi jika saya tidak bermigrasi pada 30 September 2027?

> Setelah 30 September 2027 Anda tidak akan lagi dapat mengakses konsol atau API Amazon DevOps Guru, dan jenis sumber daya Amazon DevOps Guru akan gagal masuk AWS CloudFormation dan AWS CLI.

Sumber daya tambahan

Untuk informasi selengkapnya, lihat sumber daya berikut ini.

- CloudWatch Dokumentasi Amazon
- Dokumentasi DevOps Agen Amazon
- Harga Amazon DevOps Guru
- AWS Dukungan

Jika Anda memiliki pertanyaan tambahan, hubungi AWS Dukungan.

Transisi dari Amazon DevOps Guru ke Amazon CloudWatch dan Amazon DevOps Agen

Amazon DevOps Guru mencapai akhir dukungan pada 30 September 2027. Setelah tanggal ini, DevOps Guru tidak lagi menganalisis sumber daya Anda dan wawasan yang dihasilkan sebelumnya tidak lagi tersedia. Dasar Anda AWS infrastruktur dan beban kerja tidak terpengaruh. Hanya DevOps Lapisan pemantauan Guru dihapus.

Panduan ini membantu Anda memahami apa yang berubah dan tindakan apa yang perlu Anda ambil. Amazon CloudWatch menyediakan deteksi anomali dan peringatan untuk sumber daya Anda, dan Amazon DevOps Agen menyediakan AI-assisted penyelidikan. Beban kerja Anda tetap di tempatnya tanpa perlu migrasi.

Topik

- Bagaimana DevOps Guru dan penggantinya berbeda
- Bagaimana transisi bekerja
- Bagaimana kami mendukung Anda melalui transisi
- Siapa yang perlu bertindak, dan kapan
- Apa yang berubah sekilas
- Deteksi anomali metrik dan peringatan
- Deteksi anomali log
- Deteksi anomali database
- Investigasi dan analisis akar penyebab
- Wawasan proaktif
- Infrastruktur sebagai kode dan penggunaan CLI
- Integrasi API
- Ekspor data Anda
- Hapus DevOps Sumber daya Guru
- Garis waktu dan dukungan
- Daftar periksa transisi
- Pertanyaan umum

- Sumber daya terkait

Bagaimana DevOps Guru dan penggantinya berbeda

Amazon DevOps Guru menggunakan model terkelola: Anda menambahkan sumber daya ke cakupannya, dan ia mempelajari perilaku normal mereka, mendeteksi anomali, mengelompokkan anomali terkait ke dalam wawasan, dan merekomendasikan tindakan. Anda tidak memilih metrik mana yang akan dianalisis atau mengonfigurasi ambang batas.

Amazon CloudWatch menggunakan model yang dikonfigurasi: Anda memilih metrik dan grup log untuk dipantau, dan Anda membuat detektor anomali, alarm, dan tindakan notifikasi. Ini membutuhkan pengaturan satu kali, dan ini memberi Anda kontrol langsung atas apa yang dipantau, seberapa sensitif setiap alarm, dan ke mana pemberitahuan pergi. Amazon DevOps Agen menyediakan penyelidikan dan analisis akar penyebab yang DevOps Wawasan Guru disediakan, dimulai dari a CloudWatch alarm atau sesuai permintaan.

Anda dapat menggunakan keduanya bersama-sama: CloudWatch mendeteksi dan memperingatkan, dan Amazon DevOps Agen membantu Anda menyelidiki dan menemukan akar penyebab.

Bagaimana transisi bekerja

Kami tidak memigrasikan beban kerja Anda. Aplikasi, database, dan infrastruktur Anda tetap di tempatnya. Ini adalah perubahan konfigurasi pemantauan, bukan migrasi beban kerja.

Transisi memiliki empat bagian:

1. Mereproduksi deteksi dan peringatan yang Anda andalkan di Amazon CloudWatch.
2. Siapkan Amazon DevOps Agen untuk penyelidikan.
3. Hapus DevOps Guru dari infrastruktur Anda sebagai template kode dan integrasi API.
4. Ekspor wawasan apa pun yang ingin Anda simpan, lalu setel cakupan analisis Anda ke Tidak Ada.

Anda dapat melakukan transisi satu akun atau aplikasi pada satu waktu, dan Anda dapat menjalankannya DevOps Guru dan CloudWatch berdampingan saat Anda memvalidasi konfigurasi baru Anda. Karena DevOps Guru tidak meng-host beban kerja Anda, tidak ada downtime selama transisi. Untuk panduan tentang layanan mana yang harus dipindahkan setiap kasus penggunaan, lihat Memilih jalur migrasi yang tepat di akhir halaman dukungan.

Bagaimana kami mendukung Anda melalui transisi

Hingga 30 September 2027, DevOps Guru terus beroperasi secara normal. Kami terus menyediakan tambalan keamanan, perbaikan bug kritis, dan dukungan melalui AWS Saluran dukungan, dan kami menjaga ketersediaan layanan. Tidak ada fitur baru yang ditambahkan.

Yang Amazon DevOps Guru berakhir dukungan halaman adalah referensi yang dikelola untuk tanggal dan langkah migrasi. Jika Anda memiliki pertanyaan selama transisi, hubungi AWS Dukungan. Sebaiknya selesaikan transisi Anda sebelum 30 Juni 2027 untuk mengizinkan buffer sebelum akhir tanggal dukungan 30 September 2027.

Siapa yang perlu bertindak, dan kapan

Dampak dari perubahan ini tergantung pada bagaimana Anda menggunakan DevOps Guru.

Jika Anda	Apa yang terjadi di akhir dukungan	Prioritas
Deklarasikan DevOps Sumber daya Guru di AWS CloudFormation, AWS CDK, atau templat Terraform	Operasi tumpukan yang mereferen sikan jenis sumber daya yang ditarik gagal. Satu sumber daya yang gagal dapat memblokir seluruh pembaruan tumpukan.	Tertinggi. Selesaikan ini dulu.
Panggil DevOps Guru API dari dasbor, sistem tiket, atau alat internal	Integrasi berhenti mengembalikan data.	Tinggi
Gunakan DevOps Konsol Guru untuk wawasan dan peringatan, termasuk DevOps Guru untuk Amazon RDS	Anda kehilangan deteksi anomali dan rekomendasi untuk sumber daya dalam cakupan.	Sedang
Ingin menyimpan catatan wawasan masa lalu	Wawasan tidak lagi tersedia. Ekspor sebelum Anda menghapus cakupan.	Sebelum Anda keluar

Selesaikan semua tindakan sebelum 30 September 2027. Sebaiknya selesaikan transisi Anda pada 30 Juni 2027 sehingga Anda dapat memvalidasi CloudWatch dan Amazon DevOps Konfigurasi agen sementara DevOps Guru masih tersedia untuk perbandingan.

Apa yang berubah sekilas

Tabel berikut merangkum apa yang tersedia setelah transisi dan apa yang berbeda dari DevOps Guru.

Kemampuan	Tersedia setelah transisi?	Apa yang berbeda
Deteksi anomali metrik	Ya, dikonfigurasi pelanggan	CloudWatch deteksi anomali mempelajari rentang yang diharapkan dari setiap metrik secara otomatis. Anda memilih metrik mana yang akan diaktifkan.
Peringatan operasional	Ya, dikonfigurasi pelanggan	Gunakan alarm deteksi anomali dan alarm komposit, dan rute perubahan status alarm ke Amazon SNS atau Amazon EventBridge. Anda menentukan alarm daripada menerimanya secara otomatis.
Deteksi anomali log	Ya, cakupan yang sama	Aktifkan deteksi anomali langsung pada Anda CloudWatch Log grup log dan selidiki dengan CloudWatch Wawasan Log.
Deteksi anomali database (DevOps Guru untuk Amazon RDS)	Ya, cakupan yang sama	CloudWatch Database Insights menunjukkan beban database yang sama, acara tunggu, dan data SQL teratas yang DevOps Guru untuk Amazon RDS dianalisis. Buat CloudWatch alarm deteksi anomali pada metrik DBLoad untuk diberitahu tentang beban abnormal, lalu jalankan analisis kinerja sesuai permintaan di Database Insights untuk periode alarm untuk mengidentifikasi penyebabnya.
CloudWatch alarm yang Anda tambahkan DevOps Guru	Ya, cakupan yang sama	Alarm Anda tidak berubah. Gunakan mereka untuk memulai penyelidikan di AWS DevOps Agen atau CloudWatch.
Wawasan yang dikelompokkan	Ya, yang diprakarsai oleh pelanggan	Amazon DevOps Agen dan CloudWatch investigasi mengkorelasikan metrik, log, peristiwa perubahan, dan jejak untuk mengidentifikasi akar penyebab. Investiga

Kemampuan	Tersedia setelah transisi?	Apa yang berbeda
dengan analisis akar penyebab		si dimulai dari alarm atau sesuai permintaan daripada berjalan terus menerus.
Konteks ketergantungan layanan	Ya, dikonfigurasi pelanggan	Aktifkan AWS X-Ray dan CloudWatch Sinyal Aplikasi sehingga penyelidikan dapat memetakan hubungan layanan.
Rekomendasi dan remediasi	Ya, yang diprakarsai oleh pelanggan	DevOps Guru melampirkan rekomendasi untuk setiap wawasan. Amazon DevOps Agen menghasilkan rekomendasi selama penyelidikan, dan AWS Systems Manager Otomatisasi menjalankan runbook remediasi yang Anda tentukan.
Notifikasi	Ya, cakupan yang sama	Amazon SNS, Amazon EventBridge, dan Manajer Sistem OpsCenter adalah tujuan yang sama DevOps Guru digunakan. Anda menghubungkannya dengan CloudWatch alarm.
Wawasan proaktif	Tidak tersedia	DevOps Wawasan proaktif Guru berakhir dengan layanan. Untuk sumber daya di mana peringatan dini penting bagi Anda, Anda dapat membuat CloudWatch alarm pada ambang pemanfaatan dan alarm penggunaan Kuota Layanan pada kuota akun Anda.

Deteksi anomali metrik dan peringatan

Dalam DevOps Guru, deteksi anomali pada metrik sumber daya dimulai secara otomatis ketika sumber daya berada dalam cakupan. Dalam CloudWatch, Anda mengaktifkan deteksi anomali pada metrik yang Anda pilih dan membuat alarm pada metrik tersebut.

Apa yang perlu Anda lakukan

1. Identifikasi metrik yang Anda andalkan DevOps Guru untuk menganalisis, seperti pemanfaatan CPU, jumlah permintaan, tingkat kesalahan 4XX dan 5XX, latensi, jumlah host yang tidak sehat, memori, dan disk.

2. Aktifkan CloudWatch deteksi anomali pada metrik tersebut. CloudWatch mempelajari rentang yang diharapkan dari setiap metrik dari sejarahnya.
3. Buat alarm deteksi anomali. Gunakan alarm komposit untuk menggabungkan alarm terkait dan mengurangi kebisingan.
4. Tambahkan tindakan alarm yang mengirim pemberitahuan ke topik Amazon SNS Anda yang ada atau Amazon EventBridge aturan.

Apa yang berubah

Deteksi berlaku untuk metrik yang Anda pilih, bukan untuk setiap sumber daya dalam batas cakupan. Anda mengontrol sensitivitas alarm, periode evaluasi, dan perutean notifikasi.

Deteksi anomali log

Dalam DevOps Guru, anomali log muncul di samping anomali metrik dalam wawasan. Dalam CloudWatch, Anda mengaktifkan deteksi anomali pada setiap grup log dan melihat anomali di CloudWatch Konsol log.

Apa yang perlu Anda lakukan

1. Aktifkan CloudWatch Deteksi anomali log pada grup log penting Anda.
2. Gunakan CloudWatch Logs Wawasan untuk menanyakan dan menyelidiki peristiwa log di balik anomali.
3. Jika Anda menyatakan `AWS::DevOpsGuru::LogAnomalyDetectionIntegration` jenis sumber daya, hapus dari template Anda. Lihat Infrastruktur sebagai kode dan penggunaan CLI.

Apa yang berubah

Anomali log ditampilkan per grup log di CloudWatch bukannya dikelompokkan menjadi DevOps Wawasan guru. Untuk menghubungkan anomali log dengan anomali metrik, mulai Amazon DevOps Investigasi agen.

Deteksi anomali database

Dalam DevOps Guru untuk Amazon RDS, anomali dalam pemuatan database untuk Layanan Database Relasional Amazon Anda dan database Amazon Aurora dilaporkan sebagai wawasan

dengan rekomendasi untuk peristiwa tunggu yang terlibat. Dalam CloudWatch, Database Insights menyediakan data Performance Insights yang sama, dan Anda membuat alarm untuk peringatan.

Apa yang perlu Anda lakukan

1. Aktifkan CloudWatch Wawasan Database Untuk database yang DevOps Guru untuk Amazon RDS tercakup.
2. Buat CloudWatch alarm pada `DBLoad` metrik dan metrik peristiwa tunggu yang penting untuk beban kerja Anda.
3. Sertakan alarm database di Amazon Anda DevOps Investigasi agen di samping alarm aplikasi Anda.

Apa yang berubah

Database Insights menyediakan dasbor tingkat armada dan analisis kontributor teratas untuk beban database. Deteksi anomali pada pemuatan database menjadi alarm yang Anda konfigurasikan daripada wawasan yang DevOps Guru terbuka untuk Anda.

Investigasi dan analisis akar penyebab

Dalam DevOps Guru, anomali terkait dikelompokkan menjadi wawasan dengan rekomendasi. AWS DevOps Agen menyediakan AI-assisted investigasi yang menghubungkan metrik, log, jejak, dan penerapan terbaru serta perubahan konfigurasi untuk mengidentifikasi akar penyebab. CloudWatch Investigasi menyediakan jenis investigasi yang sama dari dalam CloudWatch konsol.

Apa yang perlu Anda lakukan

1. Siapkan Amazon DevOps Agen untuk akun Anda.
2. Aktifkan AWS X-Ray dan CloudWatch Sinyal Aplikasi sehingga investigasi memiliki topologi layanan dan konteks jejak.
3. Konfigurasikan CloudWatch alarm untuk memulai penyelidikan, atau memulai penyelidikan sesuai permintaan ketika masalah terjadi.

Apa yang berubah

Investigasi dimulai dari alarm atau sesuai permintaan daripada berjalan terus menerus. Anda menerima hipotesis akar penyebab yang dapat Anda tinjau dan ditindaklanjuti, dan Anda dapat menjalankan runbook remediasi yang telah Anda tentukan AWS Systems Manager Otomatisasi

Wawasan proaktif

Dalam DevOps Guru, wawasan proaktif memperingatkan Anda tentang kondisi yang dapat menyebabkan masalah, seperti sumber daya mendekati batas kapasitasnya atau konfigurasi yang meningkatkan risiko. Wawasan proaktif bukanlah bagian dari CloudWatch atau Amazon DevOps Agen, dan mereka berakhir dengan layanan.

Untuk sumber daya di mana peringatan dini penting bagi Anda, buat CloudWatch alarm yang memberi tahu Anda sebelum batas tercapai:

1. Buat alarm pada metrik pemanfaatan dengan ambang batas di bawah batas, misalnya pada 80 persen dari kapasitas yang disediakan, dengan periode evaluasi yang cukup lama untuk mengabaikan lonjakan singkat.
2. Buat alarm penggunaan Kuota Layanan untuk kuota tingkat akun yang bergantung pada beban kerja Anda, seperti eksekusi Lambda bersamaan dan kapasitas akun DynamoDB. Untuk informasi lebih lanjut, lihat Menciptakan CloudWatch alarm untuk Kuota Layanan.

Apa yang berubah

Anda menentukan kondisi yang memperingatkan Anda, dan Anda memilih sumber daya yang mereka terapkan. DevOps Guru memilih kondisi dan sumber daya untuk Anda.

Infrastruktur sebagai kode dan penggunaan CLI

Template dan tumpukan yang mereferensikan jenis sumber daya berikut gagal dibuat atau diperbarui setelah jenis sumber daya ditarik:

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

Terraform AWS penyedia mengekspos yang setara `aws_devopsguru_resource_collection`, `aws_devopsguru_notification_channel`, `aws_devopsguru_event_sources_config`, dan `aws_devopsguru_service_integration` sumber daya.

Apa yang perlu Anda lakukan

1. Inventarisasi AWS CloudFormation, AWS CDK, dan templat Terraform dan AWS Skrip CLI yang mereferensikan jenis sumber daya ini.
2. Buat yang setara CloudWatch konfigurasi: alarm, topik Amazon SNS, dan Amazon EventBridge Aturan yang menggantikan DevOps Saluran dan cakupan notifikasi Guru, dan CloudWatch Detektor anomali log yang menggantikan integrasi deteksi anomali log.
3. Hapus DevOps Guru sumber daya dari templat Anda dan terapkan perubahan sehingga sumber daya tidak lagi dikelola oleh tumpukan Anda. Hapus mereka dari templat Anda daripada menghapusnya di luar band, sehingga tumpukan dan templat Anda tetap sesuai.

Apa yang berubah

Karena satu sumber daya yang gagal dapat memblokir seluruh operasi tumpukan, ini adalah dampak tingkat keparahan tertinggi. Selesaikan dulu.

Integrasi API

Jika dasbor, sistem tiket, atau alat internal Anda memanggil DevOps Guru API, perbarui mereka untuk menggunakan yang setara CloudWatch Operasi API sebelum akhir dukungan. Setelah dukungan berakhir, DevOps Operasi API Guru tidak lagi tersedia.

Jika perkakas Anda memanggil	Gunakan sebagai gantinya
`ListInsights` , `DescribeInsight` , `ListAnomaliesForInsight`	CloudWatch `DescribeAlarms` , `DescribeAlarmHistory` , dan `GetMetricData` ; CloudWatch Log `ListLogAnomalyDetectors` dan `ListAnomalies`
`ListRecommendations`	Amazon DevOps Hasil investigasi agen
`DescribeAccountHealth` , `DescribeResourceCollectionHealth`	CloudWatch `DescribeAlarms` disaring oleh status alarm, atau alarm komposit untuk setiap aplikasi

Jika perkakas Anda memanggil	Gunakan sebagai gantinya
`ListNotificationChannels` , `AddNotificationChannel`	Topik Amazon SNS dan Amazon EventBridge aturan untuk CloudWatch perubahan keadaan alarm

Untuk detail API, lihat Amazon DevOps Referensi API Guru dan Amazon CloudWatch Referensi API.

Ekspor data Anda

DevOps Wawasan Guru tidak tersedia setelah 30 September 2027. Jika Anda ingin menyimpan catatan wawasan Anda, ekspor sebelum tanggal tersebut. Kami menyarankan sebagian besar pelanggan melakukan kedua hal berikut:

1. Dapatkan wawasan baru hingga dukungan berakhir. Konfigurasikan saluran notifikasi Amazon SNS sehingga setiap wawasan baru dikirimkan ke topik yang dapat Anda arsipkan.
2. Ekspor wawasan yang telah Anda kumpulkan. Panggilan `ListInsights` untuk mencantumkannya, lalu menelepon `DescribeInsight`, `ListAnomaliesForInsight`, dan `ListRecommendations` untuk setiap wawasan yang ingin Anda simpan. Simpan tanggapan di Amazon S3 atau sistem tiket Anda.

Selesaikan ekspor Anda sebelum mengurangi cakupan atau menghapus sumber daya.

Hapus DevOps Sumber daya Guru

Untuk menghentikan analisis dan menghentikan biaya sebelum dukungan berakhir, hapus cakupan dan saluran notifikasi Anda setelah Anda mengekspor data dan mengatur CloudWatch konfigurasi.

1. Tetapkan cakupan analisis Anda ke Tidak ada Untuk setiap akun dan AWS Wilayah dimana DevOps Guru diaktifkan. Di konsol, pilih Pengaturan, lalu DevOps Cakupan analisis Guru, lalu Kelola, lalu Tidak ada. Anda juga dapat menelepon `UpdateResourceCollection` untuk menghapus CloudFormation tumpukan atau tag yang menentukan batas cakupan Anda.
2. Hapus saluran notifikasi Anda. Panggilan `RemoveNotificationChannel`, atau menghapusnya dari Pengaturan di konsol. Menghapus saluran tidak menghapus topik Amazon SNS atau apa pun yang telah Anda arsipkan melaluinya.

3. Jika Anda menyatakan DevOps Guru sumber daya dalam infrastruktur sebagai kode, hapus dari template Anda daripada menghapusnya di luar band. Lihat Infrastruktur sebagai kode dan penggunaan CLI.

Garis waktu dan dukungan

Tonggak pencapaian	Date
Pengumuman	September 29, 2026
Tidak ada pelanggan baru	Oktober 29, 2026
Penyelesaian transisi yang disarankan	Juni 30, 2027
Akhir dukungan	30 September 2027

Kami sarankan menyelesaikan transisi Anda sebelum 30 Juni 2027 sehingga Anda dapat memvalidasi CloudWatch dan Amazon DevOps Konfigurasi agen terhadap operasi langsung sementara DevOps Guru masih tersedia untuk perbandingan. Jika Anda memiliki pertanyaan selama transisi, hubungi AWS Dukungan.

Daftar periksa transisi

- Inventaris AWS CloudFormation, AWS CDK, Terraform, dan AWS Penggunaan CLI dari `AWS::DevOpsGuru::ResourceCollection`, `AWS::DevOpsGuru::NotificationChannel`, dan `AWS::DevOpsGuru::LogAnomalyDetectionIntegration`.
- Identifikasi setiap integrasi API yang dibaca DevOps Wawasan guru.
- Aktifkan CloudWatch deteksi anomali pada metrik utama Anda dan buat alarm.
- Aktifkan CloudWatch Deteksi anomali log pada grup log penting Anda.
- Aktifkan CloudWatch Database Insights untuk database yang DevOps Guru untuk Amazon RDS tercakup.
- Aktifkan AWS X-Ray dan CloudWatch Sinyal Aplikasi.
- Siapkan Amazon DevOps Agen untuk penyelidikan.
- Konfigurasikan pemberitahuan dengan Amazon SNS, Amazon EventBridge, atau Manajer Sistem OpsCenter.

- Ekspor DevOps Wawasan Guru melalui saluran notifikasi Amazon SNS dan API.
- Hapus DevOps Guru sumber daya dari template Anda dan atur cakupan analisis ke Tidak Ada.

Pertanyaan umum

Apakah aplikasi atau database saya berhenti bekerja setelah dukungan berakhir?

Tidak. DevOps Guru adalah layanan pemantauan. Ini mengamati sumber daya yang Anda jalankan, itu tidak meng-host mereka. Setelah dukungan berakhir, Anda kalah DevOps Visibilitas dan rekomendasi Guru, tetapi beban kerja Anda terus berjalan.

Apa yang terjadi jika saya tidak bermigrasi tepat waktu?

Anda tidak akan lagi dapat mengakses DevOps Konsol Guru atau API, dan DevOps Jenis sumber daya Guru akan gagal AWS CloudFormation dan AWS CLI. Wawasan tidak akan tersedia lagi.

Bisakah saya terus menggunakan DevOps Guru sampai akhir dukungan?

Ya, jika akun Anda mendaftar sebelum 29 Oktober 2026. Sampai akhir dukungan, kami menyediakan patch keamanan, perbaikan bug kritis, dukungan, dan ketersediaan yang terjaga. Tidak ada fitur baru yang ditambahkan.

Apakah ada satu layanan yang menggantikan DevOps Guru satu-ke-satu?

Tidak. DevOps Peta deteksi dan peringatan Guru ke Amazon CloudWatch, dan penyelidikan dan analisis akar penyebabnya dipetakan ke Amazon DevOps Agen. Anda dapat menggunakan keduanya bersama-sama.

Apa yang terjadi pada DevOps Guru untuk Amazon RDS?

Itu berakhir dengan sisa layanan. CloudWatch Database Insights menyediakan data Performance Insights yang sama. Buat alarm pada beban database untuk peringatan.

Sumber daya terkait

- Amazon DevOps Guru berakhir dukungan
- Layanan di Sunset di AWS Referensi Umum
- Amazon CloudWatch Panduan Pengguna
- Menggunakan CloudWatch deteksi anomali
- CloudWatch Deteksi anomali log

- CloudWatch Wawasan Database
- CloudWatch investigasi
- Amazon DevOps Panduan Pengguna Agen
- Amazon CloudWatch harga
- AWS Dukungan

Menyiapkan Amazon DevOps Guru

Selesaikan tugas di bagian ini untuk mengatur Amazon DevOps Guru untuk pertama kalinya. Jika Anda sudah memiliki AWS akun, tahu yang mana AWS akun atau akun yang ingin Anda analisis, dan memiliki topik Layanan Pemberitahuan Sederhana Amazon untuk digunakan untuk pemberitahuan wawasan, Anda dapat melanjutkan ke Memulai dengan DevOps Guru.

Secara opsional, Anda dapat menggunakan Quick Setup, kemampuan AWS Systems Manager, untuk mengatur DevOps Guru dan cepat mengkonfigurasi opsinya. Anda dapat menggunakan Quick Setup untuk mengatur DevOps Guru untuk akun mandiri atau organisasi. Untuk menggunakan Pengaturan Cepat di Manajer Sistem untuk mengatur DevOps Guru untuk sebuah organisasi, Anda harus memiliki prasyarat berikut:

- Sebuah organisasi dengan AWS Organizations. Untuk informasi lebih lanjut, lihat AWS Organizations terminologi dan konsep di AWS Organizations Panduan Pengguna.
- Dua atau lebih unit organisasi (OU).
- Satu atau lebih target AWS akun di setiap OU.
- Satu akun administrator dengan hak istimewa untuk mengelola akun target.

Untuk mempelajari cara mengatur DevOps Guru menggunakan Quick Setup, lihat Konfigurasikan DevOps Guru dengan Pengaturan Cepat di AWS Systems Manager Panduan Pengguna.

Gunakan langkah-langkah berikut untuk mengatur DevOps Guru tanpa Pengaturan Cepat.

- Langkah 1 - Mendaftar untuk AWS
- Langkah 2 - Tentukan cakupan untuk DevOps Guru
- Langkah 3 - Identifikasi topik pemberitahuan Amazon SNS Anda

Langkah 1 - Mendaftar untuk AWS

Mendaftar untuk Akun AWS

Untuk memulai dengan AWS, Anda membutuhkan Akun AWS. Ada dua cara untuk mendaftar AWS. Jika Anda ingin kontrol penuh atas konfigurasi akun dan tempat penyimpanan konten Anda, atau jika Anda telah mengatur beban kerja seperti HIPAA atau FedRAMP, gunakan Mendaftar untuk AWS (lanjutan). Jika Anda adalah pengguna baru dan ingin menggunakan login yang sudah Anda miliki

untuk masuk AWS dan buat AWS lingkungan dengan default yang telah dikonfigurasi sebelumnya dalam pilihan Wilayah AWS, gunakan Mendaftar untuk AWS.

Langkah 2 - Tentukan cakupan untuk DevOps Guru

Cakupan batas Anda menentukan AWS sumber daya yang dianalisis oleh Amazon DevOps Guru untuk perilaku anomali. Kami menyarankan Anda mengelompokkan sumber daya ke dalam aplikasi operasional Anda. Semua sumber daya di batas sumber daya Anda harus terdiri dari satu atau lebih aplikasi Anda. Jika Anda memiliki satu solusi operasional, maka batas cakupan Anda harus mencakup semua sumber dayanya. Jika Anda memiliki beberapa aplikasi, pilih sumber daya yang membentuk setiap solusi dan kelompokkan bersama-sama menggunakan CloudFormation tumpukan atau AWS tag. Semua sumber daya gabungan yang Anda tentukan, apakah mereka mendefinisikan satu atau lebih aplikasi, dianalisis oleh DevOps Guru dan buat batas cakupannya.

Gunakan salah satu metode berikut untuk menentukan sumber daya dalam solusi operasional Anda.

- Pilih untuk memiliki AWS Wilayah dan akun menentukan batas cakupan Anda. Dengan opsi ini, DevOps Guru menganalisis semua sumber daya di akun dan Wilayah Anda. Ini adalah opsi yang baik untuk dipilih jika Anda menggunakan akun Anda hanya untuk satu aplikasi.
- Gunakan CloudFormation tumpukan untuk menentukan sumber daya dalam aplikasi operasional Anda. CloudFormation template menentukan dan menghasilkan sumber daya Anda untuk Anda. Tentukan tumpukan yang membuat sumber daya aplikasi Anda saat Anda mengonfigurasi DevOps Guru. Anda dapat memperbarui tumpukan Anda kapan saja. Semua sumber daya di tumpukan yang Anda pilih menentukan cakupan batas Anda. Untuk informasi selengkapnya, lihat Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.
- Gunakan AWS tag untuk menentukan AWS sumber daya dalam aplikasi Anda. DevOps Guru hanya menganalisis sumber daya yang berisi tag yang Anda pilih. Sumber daya tersebut membentuk batas Anda.

  Sebuah AWS Tag terdiri dari tag kunci dan tag nilai. Anda dapat menentukan satu tag kunci dan Anda dapat menentukan satu atau lebih nilai-nilai dengan itu kunci. Gunakan satu nilai untuk semua sumber daya di salah satu aplikasi Anda. Jika Anda memiliki beberapa aplikasi, maka gunakan tag dengan yang sama kunci untuk semuanya, dan kelompokkan sumber daya ke dalam aplikasi Anda menggunakan tag ' nilai-nilai. Semua sumber daya dengan tag yang Anda pilih membentuk batas cakupan untuk DevOps Guru. Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

Jika cakupan batas Anda mencakup sumber daya yang membentuk lebih dari satu aplikasi, Anda dapat menggunakan tag untuk memfilter wawasan Anda dengan melihatnya berdasarkan satu aplikasi pada satu waktu. Untuk informasi selengkapnya, lihat Langkah 4 di Melihat wawasan DevOps Guru.

Untuk informasi selengkapnya, lihat Mendefinisikan aplikasi menggunakan sumber daya AWS. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat Amazon DevOps Harga Guru.

Langkah 3 - Identifikasi topik pemberitahuan Amazon SNS Anda

Anda menggunakan satu atau dua topik Amazon SNS untuk menghasilkan pemberitahuan tentang hal penting DevOps Peristiwa guru, seperti ketika wawasan dibuat. Ini memastikan Anda tahu tentang masalah yang DevOps Guru menemukan sesegera mungkin. Siapkan topik Anda saat Anda mengatur DevOps Guru. Saat Anda menggunakan DevOps Konsol Guru untuk mengatur DevOps Guru, Anda menentukan topik notifikasi menggunakan namanya atau Nama Sumber Daya Amazon (ARN). Untuk informasi lebih lanjut, lihat Aktifkan DevOps Guru. Anda dapat menggunakan konsol Amazon SNS untuk melihat nama dan ARN untuk setiap topik Anda. Jika Anda tidak memiliki topik, Anda dapat membuatnya saat Anda mengaktifkan DevOps Guru menggunakan DevOps Konsol Guru. Untuk informasi lebih lanjut, lihat Membuat topik di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Izin ditambahkan ke topik Amazon SNS Anda

Topik Amazon SNS adalah sumber daya yang berisi AWS Identity and Access Management (IAM) kebijakan sumber daya. Ketika Anda menentukan topik di sini, DevOps Guru menambahkan izin berikut ke kebijakan sumber dayanya.

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

Izin ini diperlukan untuk DevOps Guru untuk mempublikasikan notifikasi menggunakan topik. Jika Anda memilih untuk tidak memiliki izin ini pada topik, Anda dapat menghapusnya dengan aman dan topik akan terus berfungsi seperti sebelum Anda memilihnya. Namun, jika izin yang ditambahkan ini dihapus, DevOps Guru tidak dapat menggunakan topik untuk menghasilkan notifikasi.

Memperkirakan biaya analisis sumber daya Amazon DevOps Guru

Anda dapat memperkirakan biaya bulanan Amazon DevOps Guru untuk menganalisis sumber daya AWS Anda. Anda membayar jumlah jam yang dianalisis untuk setiap sumber daya AWS aktif dalam cakupan sumber daya yang ditentukan. Sumber daya aktif jika menghasilkan metrik, peristiwa, atau log dalam waktu satu jam.

DevOps Guru memindai sumber daya pilihan Anda untuk membuat perkiraan biaya bulanan. Anda dapat melihat sumber daya, harga per jam yang dapat ditagih, dan perkiraan biaya bulanannya. Estimator biaya mengasumsikan sebagai default bahwa sumber daya aktif yang dianalisis digunakan 100 persen dari waktu. Anda dapat mengubah persentase ini untuk setiap layanan yang dianalisis berdasarkan perkiraan penggunaan Anda untuk membuat perkiraan biaya bulanan yang diperbarui. Perkiraannya adalah biaya untuk menganalisis sumber daya Anda dan tidak termasuk biaya yang terkait dengan panggilan DevOps Guru API.

Anda dapat membuat satu perkiraan biaya pada satu waktu. Waktu yang diperlukan untuk menghasilkan perkiraan biaya tergantung pada jumlah sumber daya yang Anda tentukan saat Anda membuat perkiraan biaya. Saat Anda menentukan beberapa sumber daya, dibutuhkan 1 hingga 2 jam untuk menyelesaikannya. Ketika Anda menentukan banyak sumber daya, itu bisa memakan waktu hingga 4 jam untuk menyelesaikannya. Biaya aktual Anda bervariasi dan tergantung pada persentase waktu sumber daya aktif Anda yang dianalisis digunakan.

> **Note**
>
> Untuk perkiraan biaya, Anda hanya dapat menentukan satu CloudFormation tumpukan. Untuk batas cakupan aktual Anda, Anda dapat menentukan hingga 1000 tumpukan.

Untuk membuat estimasi biaya analisis sumber daya bulanan

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Pilih Penaksir biaya di panel navigasi.
3. Jika Anda belum mengaktifkan DevOps Guru, Anda harus membuat peran IAM. Di jendela popup Create IAM role for DevOps Guru yang muncul, pilih Agree to create IAM role. Hal ini memungkinkan DevOps Guru untuk membuat peran terkait layanan IAM untuk Anda ketika Anda

memilih untuk memulai analisis perkiraan biaya atau mulai menggunakan Guru. DevOps Dengan begitu, DevOps Guru memiliki izin yang diperlukan untuk membuat perkiraan biaya. Jika Anda telah mengaktifkan DevOps Guru, peran telah dibuat dan opsi ini tidak muncul.

4. Pilih sumber daya yang ingin Anda gunakan untuk membuat perkiraan Anda.

   - Jika Anda ingin memperkirakan biaya DevOps Guru untuk menganalisis sumber daya yang ditentukan oleh satu CloudFormation tumpukan, lakukan hal berikut.

     1. Pilih CloudFormation tumpukan di Wilayah saat ini.
     2. Di Pilih CloudFormation tumpukan, pilih nama CloudFormation tumpukan di AWS akun Anda. Anda juga dapat memasukkan nama tumpukan untuk menemukannya dengan cepat. Untuk informasi tentang bekerja dengan dan melihat tumpukan Anda, lihat Bekerja dengan tumpukan di CloudFormation Panduan Pengguna.
     3. (Opsional) Jika Anda menggunakan CloudFormation tumpukan yang saat ini tidak Anda analisis, pilih Aktifkan analisis sumber daya untuk memungkinkan DevOps Guru mulai menganalisis sumber dayanya. Opsi ini tidak tersedia jika Anda belum mengaktifkan DevOps Guru atau jika Anda sudah menganalisis sumber daya di tumpukan.

   - Jika Anda ingin memperkirakan biaya DevOps Guru untuk menganalisis sumber daya dengan tag, lakukan hal berikut.

     1. Pilih Tag pada AWS sumber daya di Wilayah saat ini
     2. Di kunci Tag pilih kunci tag Anda
     3. Di Nilai tag pilih (semua nilai) atau pilih satu nilai.

   - Jika Anda ingin memperkirakan biaya DevOps Guru untuk menganalisis sumber daya di AWS akun dan Wilayah Anda, pilih AWS akun di Wilayah saat ini.

5. Pilih Perkirakan biaya bulanan.

6. (Opsional) Di kolom% pemanfaatan sumber daya aktif, masukkan nilai persentase yang diperbarui untuk satu atau beberapa layanan AWS. % pemanfaatan sumber daya aktif default adalah 100%. Ini berarti bahwa DevOps Guru menghasilkan perkiraan untuk layanan AWS dengan menghitung biaya satu jam menganalisis sumber dayanya, kemudian mengekstrapolasinya selama 30 hari dengan total 720 jam. Jika layanan aktif kurang dari 100% dari waktu, Anda dapat memperbarui persentase berdasarkan perkiraan penggunaan Anda untuk perkiraan yang lebih akurat. Misalnya, jika Anda memperbarui pemanfaatan sumber daya aktif layanan menjadi 75%, biaya satu jam untuk menganalisis sumber dayanya diekstrapolasi selama (720 x 0,75) jam, atau 540 jam.

Jika perkiraan Anda nol dolar, maka sumber daya yang Anda pilih kemungkinan tidak termasuk sumber daya yang didukung oleh DevOps Guru. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

Memulai dengan DevOps Guru

Di bagian ini, Anda mempelajari cara memulai dengan Amazon DevOps Guru sehingga dapat menganalisis data dan metrik operasional aplikasi Anda untuk menghasilkan wawasan.

Topik

- Langkah 1: Siapkan
- Langkah 2: Aktifkan DevOps Guru
- Langkah 3: Tentukan DevOps Cakupan sumber daya Guru

Langkah 1: Siapkan

Sebelum Anda memulai, persiapkan dengan menjalankan langkah-langkah di Menyiapkan Amazon DevOps Guru.

Langkah 2: Aktifkan DevOps Guru

Untuk mengkonfigurasi Amazon DevOps Guru untuk digunakan untuk pertama kalinya, Anda harus memilih bagaimana Anda ingin mengatur DevOps Guru. Anda dapat memantau aplikasi di seluruh organisasi atau memantau aplikasi di akun Anda saat ini.

Anda dapat memantau aplikasi di seluruh organisasi atau mengaktifkan DevOps Guru untuk akun saat ini secara eksklusif. Prosedur berikut menguraikan berbagai cara untuk mengatur DevOps Guru berdasarkan kebutuhan Anda.

Memantau akun di seluruh organisasi

Jika Anda memilih untuk memantau aplikasi di seluruh organisasi Anda, masuk ke akun manajemen organisasi Anda. Anda dapat secara opsional mengatur akun anggota organisasi sebagai administrator yang didelegasikan. Anda hanya dapat memiliki satu administrator yang didelegasikan pada satu waktu dan dapat mengubah pengaturan administrator nanti. Akun manajemen dan akun administrator yang didelegasikan yang Anda atur memiliki akses ke semua wawasan di semua akun di organisasi Anda.

Anda dapat menambahkan dukungan lintas akun untuk organisasi Anda menggunakan Konsol, atau Anda dapat melakukannya dengan menggunakan AWS CLI.

Di atas kapal dengan DevOps Konsol Guru

Anda dapat menggunakan Konsol untuk menambahkan dukungan untuk akun di seluruh organisasi Anda.

Gunakan Konsol untuk mengaktifkan DevOps Guru untuk melihat wawasan agregat

1. Buka Amazon DevOps Konsol Guru di https://console.aws.amazon.com/devops-guru/.
2. Memilih Memantau aplikasi di seluruh organisasi Anda sebagai tipe setup.
3. Pilih akun mana yang ingin Anda gunakan sebagai administrator yang didelegasikan. Kemudian, pilih Daftarkan administrator yang didelegasikan. Ini memberikan akses ke tampilan konsolidasi untuk setiap akun yang memiliki DevOps Guru diaktifkan. Administrator yang didelegasikan memiliki pandangan konsolidasi dari semua DevOps Wawasan dan metrik Guru di seluruh organisasi Anda. Anda dapat mengaktifkan akun lain dengan pengaturan cepat SSM atau AWS CloudFormation set tumpukan. Untuk mempelajari lebih lanjut tentang penyiapan cepat, lihat Konfigurasikan DevOps Guru dengan Pengaturan Cepat. Untuk mempelajari selengkapnya tentang pengaturan dengan kumpulan tumpukan, lihat Bekerja dengan tumpukan di CloudFormation Panduan Pengguna, dan Langkah 2 - Tentukan cakupan untuk DevOps Guru. dan Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

Di atas kapal dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk mengaktifkan DevOps Guru untuk melihat wawasan agregat. Jalankan perintah berikut.

```
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
```

Tabel berikut menjelaskan perintah.

Perintah	Deskripsi

Perintah	Deskripsi
`create-service-linked-role`	Memberi DevOps Izin Guru untuk mengumpul kan informasi tentang organisasi Anda. Jangan lanjutkan jika langkah ini tidak berhasil.
`enable-aws-service-access`	Memasukkan organisasi Anda ke DevOps Guru.
`register-delegated-administrator`	Memberikan akses ke akun anggota untuk melihat wawasan.

Pantau akun Anda saat ini

Jika Anda memilih untuk memantau aplikasi saat ini AWS akun, pilih yang mana AWS sumber daya di akun dan Wilayah Anda dicakup atau dianalisis dan menentukan satu atau dua topik Layanan Pemberitahuan Sederhana Amazon yang digunakan untuk memberi tahu Anda saat wawasan dibuat. Anda dapat memperbarui pengaturan ini nanti sesuai kebutuhan.

Aktifkan DevOps Guru untuk memantau aplikasi di saat ini AWS akun

1. Buka Amazon DevOps Konsol Guru di https://console.aws.amazon.com/devops-guru/.
2. Memilih Memantau aplikasi saat ini AWS akun sebagai tipe setup.
3. Dalam DevOps Cakupan analisis Guru, pilih salah satu dari berikut ini.

   - Analisis semua AWS sumber daya saat ini AWS akun: DevOps Guru menganalisis semua AWS sumber daya di akun Anda.
   - Pilih sumber daya AWS untuk dianalisis nanti: Anda memilih batas analisis Anda nanti. Untuk informasi selengkapnya, lihat Tentukan cakupan untuk DevOps Guru dan Memperbarui cakupan AWS analisis Anda di DevOps Guru.

   DevOps Guru dapat menganalisis sumber daya apa pun yang terkait dengan AWS akun yang didukungnya. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat Amazon DevOps Harga Guru.

4. Anda dapat menambahkan hingga dua topik. DevOps Guru menggunakan topik atau topik untuk memberi tahu Anda tentang hal penting DevOps Peristiwa guru, seperti penciptaan wawasan baru. Jika Anda tidak menentukan topik sekarang, Anda dapat menambahkannya nanti dengan memilih Pengaturan di panel navigasi.

   a. Dalam Tentukan topik Amazon SNS, pilih topik yang akan digunakan.

   b. Untuk menambahkan topik Amazon SNS, lakukan salah satu hal berikut.

      - Pilih Buat topik SNS baru menggunakan email. Kemudian, dari Tentukan alamat email, masukkan alamat email yang ingin Anda terima pemberitahuan. Untuk memasukkan alamat email tambahan, pilih Tambahkan email baru.
      - Memilih Menggunakan topik SNS yang ada. Kemudian, dari Pilih topik di AWS akun, pilih topik yang ingin Anda gunakan.
      - Pilih Menggunakan topik SNS yang ada ARN untuk menentukan topik yang ada dari akun lain. Kemudian, di Masukkan ARN untuk topik, masukkan topik ARN. ARN adalah Nama Sumber Daya Amazon topik. Anda dapat menentukan topik di akun yang berbeda. Jika Anda menggunakan topik di akun lain, Anda harus menambahkan kebijakan sumber daya ke topik tersebut. Untuk informasi selengkapnya, lihat Izin untuk topik Amazon SNS.

5. Pilih Aktifkan.

Untuk mengkonfigurasi Amazon DevOps Guru untuk digunakan untuk pertama kalinya, Anda harus memilih yang mana AWS sumber daya di akun dan Wilayah Anda dicakup, atau dianalisis, dan tentukan satu atau dua topik Layanan Pemberitahuan Sederhana Amazon yang digunakan untuk memberi tahu Anda saat wawasan dibuat. Anda dapat memperbarui pengaturan ini nanti sesuai kebutuhan.

Langkah 3: Tentukan DevOps Cakupan sumber daya Guru

Jika Anda memilih untuk menentukan AWS sumber daya nanti saat Anda mengaktifkan DevOps Guru, Anda harus memilih CloudFormation menumpuk di Anda AWS akun yang membuat sumber daya yang ingin Anda analisis. Sebuah CloudFormation stack adalah kumpulan AWS sumber daya yang Anda kelola sebagai satu unit. Anda dapat menggunakan satu atau lebih tumpukan untuk menyertakan semua sumber daya yang diperlukan untuk menjalankan aplikasi operasional Anda, lalu tentukan mereka sehingga mereka dianalisis oleh DevOps Guru. Jika Anda tidak menentukan tumpukan, maka DevOps Guru menganalisis semua AWS sumber daya di akun Anda. Untuk informasi lebih lanjut, lihat Bekerja dengan tumpukan di CloudFormation Panduan Pengguna,

dan Tentukan cakupan untuk DevOps Guru. dan Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

> **Note**
>
> Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat Amazon DevOps Harga Guru.

Tentukan DevOps Cakupan sumber daya Guru

1. Buka Amazon DevOps Konsol Guru di https://console.aws.amazon.com/devops-guru/.
2. Memperluas Pengaturan di panel navigasi.
3. Dalam Sumber daya yang dianalisis, pilih Edit sumber daya yang dianalisis.
4. Pilih salah satu opsi cakupan berikut.

   - Memilih Semua sumber daya akun jika Anda ingin DevOps Guru untuk menganalisis semua sumber daya yang didukung di Anda AWS akun dan wilayah. Jika Anda memilih opsi ini, Anda AWS akun adalah batas cakupan analisis sumber daya Anda. Semua sumber daya di setiap tumpukan di akun Anda dikelompokkan ke dalam aplikasi mereka sendiri. Semua sumber daya yang tersisa yang tidak ada dalam tumpukan dikelompokkan ke dalam aplikasi mereka sendiri.
   - Memilih CloudFormation tumpukan jika Anda ingin DevOps Guru untuk menganalisis sumber daya yang ada di tumpukan yang Anda pilih, lalu pilih salah satu opsi berikut.
     - Semua sumber daya — Semua sumber daya yang ada di tumpukan di akun Anda dianalisis. Sumber daya di setiap tumpukan dikelompokkan ke dalam aplikasi mereka sendiri. Sumber daya apa pun di akun Anda yang tidak ada dalam tumpukan tidak dianalisis.
     - Pilih tumpukan — Pilih tumpukan yang Anda inginkan DevOps Guru untuk menganalisis. Sumber daya di setiap tumpukan yang Anda pilih dikelompokkan ke dalam aplikasi mereka sendiri. Anda dapat memasukkan nama tumpukan di Temukan tumpukan untuk menemukan tumpukan tertentu dengan cepat. Anda dapat memilih hingga 1.000 tumpukan.

     Untuk informasi selengkapnya, lihat Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.
   - Memilih Tag jika Anda ingin DevOps Guru untuk menganalisis semua sumber daya yang berisi tag yang Anda pilih. Pilih a kunci, lalu pilih salah satu opsi berikut.

- Semua sumber daya akun —Analisis semua sumber daya AWS di Wilayah dan akun saat ini. Sumber daya dengan kunci tag yang dipilih dikelompokkan berdasarkan nilai tag, jika ada. Sumber daya tanpa kunci tag ini dikelompokkan dan dianalisis secara terpisah.
- Pilih nilai tag tertentu — Semua sumber daya yang berisi tag dengan kunci yang Anda pilih dianalisis. DevOps Guru mengelompokkan sumber daya Anda ke dalam aplikasi berdasarkan tag Anda nilai-nilai.

Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

- Memilih Tidak ada jika Anda tidak mau DevOps Guru untuk menganalisis sumber daya apa pun. Opsi ini menonaktifkan DevOps Guru sehingga Anda berhenti menimbulkan biaya dari analisis sumber daya.

5. Pilih Simpan.

Mengaktifkan AWS layanan untuk analisis DevOps Guru

Amazon DevOps Guru dapat menganalisis kinerja AWS sumber daya apa pun yang didukungnya. Ketika menemukan perilaku anomali, itu menghasilkan wawasan dengan detail tentang perilaku dan bagaimana mengatasinya. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

DevOpsGuru menggunakan CloudWatch metrik Amazon, AWS CloudTrail peristiwa, dan lainnya untuk membantu menganalisis sumber daya. Sebagian besar sumber daya yang didukungnya menghasilkan metrik yang diperlukan untuk analisis DevOps Guru secara otomatis. Namun, beberapa AWS layanan memerlukan tindakan ekstra untuk menghasilkan metrik yang diperlukan. Untuk beberapa layanan, mengaktifkan metrik ini memberikan analisis tambahan untuk cakupan DevOps Guru yang ada. Bagi yang lain, analisis tidak dimungkinkan sampai Anda mengaktifkan metrik ini. Untuk informasi selengkapnya, silakan lihat Tentukan cakupan untuk DevOps Guru dan Memperbarui cakupan AWS analisis Anda di DevOps Guru.

Layanan yang membutuhkan tindakan untuk analisis DevOps Guru

- Amazon Elastic Container Service — Untuk menghasilkan metrik tambahan yang meningkatkan cakupan sumber daya DevOps Guru, ikuti langkah-langkah dalam Menyiapkan wawasan kontainer di Amazon ECS. Melakukan hal ini mungkin menimbulkan CloudWatch biaya Amazon.
- Amazon Elastic Kubernetes Service — Untuk menghasilkan metrik DevOps yang dapat dianalisis Guru, ikuti langkah-langkah dalam Menyiapkan wawasan kontainer di Amazon EKS dan Kubernetes. DevOpsGuru tidak menganalisis sumber daya Amazon EKS apa pun hingga pembuatan metrik ini disiapkan. Melakukan hal ini mungkin menimbulkan CloudWatch biaya Amazon.
- Amazon Simple Storage Service — Untuk menghasilkan metrik untuk dianalisis DevOps Guru, Anda harus mengaktifkan metrik permintaan. Ikuti langkah-langkah dalam Membuat konfigurasi CloudWatch metrik untuk semua objek di bucket Anda. DevOps Guru tidak menganalisis sumber daya Amazon S3 apa pun hingga pembuatan metrik ini disiapkan. Melakukan hal ini mungkin dikenakan biaya CloudWatch dan Amazon S3.

Untuk informasi selengkapnya, lihat CloudWatch harga Amazon.

Bekerja dengan wawasan di Guru DevOps

Amazon DevOps Guru menghasilkan wawasan saat mendeteksi perilaku anomali dalam aplikasi operasional Anda. DevOpsGuru menganalisis metrik, peristiwa, dan lainnya di AWS sumber daya yang Anda tentukan saat menyiapkan DevOps Guru. Setiap wawasan berisi satu atau lebih rekomendasi untuk Anda ambil untuk mengurangi masalah ini. Ini juga berisi daftar metrik, daftar grup log, dan daftar peristiwa yang digunakan untuk mengidentifikasi perilaku yang tidak biasa.

Ada dua jenis wawasan.

- Wawasan reaktif memiliki rekomendasi yang dapat Anda ambil untuk mengatasi masalah yang terjadi sekarang.
- Wawasan proaktif memiliki rekomendasi yang membahas masalah yang diprediksi DevOps Guru akan terjadi di masa depan.

Topik

- Melihat wawasan DevOps Guru
- Memahami wawasan di konsol DevOps Guru
- Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan
- Memahami keparahan wawasan

Melihat wawasan DevOps Guru

Anda dapat melihat wawasan Anda menggunakan. Konsol Manajemen AWS

Lihat wawasan DevOps Guru Anda

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Buka panel navigasi, lalu pilih Wawasan.
3. Pada tab Reaktif, Anda dapat melihat daftar wawasan reaktif. Pada tab Proaktif, Anda dapat melihat daftar wawasan proaktif.
4. (Opsional) Gunakan satu atau beberapa filter berikut untuk menemukan wawasan yang Anda cari.

    - Pilih tab Reaktif atau Proaktif, tergantung pada jenis wawasan yang Anda cari.

- Pilih Filter wawasan, lalu pilih opsi untuk menentukan filter. Anda dapat menambahkan kombinasi status, tingkat keparahan, sumber daya, dan filter tag. Gunakan filter AWS tag untuk melihat wawasan yang dihasilkan hanya oleh sumber daya dengan tag tertentu. Untuk mempelajari selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

> **Note**
>
> DevOpsGuru dapat menganalisis sumber daya berikut, tetapi tidak dapat memfilter wawasan mereka menggunakan tag.
>
> - Jalur dan rute Amazon API Gateway
> - Aliran Amazon DynamoDB
> - Instans grup Amazon EC2 Auto Scaling
> - AWS Elastic Beanstalk lingkungan
> - Node Pergeseran Merah Amazon

- Pilih atau tentukan rentang waktu untuk difilter berdasarkan waktu pembuatan wawasan.
  - 12h menunjukkan wawasan yang dibuat dalam 12 jam terakhir.
  - 1d menunjukkan wawasan yang dibuat di hari terakhir.
  - 1w menunjukkan wawasan yang dibuat dalam seminggu terakhir.
  - 1m menunjukkan wawasan yang dibuat dalam sebulan terakhir.
  - Kustom memungkinkan Anda menentukan rentang waktu lain. Rentang waktu maksimum yang dapat Anda gunakan untuk memfilter wawasan adalah 180 hari.

5. Untuk melihat detail tentang wawasan, pilih namanya.

Memahami wawasan di konsol DevOps Guru

Gunakan konsol Amazon DevOps Guru untuk melihat informasi berguna dalam wawasan Anda guna membantu Anda mendiagnosis dan mengatasi perilaku anomali. Saat DevOps Guru menganalisis sumber daya Anda dan menemukan CloudWatch metrik Amazon terkait, AWS CloudTrail peristiwa, dan data operasional yang menunjukkan perilaku yang tidak biasa, ia akan menciptakan wawasan yang berisi rekomendasi untuk mengatasi masalah dan informasi tentang metrik dan peristiwa terkait.

Gunakan data wawasan Praktik terbaik di DevOps Guru untuk mengatasi masalah operasional yang terdeteksi oleh DevOps Guru.

Untuk melihat wawasan, ikuti langkah-langkah Melihat wawasan untuk menemukannya, lalu pilih namanya. Halaman wawasan berisi detail berikut.

Gambaran umum wawasan

Gunakan bagian ini untuk mendapatkan gambaran umum tingkat tinggi tentang wawasan. Anda dapat melihat status wawasan (Sedang Berlangsung atau Ditutup), berapa banyak CloudFormation tumpukan yang terpengaruh, kapan wawasan dimulai, berakhir, dan terakhir diperbarui, dan item operasi terkait jika ada.

Jika wawasan dikelompokkan pada tingkat tumpukan, maka Anda dapat memilih jumlah tumpukan yang terpengaruh untuk melihat namanya. Perilaku anomali yang menciptakan wawasan terjadi pada sumber daya yang diciptakan oleh tumpukan yang terpengaruh. Jika wawasan dikelompokkan pada tingkat akun, maka jumlahnya nol atau tidak muncul.

Untuk informasi selengkapnya, lihat Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan.

Nama wawasan

Nama wawasan tergantung pada apakah itu dikelompokkan pada tingkat tumpukan atau tingkat akun.

- Nama wawasan tingkat tumpukan menyertakan nama tumpukan yang berisi sumber daya dengan perilaku anomali.
- Nama wawasan tingkat akun tidak menyertakan nama tumpukan.

Untuk informasi selengkapnya, lihat Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan.

Metrik agregat

Pilih tab Metrik teragregasi untuk melihat metrik yang terkait dengan wawasan. Dalam tabel, setiap baris mewakili satu metrik. Anda dapat melihat CloudFormation tumpukan mana yang menciptakan sumber daya yang memancarkan metrik, nama sumber daya, dan jenisnya. Tidak semua metrik dikaitkan dengan CloudFormation tumpukan atau memiliki nama.

Ketika ada beberapa sumber daya yang anomali pada saat yang sama, tampilan garis waktu mengumpulkan sumber daya dan menyajikan metrik anomali mereka dalam satu garis waktu

untuk analisis yang mudah. Garis merah pada garis waktu menunjukkan rentang waktu ketika metrik memancarkan nilai yang tidak biasa. Untuk memperbesar, gunakan mouse Anda untuk memilih rentang waktu tertentu. Anda juga dapat menggunakan ikon kaca pembesar untuk memperbesar dan memperkecil.

Pilih garis merah di timeline untuk melihat informasi terperinci. Di jendela yang terbuka, Anda dapat:

- Pilih Lihat di CloudWatch untuk melihat tampilan metrik di CloudWatch konsol. Untuk informasi selengkapnya, lihat Statistik dan Dimensi di Panduan CloudWatch Pengguna Amazon.
- Arahkan kursor ke grafik untuk melihat detail tentang data metrik anomali dan kapan itu terjadi.
- Pilih kotak dengan panah ke bawah untuk mengunduh gambar PNG dari grafik.

Anomali grafik

Pilih tab Graphed anomalies untuk melihat grafik terperinci untuk setiap anomali wawasan. Satu ubin muncul untuk setiap anomali dengan detail tentang perilaku tidak biasa yang terdeteksi dalam metrik terkait. Anda dapat menyelidiki dan melihat anomali di tingkat sumber daya dan per statistik. Grafik dikelompokkan berdasarkan nama metrik. Di setiap ubin, Anda dapat memilih rentang waktu tertentu di timeline untuk memperbesar. Anda juga dapat menggunakan ikon kaca pembesar untuk memperbesar dan memperkecil, atau memilih durasi yang telah ditentukan dalam jam, hari, atau minggu (1H, 3H, 12H, 1D, 3D, 1W, atau 2W).

Pilih Lihat semua statistik dan dimensi untuk melihat detail tentang anomali. Di jendela yang terbuka, Anda dapat:

- Pilih Lihat di CloudWatch untuk melihat tampilan metrik di CloudWatch konsol.
- Arahkan kursor ke grafik untuk melihat detail tentang data metrik anomali dan kapan itu terjadi.
- Pilih Statistik atau Dimensi untuk menyesuaikan tampilan grafik. Untuk informasi selengkapnya, lihat Statistik dan Dimensi di Panduan CloudWatch Pengguna Amazon.

Grup log

Saat Anda mengaktifkan deteksi anomali log, DevOps Guru memberi tag pada grup CloudWatch log Anda sehingga Anda dapat melihat grup log yang terkait dengan wawasan Anda. Di bagian Grup log di halaman detail wawasan, setiap baris dalam tabel mewakili satu grup log dan mencantumkan sumber daya terkait.

Ketika ada beberapa grup log anomali pada saat yang sama, tampilan garis waktu menggabungkannya dan menyajikannya dalam satu garis waktu untuk analisis yang mudah. Garis ungu pada garis waktu menunjukkan rentang waktu ketika grup log mengalami anomali log.

Pilih garis ungu di timeline untuk melihat contoh informasi anomali log seperti pengecualian kata kunci dan penyimpangan numerik. Pilih Lihat detail grup log untuk melihat anomali log. Di jendela yang terbuka, Anda dapat:

- Lihat grafik anomali log dan peristiwa yang relevan.
- Arahkan kursor ke grafik untuk melihat detail tentang data log anomali dan kapan itu terjadi.
- Lihat anomali log secara rinci dengan pesan sampel, frekuensi kejadian, rekomendasi terkait, dan waktu terjadinya.
- Klik Lihat detail CloudWatch untuk melihat baris log dari anomali log.

Peristiwa terkait

Dalam acara terkait, lihat AWS CloudTrail peristiwa yang terkait dengan wawasan Anda. Gunakan peristiwa ini untuk membantu memahami, mendiagnosis, dan mengatasi penyebab yang mendasari perilaku anomali.

Rekomendasi

Dalam Rekomendasi, Anda dapat melihat saran yang dapat membantu Anda menyelesaikan masalah mendasar. Ketika DevOps Guru mendeteksi perilaku anomali, ia mencoba untuk membuat rekomendasi. Wawasan mungkin berisi satu, beberapa, atau nol rekomendasi.

Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan

Wawasan dikelompokkan pada tingkat tumpukan atau tingkat akun. Jika wawasan dihasilkan untuk sumber daya yang ada di AWS CloudFormation tumpukan, maka itu adalah wawasan tingkat tumpukan. Jika tidak, ini adalah wawasan tingkat akun.

Bagaimana tumpukan dikelompokkan dapat bergantung pada cara Anda mengonfigurasi cakupan analisis sumber daya Anda di Amazon DevOps Guru.

Jika cakupan Anda ditentukan oleh CloudFormation tumpukan

Semua sumber daya yang terkandung dalam tumpukan yang Anda pilih dianalisis, dan semua wawasan yang terdeteksi dikelompokkan pada tingkat tumpukan.

Jika cakupan Anda adalah AWS akun dan Wilayah Anda saat ini

Semua sumber daya di akun dan Wilayah Anda dianalisis, dan ada tiga kemungkinan skenario pengelompokan untuk wawasan yang terdeteksi.

- Wawasan yang dihasilkan dari sumber daya yang bukan bagian dari tumpukan dikelompokkan di tingkat akun.
- Wawasan yang dihasilkan dari sumber daya yang ada di salah satu dari 10.000 tumpukan yang dianalisis pertama dikelompokkan pada tingkat tumpukan.
- Wawasan yang dihasilkan dari sumber daya yang tidak ada di salah satu dari 10.000 tumpukan yang dianalisis pertama dikelompokkan di tingkat akun. Misalnya, wawasan yang dihasilkan untuk sumber daya di tumpukan yang dianalisis ke 10.000 dikelompokkan pada tingkat akun.

Untuk informasi selengkapnya, lihat Tentukan cakupan untuk DevOps Guru.

Memahami keparahan wawasan

Wawasan dapat memiliki salah satu dari tiga tingkat keparahan, tinggi, sedang, atau rendah. Wawasan dibuat oleh Amazon DevOps Guru setelah mendeteksi anomali terkait dan menetapkan tingkat keparahan setiap anomali. DevOpsGuru memberikan anomali tingkat keparahan tinggi, sedang, atau rendah menggunakan pengetahuan domain dan pengalaman kolektif bertahun-tahun. Tingkat keparahan wawasan ditentukan oleh anomali paling parah yang berkontribusi untuk menciptakan wawasan.

- Jika tingkat keparahan semua anomali yang menghasilkan wawasan rendah, maka tingkat keparahan wawasannya rendah.
- Jika tingkat keparahan tertinggi dari semua anomali yang menghasilkan wawasan adalah sedang, maka tingkat keparahan wawasan adalah sedang. Tingkat keparahan beberapa anomali yang menghasilkan wawasan mungkin rendah.
- Jika tingkat keparahan tertinggi dari semua anomali yang menghasilkan wawasan tinggi, maka tingkat keparahan wawasannya tinggi. Tingkat keparahan beberapa anomali yang menghasilkan wawasan mungkin rendah atau sedang.

Memantau database menggunakan Guru DevOps

DevOpsGuru memberikan nilai yang signifikan untuk mengoperasikan database pada AWS. Dengan memanfaatkan algoritma pembelajaran mesinnya, DevOps Guru dapat membantu mengoptimalkan kinerja database, meningkatkan keandalan, dan mengurangi overhead operasional. Bagian panduan pengguna ini memberikan gambaran tingkat tinggi dari kemampuan database ini, termasuk kasus penggunaan DevOps Guru khusus untuk layanan AWS database yang berbeda.

DevOpsGuru dapat memberikan wawasan untuk database relasional seperti Amazon RDS dan. Amazon Redshift Ini juga dapat memberikan wawasan untuk database non-relasional atau NoSQL seperti dan. Amazon DynamoDB Amazon ElastiCache

Topik

- Memantau database relasional menggunakan Guru DevOps
- Memantau database non-relasional menggunakan Guru DevOps

Memantau database relasional menggunakan Guru DevOps

DevOpsGuru menarik dari dua sumber data utama untuk mencari wawasan dan anomali dalam database relasional. Untuk Amazon RDS dan Amazon Redshift, metrik CloudWatch vended dianalisis untuk semua jenis instans. Untuk Amazon RDS, data Performance Insights juga dicerna untuk jenis engine berikut: RDS untuk PostgreSQL, Aurora PostgreSQL, dan Aurora MySQL.

Memantau operasi basis data di Amazon RDS

Bagian ini mencakup informasi spesifik tentang kasus penggunaan dan metrik yang dipantau di DevOps Guru for RDS, termasuk data dari metrik CloudWatch terjual dan Performance Insights. Untuk informasi selengkapnya tentang DevOps Guru untuk RDS, termasuk konsep kunci, konfigurasi, dan manfaat, lihat. the section called “Bekerja dengan anomali di DevOps Guru untuk RDS”

Memantau RDS menggunakan data dari metrik yang CloudWatch dijual

DevOpsGuru mampu memantau setiap jenis instans RDS dengan menelan CloudWatch metrik default, seperti pemanfaatan CPU dan latensi operasi baca dan tulis. Karena metrik ini dijual secara default, saat Anda memantau instans RDS Anda dengan DevOps Guru, tidak diperlukan konfigurasi lebih lanjut untuk mendapatkan wawasan. DevOpsGuru secara otomatis menetapkan dasar untuk

metrik ini berdasarkan pola historis dan membandingkannya dengan data real-time untuk mendeteksi anomali dan potensi masalah dalam database Anda.

Tabel berikut menunjukkan daftar wawasan reaktif potensial untuk Amazon RDS dari CloudWatch metrik yang dijual.

AWS sumber daya yang dipantau oleh Guru DevOps	Skenario yang diidentifikasi DevOps Guru	CloudWatch metrik dipantau
Amazon RDS (semua jenis instans)	CPU atau memori mencapai batas	DBLoad, DBLoad CPU
RDS for PostgreSQL	Jeda slot replikasi tinggi	OldestReplicationSlotLag

Metrik CloudWatch vended tambahan dari instans Amazon RDS yang dipantau Guru: DevOps

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

Memantau RDS menggunakan data dari Performance Insights

Untuk jenis instans Amazon RDS tertentu, seperti Aurora PostgreSQL, Aurora MySQL, dan RDS untuk PostgreSQL, Anda membuka lebih banyak kemampuan dari pemantauan Guru dengan memastikan bahwa Performance Insights diaktifkan pada instans tersebut. DevOps

DevOpsGuru memberikan wawasan reaktif untuk berbagai situasi, termasuk skenario berikut:

Skenario yang diidentifikasi DevOps Guru untuk menghasilkan wawasan reaktif
Mengunci masalah pertikaian

Skenario yang diidentifikasi DevOps Guru untuk menghasilkan wawasan reaktif
Indeks hilang
Kesalahan konfigurasi kumpulan aplikasi
Default JDBC yang kurang optimal

DevOpsGuru memberikan wawasan proaktif untuk berbagai situasi, termasuk skenario berikut:

AWS sumber daya yang dipantau oleh Guru DevOps	Skenario yang diidentifikasi DevOps Guru untuk menghasilkan wawasan proaktif
Aurora MySQL	Daftar riwayat InnoDB tumbuh terlalu besar, yang dapat menyebabkan penurunan kinerja seperti waktu shutdown database yang lama
Aurora MySQL	Peningkatan tabel sementara yang dibuat pada disk yang dapat memengaruhi kinerja database
RDS untuk PostgreSQL, Aurora PostgreSQL	Koneksi yang telah menganggur dalam transaksi terlalu lama, dampak potensial dari menahan kunci, memblokir kueri lain, dan mencegah vakum (termasuk autovacuum) membersihkan baris mati

Memantau operasi database di Amazon Redshift

DevOpsGuru mampu memantau sumber Amazon Redshift daya Anda dengan menelan CloudWatch metrik default, termasuk pemanfaatan CPU dan persentase ruang disk yang digunakan. Karena metrik ini dijual secara default, tidak ada konfigurasi lebih lanjut yang diperlukan agar DevOps Guru memantau sumber daya Anda Amazon Redshift secara otomatis. DevOpsGuru menetapkan dasar untuk metrik ini berdasarkan pola historis dan membandingkannya dengan data real-time untuk mendeteksi anomali.

Skenario yang diidentifikasi DevOps Guru	CloudWatch metrik dipantau
Mendeteksi pemanfaatan CPU yang tinggi dari sebuah Amazon Redshift instance yang disebabkan oleh faktor-faktor seperti beban kerja cluster, data miring dan tidak disortir, atau tugas node pemimpin	CPUUtilization
Mendeteksi ketika sebuah Amazon Redshift instance kehabisan ruang disk karena masalah dengan pemrosesan kueri, distribusi dan kunci pengurutan, operasi pemeliharaan, atau blok batu nisan	PercentageDiskSpaceUsed

Metrik CloudWatch vended tambahan dari Amazon Redshift instance yang DevOps dipantau Guru:

- DatabaseConnections
- HealthStatus
- MaintenanceMode
- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- ReadIOPS
- ReadLatency
- WLMQueuePanjangnya
- WLMQueueWaitTime
- WLMQueryDurasi
- WriteLatency

Bekerja dengan anomali di DevOps Guru untuk RDS

DevOpsGuru mendeteksi, menganalisis, dan memberikan rekomendasi untuk AWS sumber daya yang didukung, termasuk mesin Amazon RDS. Untuk instans database Amazon Aurora dan RDS for

PostgreSQL dengan Performance Insights diaktifkan, DevOps Guru for RDS menyediakan analisis terperinci dan spesifik database tentang masalah kinerja dan merekomendasikan tindakan korektif.

Topik

- Ikhtisar DevOps Guru untuk RDS
- Mengaktifkan DevOps Guru untuk RDS
- Menganalisis anomali di Amazon RDS

Ikhtisar DevOps Guru untuk RDS

Berikut ini, Anda dapat menemukan ringkasan manfaat dan fitur utama DevOps Guru untuk RDS. Untuk latar belakang wawasan dan anomali, lihatDevOpsKonsep guru.

Topik

- Manfaat DevOps Guru untuk RDS
- Konsep kunci untuk penyetelan kinerja database
- Konsep kunci untuk DevOps Guru untuk RDS
- Bagaimana DevOps Guru untuk RDS bekerja
- Mesin database yang didukung

Manfaat DevOps Guru untuk RDS

Jika Anda bertanggung jawab atas database Amazon RDS, Anda mungkin tidak tahu bahwa peristiwa atau regresi yang memengaruhi database tersebut sedang terjadi. Ketika mengetahui masalah ini, Anda mungkin tidak tahu alasannya terjadi atau apa yang harus dilakukan terhadapnya. Daripada beralih ke administrator database (DBA) untuk bantuan atau mengandalkan alat pihak ketiga, Anda dapat mengikuti rekomendasi dari DevOps Guru untuk RDS.

Anda mendapatkan keuntungan berikut dari analisis rinci DevOps Guru untuk RDS:

Diagnosis cepat

DevOpsGuru untuk RDS terus memantau dan menganalisis telemetri database. Performance Insights, Enhanced Monitoring, dan Amazon CloudWatch mengumpulkan data telemetri untuk instans database Anda. DevOpsGuru untuk RDS menggunakan teknik statistik dan pembelajaran mesin untuk menambang data ini dan mendeteksi anomali. Untuk mempelajari lebih lanjut tentang data telemetri untuk database Amazon Aurora, lihat Meman tau beban DB dengan Performance

Insights di Amazon Aurora dan Meman tau OS dengan menggunakan Pemantauan yang Dit ingkatkan di Panduan Pengguna Amazon Aurora. Untuk mempelajari lebih lanjut tentang data telemetri untuk database Amazon RDS lainnya, lihat Memantau beban DB dengan W awasan Kinerja pada Layanan Database Relasional Amazon dan Memantau metrik OS dengan Pemantauan yang Ditingkatkan di Panduan Pengguna Amazon RDS.

Resolusi cepat

Setiap anomali mengidentifikasi masalah performa dan menyarankan alur investigasi atau tindakan korektif. Misalnya, DevOps Guru untuk RDS mungkin merekomendasikan agar Anda menyelidiki peristiwa tunggu tertentu. Atau mungkin menyarankan agar Anda menyetel pengaturan kumpulan aplikasi Anda untuk membatasi jumlah koneksi basis data. Berdasarkan rekomendasi ini, Anda dapat menyelesaikan masalah performa lebih cepat daripada dengan memecahkan masalah secara manual.

Wawasan proaktif

DevOpsGuru untuk RDS menggunakan metrik dari sumber daya Anda untuk mendeteksi perilaku yang berpotensi bermasalah sebelum menjadi masalah yang lebih besar. Misalnya, dapat mendeteksi ketika sesi yang terhubung ke database tidak melakukan pekerjaan aktif dan mungkin menjaga sumber daya database diblokir. DevOps Guru kemudian memberikan rekomendasi untuk membantu Anda mengatasi masalah sebelum menjadi masalah yang lebih besar.

Pengetahuan mendalam insinyur Amazon dan machine learning

Untuk mendeteksi masalah kinerja dan membantu Anda mengatasi hambatan, DevOps Guru untuk RDS mengandalkan pembelajaran mesin (ML) dan analisis statistik lanjutan. Insinyur database Amazon berkontribusi pada pengembangan temuan DevOps Guru for RDS, yang merangkum bertahun-tahun mengelola ratusan ribu database. Dengan memanfaatkan pengetahuan kolektif ini, DevOps Guru untuk RDS dapat mengajarkan Anda praktik terbaik.

Konsep kunci untuk penyetelan kinerja database

DevOpsGuru untuk RDS mengasumsikan bahwa Anda akrab dengan beberapa konsep kinerja utama. Untuk mempelajari lebih lanjut tentang konsep-konsep ini, lihat Ringkasan Wawasan Kinerja di Panduan Pengguna Amazon Aurora atau I khtisar Wawasan Kinerja di Panduan Pengguna Amazon RDS.

Topik

- Metrik-metrik

- Deteksi masalah
- Muatan DB
- Peristiwa tunggu

Metrik-metrik

Sebuah metrik merupakan serangkaian titik data yang diurutkan berdasarkan waktu. Pikirkan metrik sebagai variabel untuk memantau, dan titik data sebagai representasi nilai-nilai variabel tersebut dari waktu ke waktu. Amazon RDS menyediakan metrik secara real time untuk database dan untuk sistem operasi (OS) tempat instans DB Anda berjalan. Anda dapat melihat semua metrik sistem dan informasi proses untuk instans Amazon RDS DB Anda di konsol Amazon RDS. DevOps Guru untuk RDS memantau dan memberikan wawasan untuk beberapa metrik ini. Untuk informasi selengkapnya, lihat Metrik pemantauan di cluster Amazon Aurora atau Metrik pemantauan di instans Layanan Database Relasional Amazon.

Deteksi masalah

DevOpsGuru untuk RDS menggunakan metrik database dan sistem operasi (OS) untuk mendeteksi masalah kinerja database yang kritis, apakah masalah tersebut akan datang atau sedang berlangsung. Ada 2 cara utama DevOps Guru untuk deteksi masalah RDS bekerja:

- Menggunakan ambang batas
- Menggunakan anomali

Mendeteksi masalah dengan ambang batas

Ambang batas adalah nilai pembatas yang digunakan untuk mengevaluasi metrik yang dipantau. Anda dapat menganggap ambang batas sebagai garis horizontal pada bagan metrik yang memisahkan perilaku normal dari perilaku yang berpotensi bermasalah. DevOps Guru untuk RDS memantau metrik tertentu dan membuat ambang batas dengan menganalisis level apa yang dianggap berpotensi bermasalah untuk sumber daya tertentu. DevOpsGuru untuk RDS kemudian menciptakan wawasan di konsol DevOps Guru ketika nilai metrik baru melewati ambang batas tertentu selama periode waktu tertentu secara konsisten. Wawasan berisi rekomendasi untuk mencegah dampak kinerja database di masa mendatang.

Misalnya, DevOps Guru untuk RDS mungkin memantau jumlah tabel sementara menggunakan disk selama periode 15 menit dan membuat wawasan ketika tingkat tabel sementara menggunakan

disk per detik sangat tinggi. Peningkatan tingkat penggunaan tabel sementara pada disk dapat memengaruhi kinerja database. Dengan mengekspos situasi ini sebelum menjadi kritis, DevOps Guru untuk RDS membantu Anda mengambil tindakan korektif untuk mencegah masalah.

Mendeteksi masalah dengan anomali

Sementara ambang batas menyediakan cara sederhana dan efektif untuk mendeteksi masalah database, dalam beberapa situasi mereka tidak cukup. Pertimbangkan kasus di mana nilai metrik melonjak dan menyilang ke perilaku yang berpotensi bermasalah secara teratur karena proses yang diketahui, seperti pekerjaan pelaporan harian. Karena lonjakan seperti itu diharapkan, membuat wawasan dan pemberitahuan untuk masing-masing akan menjadi kontraproduktif dan kemungkinan akan menyebabkan kelelahan waspada.

Namun, masih perlu untuk mendeteksi lonjakan yang sangat tidak biasa, karena metrik yang jauh lebih tinggi daripada yang lain atau bertahan lebih lama dapat mewakili masalah kinerja database yang nyata. Untuk mengatasi masalah ini, DevOps Guru untuk RDS memantau metrik tertentu untuk mendeteksi kapan perilaku metrik menjadi sangat tidak biasa atau anomali. DevOpsGuru kemudian melaporkan anomali ini dalam wawasan.

Misalnya, DevOps Guru untuk RDS mungkin membuat wawasan ketika beban DB tidak hanya tinggi, tetapi juga secara signifikan menyimpang dari perilaku biasanya, yang menunjukkan perlambatan besar yang tidak terduga dari operasi database. Dengan hanya mengenali lonjakan beban DB yang tidak normal, DevOps Guru untuk RDS memungkinkan Anda fokus pada masalah yang benar-benar penting.

Muatan DB

Konsep kunci untuk penyetelan database adalah metrik beban database (beban DB). Beban DB menunjukkan seberapa sibuk database Anda pada waktu tertentu. Peningkatan beban DB berarti peningkatan aktivitas database.

Sesi basis data mewakili dialog aplikasi dengan basis data relasional. Sesi aktif adalah sesi yang sedang dalam proses menjalankan permintaan database. Sesi dianggap aktif jika berjalan di CPU atau menunggu sumber daya tersedia sehingga dapat dilanjutkan. Misalnya, sesi aktif mungkin menunggu halaman dibaca ke dalam memori, dan kemudian menggunakan CPU saat membaca data dari halaman.

`DBLoad`Metrik di Performance Insights diukur dalam sesi aktif rata-rata (AAS). Untuk menghitung AAS, Performance Insights mengambil sampel jumlah sesi aktif setiap detik. Untuk periode waktu

tertentu, AAS adalah jumlah total sesi aktif dibagi dengan jumlah total sampel. Nilai AAS 2 berarti bahwa, rata-rata, 2 sesi aktif dalam permintaan pada waktu tertentu.

Analogi untuk beban DB adalah aktivitas di gudang. Misalkan gudang mempekerjakan 100 pekerja. Jika 1 pesanan masuk, 1 pekerja memenuhi pesanan sementara pekerja lainnya menganggur. Jika 100 pesanan atau lebih masuk, semua 100 pekerja memenuhi pesanan secara bersamaan. Jika Anda secara berkala mengambil sampel berapa banyak pekerja yang aktif selama periode waktu tertentu, Anda dapat menghitung jumlah rata-rata pekerja aktif. Perhitungan menunjukkan bahwa, rata-rata, pekerja N sibuk memenuhi pesanan pada waktu tertentu. Jika rata-rata 50 pekerja kemarin dan 75 pekerja hari ini, tingkat aktivitas di gudang meningkat. Dengan cara yang sama, beban DB meningkat saat aktivitas sesi meningkat.

Untuk mempelajari selengkapnya, lihat Pemuatan database di Panduan Pengguna Amazon Aurora atau Pemuatan Database di Panduan Pengguna Amazon RDS.

Peristiwa tunggu

A cara tunggu adalah jenis instrumentasi database yang memberi tahu Anda sumber daya mana yang sedang ditunggu sesi database sehingga dapat dilanjutkan. Ketika Performance Insights menghitung sesi aktif untuk menghitung beban database, ini juga mencatat peristiwa tunggu yang menyebabkan sesi aktif menunggu. Teknik ini memungkinkan Performance Insights untuk menunjukkan kepada Anda peristiwa tunggu mana yang berkontribusi terhadap beban DB.

Setiap sesi aktif berjalan di CPU atau menunggu. Misalnya, sesi menggunakan CPU ketika mereka mencari memori, melakukan perhitungan, atau menjalankan kode prosedural. Ketika sesi tidak menggunakan CPU, mereka mungkin menunggu file data untuk dibaca atau log untuk ditulis. Semakin banyak waktu untuk sesi menunggu sumber daya, semakin sedikit waktu untuk sesi dijalankan di CPU.

Saat Anda menyetel database, Anda sering mencoba menemukan sumber daya yang ditunggu sesi. Misalnya, dua atau tiga peristiwa tunggu mungkin menyumbang 90% dari beban DB. Ukuran ini berarti bahwa, rata-rata, sesi aktif menghabiskan sebagian besar waktunya menunggu sejumlah kecil sumber daya. Jika Anda dapat mengetahui penyebab penantian ini, Anda dapat mencoba memperbaiki masalahnya.

Pertimbangkan analogi pekerja gudang. Pesanan masuk. Pekerja mungkin terlambat memenuhi pesanan. Misalnya, pekerja lain mungkin sedang mengisi ulang rak, atau troli mungkin tidak tersedia. Atau sistem yang digunakan untuk memasukkan status pesanan lambat. Semakin lama pekerja menunggu, semakin lama pesanan yang dibutuhkan untuk dipenuhi. Menunggu adalah bagian alami

dari alur kerja gudang, tetapi jika waktu tunggu menjadi berlebihan, produktivitas menurun. Sama halnya, menunggu sesi berulang atau panjang dapat menurunkan performa basis data.

Untuk informasi selengkapnya tentang acara tunggu di Amazon Aurora, lihat Men yetel dengan acara tunggu untuk Aurora PostgreSQL dan Men yetel dengan acara tunggu untuk Aurora MySQL di Panduan Pengguna Amazon Aurora.

Untuk informasi selengkapnya tentang peristiwa tunggu di database Amazon RDS lainnya, lihat Menyet el dengan peristiwa tunggu untuk RDS untuk PostgreSQL di Panduan Pengguna Amazon RDS.

Konsep kunci untuk DevOps Guru untuk RDS

W awasan dihasilkan oleh DevOps Guru ketika mendeteksi perilaku anomali atau bermasalah dalam aplikasi operasional Anda. Wawasan berisi anomali untuk satu atau lebih sumber daya. Anomali mewakili satu atau lebih metrik terkait yang terdeteksi oleh DevOps Guru yang tidak terduga atau tidak biasa.

Wawasan memiliki tingkat keparahan tinggi, sedang, atau rendah. Tingkat keparahan wawasan ditentukan oleh anomali paling parah yang berkontribusi untuk menciptakan wawasan. Misalnya, jika wawasan AWS-ECS _ MemoryUtilization _dan_others mencakup satu anomali dengan tingkat keparahan rendah dan yang lain dengan tingkat keparahan tinggi, tingkat keparahan wawasan secara keseluruhan tinggi.

Jika instans Amazon RDS DB mengaktifkan Performance Insights, DevOps Guru for RDS memberikan analisis dan rekomendasi terperinci dalam anomali untuk instans ini. Untuk mengidentifikasi anomali, DevOps Guru untuk RDS mengembangkan baseline untuk nilai metrik database. DevOpsGuru untuk RDS kemudian membandingkan nilai metrik saat ini dengan baseline historis.

Topik

- Wawasan proaktif
- Wawasan reaktif
- Rekomendasi

Wawasan proaktif

Wawasan proaktif memberi tahu Anda tentang perilaku bermasalah sebelum menimbulkan masalah. Ini berisi anomali dengan rekomendasi dan metrik terkait untuk membantu Anda mengatasi masalah sebelum menjadi masalah yang lebih besar.

Setiap halaman wawasan proaktif memberikan rincian tentang satu anomali.

Wawasan reaktif

Wawasan reaktif mengidentifikasi perilaku anomali saat terjadi. Ini berisi anomali dengan rekomendasi, metrik terkait, dan peristiwa untuk membantu Anda memahami dan mengatasi masalah sekarang.

Anomali kausal

Anomali kausal adalah anomali tingkat puncak dalam wawasan reaktif. Ini ditampilkan sebagai metrik Utama pada halaman detail anomali di konsol DevOps Guru. Beban database (beban DB) adalah anomali kausal untuk DevOps Guru untuk RDS. Misalnya, wawasan AWS-ECS _ MemoryUtilization _dan_others dapat memiliki beberapa anomali metrik, salah satunya adalah beban database (beban DB) untuk sumber daya. AWS/RDS

Dalam wawasan, beban Database anomali (beban DB) dapat terjadi untuk beberapa instans Amazon RDS DB. Tingkat keparahan anomali mungkin berbeda untuk setiap instance DB. Misalnya, tingkat keparahan untuk satu instans DB mungkin tinggi sementara tingkat keparahan untuk yang lain rendah. Konsol default ke anomali dengan tingkat keparahan tertinggi.

Anomali kontekstual

Anomali kontekstual adalah temuan dalam Beban basis data (Beban DB) yang terkait dengan wawasan reaktif. Ini ditampilkan di bagian Metrik Ter kait dari halaman detail anomali di konsol DevOps Guru. Setiap anomali kontekstual menggambarkan masalah kinerja Amazon RDS tertentu yang memerlukan penyelidikan. Misalnya, anomali kausal dapat mencakup anomali kontekstual berikut:

- Kapasitas CPU ter lampaui — Antrian berjalan CPU atau pemanfaatan CPU di atas normal.
- Memori database rendah — Proses tidak memiliki cukup memori.
- Koneksi database mel onjak — Jumlah koneksi database di atas normal.

Rekomendasi

Setiap wawasan memiliki setidaknya satu tindakan yang disarankan. Contoh berikut adalah rekomendasi yang dihasilkan oleh DevOps Guru untuk RDS:

- Setel ID SQL *list_of_IDs* untuk mengurangi penggunaan CPU, atau tingkatkan jenis instance untuk meningkatkan kapasitas CPU.
- Tinjau lonjakan terkait koneksi database saat ini. Pertimbangkan untuk menyetel pengaturan kumpulan aplikasi untuk menghindari alokasi dinamis yang sering dari koneksi database baru.
- Cari pernyataan SQL yang melakukan operasi memori berlebihan, seperti penyortiran dalam memori atau gabungan besar.
- Selidiki I/O penggunaan berat untuk ID SQL berikut:*list_of_IDs*.
- Periksa pernyataan yang membuat sejumlah besar data sementara, misalnya yang melakukan pengurutan besar atau menggunakan tabel sementara besar.
- Periksa aplikasi untuk melihat apa yang menyebabkan peningkatan beban kerja database.
- Pertimbangkan untuk mengaktifkan Skema Kinerja MySQL.
- Periksa transaksi yang berjalan lama dan akhiri dengan komit atau rollback.
- Konfigurasikan parameter idle_in_transaction_session_timeout untuk mengakhiri sesi apa pun yang telah berada dalam status 'idle dalam transaksi' lebih lama dari waktu yang ditentukan.

Bagaimana DevOps Guru untuk RDS bekerja

DevOpsGuru untuk RDS mengumpulkan data metrik, menganalisisnya, dan kemudian menerbitkan anomali di dasbor.

Topik

- Pengumpulan dan analisis data
- Publikasi anomali

Pengumpulan dan analisis data

DevOpsGuru untuk RDS mengumpulkan data tentang database Amazon RDS Anda dari Amazon RDS Performance Insights. Fitur ini memantau instans Amazon RDS DB, mengumpulkan metrik, dan memungkinkan Anda untuk menjelajahi metrik dalam bagan. Metrik kinerja yang paling penting adalah`DBLoad`. DevOpsGuru untuk RDS menggunakan metrik Performance Insights dan menganalisisnya untuk mendeteksi anomali. Untuk informasi selengkapnya tentang Performance

Insights, lihat Meman tau beban DB dengan Performance Insights di Amazon Aurora di Panduan Pengguna Amazon Aurora atau Meman tau beban DB dengan Performance Insights di Amazon RDS di Panduan Pengguna Amazon RDS.

DevOpsGuru untuk RDS menggunakan pembelajaran mesin dan analisis statistik lanjutan untuk menganalisis data yang dikumpulkan dari Performance Insights. Jika DevOps Guru untuk RDS menemukan masalah kinerja, ia melanjutkan ke langkah berikutnya.

Publikasi anomali

Masalah kinerja database seperti beban DB yang tinggi dapat menurunkan kualitas layanan untuk database Anda. Ketika DevOps Guru mendeteksi masalah dalam database RDS, ia menerbitkan wawasan di dasbor. Wawasan berisi anomali untuk sumber daya AWS/RDS.

Jika Performance Insights diaktifkan untuk instans Anda, anomali tersebut berisi analisis rinci masalah. DevOps Guru untuk RDS juga merekomendasikan agar Anda melakukan penyelidikan atau tindakan korektif tertentu. Misalnya, rekomendasinya mungkin untuk menyelidiki pernyataan SQL beban tinggi tertentu, mempertimbangkan untuk meningkatkan kapasitas CPU, atau untuk menutup sesi idle-in-transaksi.

Mesin database yang didukung

DevOpsGuru untuk RDS didukung untuk mesin database berikut:

Amazon Aurora dengan kompatibilitas MySQL

- Untuk mempelajari selengkapnya tentang mesin ini, lihat Bek erja dengan Amazon Aurora MySQL di Panduan Pengguna Amazon Aurora.

Amazon Aurora dengan kompatibilitas PostgreSQL

- Untuk mempelajari selengkapnya tentang mesin ini, lihat Bekerja dengan Amazon Aurora PostgreSQL di Panduan Pengguna Amazon Aurora.

Amazon RDS untuk kompatibilitas PostgreSQL

- Untuk mempelajari lebih lanjut tentang mesin ini, lihat Amazon RDS for PostgreSQL di Panduan Pengguna Amazon RDS.

DevOpsGuru melaporkan anomali dan memberikan analisis dasar untuk mesin database lainnya. DevOpsGuru untuk RDS memberikan analisis terperinci dan rekomendasi hanya untuk instans Amazon Aurora dan RDS untuk PostgreSQL.

Mengaktifkan DevOps Guru untuk RDS

Ketika Anda mengaktifkan DevOps Guru untuk RDS, Anda mengaktifkan DevOps Guru untuk menganalisis anomali dalam sumber daya seperti instans DB. Amazon RDS memudahkan untuk menemukan dan mengaktifkan fungsionalitas yang direkomendasikan untuk instans DB RDS atau cluster DB. Untuk mencapai hal ini, RDS membuat panggilan API ke layanan lain, seperti Amazon EC2, DevOps Guru, dan IAM. Saat konsol RDS melakukan panggilan API ini, catat mereka AWS CloudTrail untuk visibilitas.

Untuk mengi DevOps zinkan Guru mempublikasikan wawasan untuk database Amazon RDS, selesaikan tugas di bagian berikut.

Topik

- Mengaktifkan Performance Insights untuk instans Amazon RDS DB
- Mengkonfigurasi kebijakan akses untuk DevOps Guru untuk RDS
- Menambahkan instans Amazon RDS DB ke cakupan DevOps Guru

Mengaktifkan Performance Insights untuk instans Amazon RDS DB

Agar DevOps Guru for RDS dapat menganalisis anomali pada instans DB, pastikan bahwa Performance Insights diaktifkan. Jika Performance Insights tidak diaktifkan untuk instans DB, DevOps Guru for RDS akan memberi tahu Anda di tempat-tempat berikut:

Dasbor

Jika Anda melihat wawasan berdasarkan jenis sumber daya, ubin RDS memberi tahu Anda bahwa Performance Insights tidak diaktifkan. Pilih tautan untuk mengaktifkan Performance Insights di konsol Amazon RDS.

Wawasan

Di bagian Rekomendasi di bagian bawah halaman, pilih Aktifkan Amazon RDS Performance Insights.

Pengaturan

Di bagian Layanan: Amazon RDS, pilih tautan untuk mengaktifkan Performance Insights di konsol Amazon RDS.

Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan Performance Insights di Panduan Pengguna Amazon Aurora, atau Mengaktifkan dan menonaktifkan Performance Insights di Panduan Pengguna Amazon RDS.

Mengkonfigurasi kebijakan akses untuk DevOps Guru untuk RDS

Agar pengguna dapat mengakses DevOps Guru untuk RDS, mereka harus memiliki izin dari salah satu kebijakan berikut:

- Kebijakan yang AWS dikelola `AmazonRDSFullAccess`
- Kebijakan yang dikelola pelanggan yang memungkinkan tindakan berikut:
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

Untuk informasi selengkapnya, lihat Mengonfigurasi kebijakan akses untuk W awasan Kinerja di Panduan Pengguna Amazon Aurora atau Meng onfigurasi kebijakan akses untuk Wawasan Kinerja di Panduan Pengguna Amazon RDS.

Menambahkan instans Amazon RDS DB ke cakupan DevOps Guru

Anda dapat mengonfigurasi DevOps Guru untuk memantau database Amazon RDS Anda baik di konsol DevOps Guru atau konsol Amazon RDS.

Di konsol DevOps Guru, Anda memiliki opsi berikut:

- Aktif DevOps kan Guru di tingkat akun. Ini adalah opsi default. Ketika Anda memilih opsi ini, DevOps Guru menganalisis semua AWS sumber daya yang didukung di Wilayah AWS dan Akun AWS, termasuk database Amazon RDS.
- Tentukan AWS CloudFormation tumpukan untuk DevOps Guru untuk RDS.

  Untuk informasi selengkapnya, lihat Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.
- Tandai sumber daya Amazon RDS Anda.

  Tag adalah label atribut khusus yang Anda tetapkan ke AWS sumber daya. Gunakan tag untuk mengidentifikasi AWS sumber daya yang membentuk aplikasi Anda. Anda kemudian dapat memfilter wawasan berdasarkan tag untuk hanya melihat yang dibuat oleh aplikasi Anda. Untuk

hanya melihat wawasan yang dihasilkan oleh sumber daya Amazon RDS di aplikasi Anda, tambahkan nilai seperti `Devops-guru-rds` tag sumber daya Amazon RDS Anda. Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

> **Note**
>
> Saat menandai sumber daya Amazon RDS, Anda harus menandai instance database dan bukan cluster.

Untuk mengaktifkan pemantauan DevOps Guru dari konsol Amazon RDS, lihat Mengaktifkan DevOps Guru di konsol RDS. Perhatikan bahwa untuk mengaktifkan DevOps Guru dari konsol Amazon RDS Anda harus menggunakan tag. Untuk informasi selengkapnya tentang tag, lihat the section called “Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi Anda”.

Menganalisis anomali di Amazon RDS

Ketika DevOps Guru untuk RDS menerbitkan anomali kinerja di dasbor, Anda biasanya melakukan langkah-langkah berikut:

1. Lihat wawasan di dasbor DevOps Guru. DevOpsGuru untuk RDS melaporkan wawasan reaktif dan proaktif.

   Untuk informasi selengkapnya, lihat Melihat wawasan.

2. Lihat anomali untuk AWS/RDS sumber daya.

   Untuk informasi selengkapnya, lihat Melihat anomali reaktif dan Melihat anomali proaktif.

3. Tanggapi DevOps Guru untuk rekomendasi RDS.

   Untuk informasi selengkapnya, lihat Menanggapi rekomendasi.

4. Pantau kesehatan instans DB Anda untuk memastikan bahwa masalah kinerja yang diselesaikan tidak berulang.

   Untuk informasi selengkapnya, lihat Metrik pemantauan di cluster Amazon Aurora DB di Panduan Pengguna Amazon Aurora dan Metrik Pem antauan dalam instans Amazon RDS di Panduan Pengguna Amazon RDS.

Melihat wawasan

Akses halaman Wawasan di konsol DevOps Guru untuk menemukan wawasan reaktif dan proaktif. Dari sana, Anda dapat memilih wawasan dari daftar untuk melihat halaman rinci metrik, rekomendasi, dan informasi lebih lanjut tentang wawasan.

Untuk melihat wawasan

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Buka panel navigasi, lalu pilih Wawasan.
3. Pilih tab Reaktif untuk melihat wawasan reaktif, atau pilih Proaktif untuk melihat wawasan proaktif.
4. Pilih nama wawasan, memprioritaskan berdasarkan status dan tingkat keparahan.

   Halaman wawasan terperinci muncul.

Melihat anomali reaktif

Dalam wawasan, Anda dapat melihat anomali untuk sumber daya Amazon RDS. Pada halaman wawasan reaktif, di bagian Metrik agregat, Anda dapat melihat daftar anomali dengan garis waktu yang sesuai. Ada juga bagian yang menampilkan informasi tentang grup log dan peristiwa yang terkait dengan anomali. Anomali kausal dalam wawasan reaktif masing-masing memiliki halaman yang sesuai dengan detail tentang anomali tersebut.

Melihat analisis terperinci dari anomali reaktif RDS

Pada tahap ini, teliti anomali untuk mendapatkan analisis dan rekomendasi terperinci untuk instans Amazon RDS DB Anda.

Analisis terperinci hanya tersedia untuk instans Amazon RDS DB yang mengaktifkan Performance Insights.

Untuk menelusuri ke halaman detail anomali

1. Pada halaman wawasan, temukan metrik gabungan dengan jenis sumber daya AWS/RDS.
2. Pilih Lihat detail.

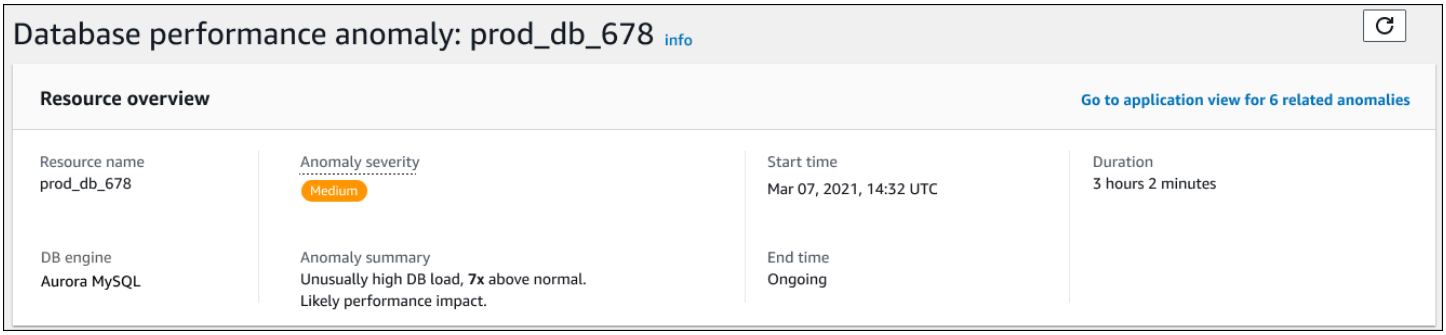
   Halaman detail anomali muncul. Judul dimulai dengan anomali kinerja Database dan memberi nama sumber daya yang ditampilkan. Konsol default ke anomali dengan tingkat keparahan tertinggi, terlepas dari kapan anomali terjadi.

3. (Opsional) Jika beberapa sumber daya terpengaruh, pilih sumber daya yang berbeda dari daftar di bagian atas halaman.

Berikut ini, Anda dapat menemukan deskripsi untuk komponen halaman detail.

Gambaran umum sumber daya

Bagian atas halaman detail adalah ikhtisar sumber daya. Bagian ini merangkum anomali kinerja yang dialami oleh instans DB Amazon RDS Anda.

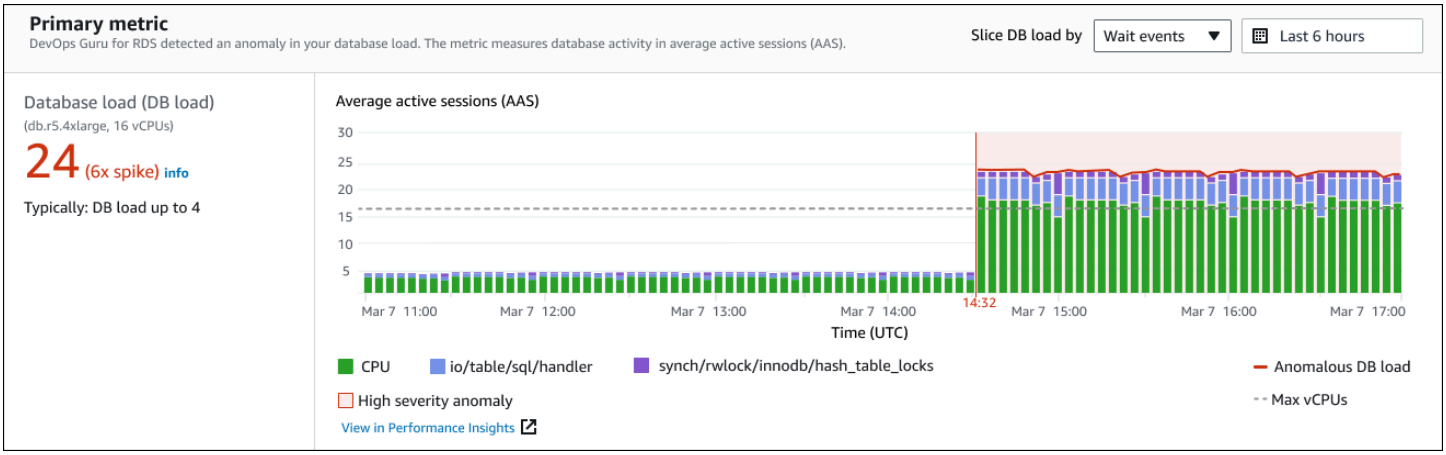


Bagian ini memiliki bidang berikut:

- Nama sumber daya — Nama instance DB yang mengalami anomali. Dalam contoh ini, sumber daya bernama prod_db_678.
- Mesin DB — Nama instance DB yang mengalami anomali. Dalam contoh ini, mesinnya adalah Aurora MySQL.
- Tingkat keparahan anomali — Ukuran dampak negatif anomali pada instans Anda. Kemungkinan tingkat keparahan adalah Tinggi, Sedang, dan R endah.
- Ringkasan anomali — Ringkasan singkat dari masalah ini. Ringkasan tipikal adalah beban DB yang luar biasa tinggi.
- Waktu mulai dan waktu akhir — Waktu ketika anomali dimulai dan berakhir. Jika waktu akhir sedang berlangsung, anomali masih terjadi.
- Durasi — Durasi perilaku anomali. Dalam contoh ini, anomali sedang berlangsung dan telah terjadi selama 3 jam 2 menit.

Metrik utama

Bagian metrik primer merangkum anomali kasual, yang merupakan anomali tingkat atas dalam wawasan. Anda dapat menganggap anomali kausal sebagai masalah umum yang dialami oleh instance DB Anda.



Panel kiri memberikan rincian lebih lanjut tentang masalah ini. Dalam contoh ini, ringkasan mencakup informasi berikut:

- Beban database (beban DB) — Kategorisasi anomali sebagai masalah beban database. Metrik yang sesuai dalam Performance Insights adalah`DBLoad`. Metrik ini juga dipublikasikan ke Amazon CloudWatch.
- db.r5.4xlarge — Kelas instans DB. Jumlah vCPU, yaitu 16 dalam contoh ini, sesuai dengan garis putus-putus di grafik Aver age active sessions (AAS).
- 24 (lonjakan 6x) — Beban DB, diukur dalam sesi aktif rata-rata (AAS) selama interval waktu yang dilaporkan dalam wawasan. Dengan demikian, pada waktu tertentu selama periode anomali, rata-rata 24 sesi aktif di database. Beban DB adalah 6 kali beban DB normal untuk contoh ini.
- Biasanya: beban DB hingga 4 - Dasar beban DB, diukur dalam AAS, selama beban kerja tipikal. Nilai 4 berarti bahwa, selama operasi normal, rata-rata 4 sesi atau lebih sedikit aktif di database pada waktu tertentu.

Secara default, bagan beban diiris oleh peristiwa tunggu. Ini berarti bahwa untuk setiap batang dalam grafik, area berwarna terbesar mewakili peristiwa tunggu yang berkontribusi paling besar terhadap total beban DB. Bagan menunjukkan waktu (berwarna merah) ketika masalah dimulai. Fokuskan perhatian Anda pada acara tunggu yang memakan ruang paling banyak di bar:

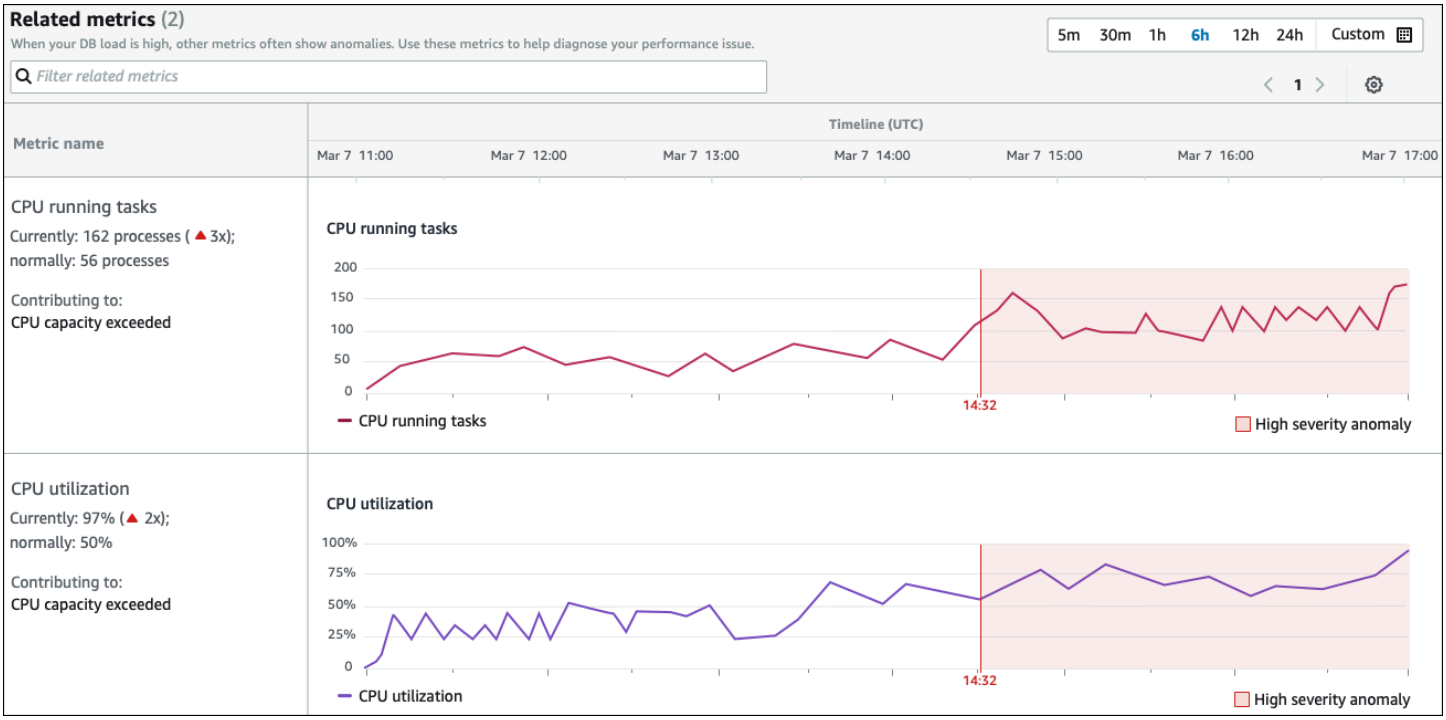
- `CPU`
- `IO:wait/io/sql/table/handler`

Peristiwa tunggu sebelumnya muncul lebih dari biasanya untuk database Aurora MySQL ini. Untuk mempelajari cara menyetel kinerja menggunakan acara tunggu di Amazon Aurora, lihat Menyet

el dengan acara tunggu untuk Aurora MySQL dan Menyetel dengan acara tunggu untuk Aurora PostgreSQL di Panduan Pengguna Amazon Aurora. Untuk mempelajari cara menyetel kinerja menggunakan peristiwa tunggu di RDS untuk PostgreSQL, lihat Menyetel dengan peristiwa tunggu untuk RDS untuk PostgreSQL di Panduan Pengguna Amazon RDS.

Metrik terkait

Bagian Metrik Ter kait mencantumkan anomali kontekstual, yang merupakan temuan spesifik dalam anomali kausal. Temuan ini memberikan informasi tambahan tentang masalah kinerja.



Tabel Metrik Ter kait memiliki dua kolom: Nama metrik dan Timeline (UTC). Setiap baris dalam tabel sesuai dengan metrik tertentu.

Kolom pertama dari setiap baris memiliki informasi berikut:

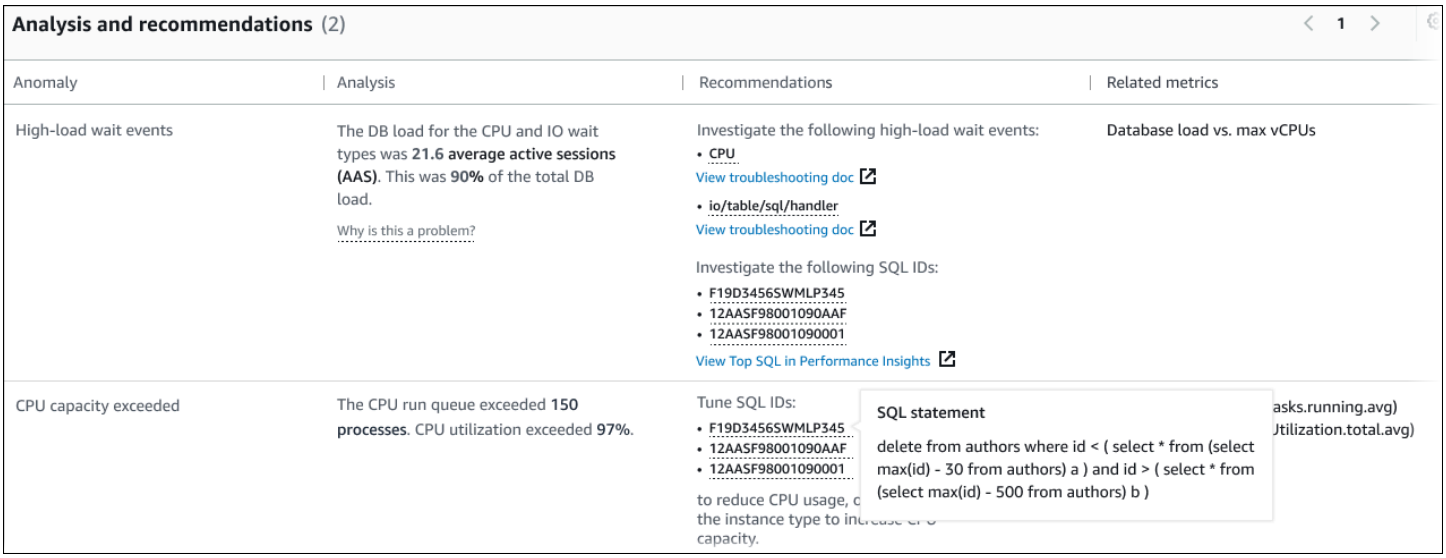
- ***Name***— Nama metrik. Baris pertama mengidentifikasi metrik sebagai tugas yang sedang berjalan CPU.
- Saat ini — Nilai metrik saat ini. Di baris pertama, nilai saat ini adalah 162 proses (3x).
- Biasanya — Basis dasar metrik ini untuk database ini ketika berfungsi normal. DevOpsGuru untuk RDS menghitung baseline sebagai nilai persentil ke-95 selama 1 minggu sejarah. Baris pertama menunjukkan bahwa 56 proses biasanya berjalan pada CPU.
- Berkontribusi pada — Temuan yang terkait dengan metrik ini. Di baris pertama, metrik tugas yang menjalankan CPU dikaitkan dengan kapasitas CPU melebihi anomali.

Kol om Timeline menunjukkan bagan garis untuk metrik. Area yang teduh menunjukkan interval waktu ketika DevOps Guru untuk RDS menetapkan temuan sebagai tingkat keparahan tinggi.

Analisis dan rekomendasi

Sedangkan anomali kausal menggambarkan masalah keseluruhan, anomali kontekstual menggambarkan temuan spesifik yang memerlukan penyelidikan. Setiap temuan sesuai dengan satu set metrik terkait.

Dalam contoh berikut dari bagian Analisis dan rekomendasi, anomali beban DB tinggi memiliki dua temuan.



Tabel memiliki kolom berikut:

- Anomali — Deskripsi umum dari anomali kontekstual ini. Dalam contoh ini, anomali pertama adalah peristiwa tunggu beban tinggi, dan yang kedua adalah kapasitas CPU terlampaui.
- Analisis — Penjelasan rinci tentang anomali.

  Pada anomali pertama, tiga jenis tunggu berkontribusi pada 90% beban DB. Pada anomali kedua, antrian berjalan CPU melebihi 150, yang berarti bahwa pada waktu tertentu, lebih dari 150 sesi menunggu waktu CPU. Pemanfaatan CPU lebih dari 97%, yang berarti bahwa selama masalah, CPU sibuk 97% dari waktu. Dengan demikian, CPU hampir terus-menerus ditempati sementara rata-rata 150 sesi menunggu untuk berjalan pada CPU.
- Rekomendasi — Respons pengguna yang disarankan terhadap anomali.

  Dalam anomali pertama, DevOps Guru untuk RDS merekomendasikan agar Anda menyelidiki peristiwa tunggu `cpu` dan`io/table/sql/handler`. Untuk mempelajari cara menyetel kinerja

database berdasarkan peristiwa ini, lihat cpu dan io/table/sql/handlerdi Panduan Pengguna Amazon Aurora.

Dalam anomali kedua, DevOps Guru untuk RDS merekomendasikan agar Anda mengurangi konsumsi CPU dengan menyetel tiga pernyataan SQL. Anda dapat mengarahkan kursor ke tautan untuk melihat teks SQL.

- Metrik terkait — Metrik yang memberi Anda pengukuran spesifik untuk anomali. Untuk informasi selengkapnya tentang metrik ini, lihat Referensi metrik untuk Amazon Aurora di Panduan Pengguna Amazon Aurora atau Refer ensi Metrik untuk Amazon RDS di Panduan Pengguna Amazon RDS.

  Dalam anomali pertama, DevOps Guru untuk RDS merekomendasikan agar membandingkan beban DB dengan CPU maksimum untuk instance Anda. Pada anomali kedua, rekomendasinya adalah melihat antrian berjalan CPU, pemanfaatan CPU, dan tingkat eksekusi SQL.

Melihat anomali proaktif

Dalam wawasan, Anda dapat melihat anomali untuk sumber daya Amazon RDS. Setiap wawasan proaktif memberikan rincian tentang satu anomali proaktif. Pada halaman wawasan proaktif, Anda dapat melihat ikhtisar wawasan, metrik terperinci tentang anomali, dan rekomendasi untuk mencegah masalah di masa mendatang. Untuk melihat anomali proaktif, buka halaman wawasan proaktif.

Gambaran umum wawasan

Bagian ikhtis ar Wawasan memberikan rincian tentang mengapa wawasan dibuat. Ini menampilkan tingkat keparahan wawasan serta deskripsi anomali dan jangka waktu kapan anomali terjadi. Ini juga mencantumkan jumlah layanan dan aplikasi yang terpengaruh yang terdeteksi oleh DevOps Guru.

Metrik-metrik

Bagian Metrik menyediakan grafik anomali. Setiap grafik menampilkan ambang batas yang ditentukan oleh perilaku dasar sumber daya, serta data metrik yang dilaporkan dari waktu anomali.

Rekomendasi untuk sumber daya agregat

Bagian ini menyarankan tindakan yang dapat Anda ambil untuk mengurangi masalah yang dilaporkan sebelum menjadi masalah yang lebih besar. Tindakan yang dapat Anda lakukan disajikan di kolom Perubahan kustom yang disarankan. Alasan di balik rekomendasi disajikan dalam Mengapa DevOps Guru merekomendasikan hal ini? kolom. Untuk informasi selengkapnya tentang cara menanggapi rekomendasi, lihatthe section called “Menanggapi rekomendasi”.

Menanggapi rekomendasi

Rekomendasi adalah bagian terpenting dari wawasan. Pada tahap analisis ini, Anda bertindak untuk menyelesaikan masalah kinerja. Biasanya, Anda mengambil langkah-langkah berikut:

1. Putuskan apakah masalah kinerja yang dilaporkan menunjukkan masalah nyata.

   Dalam beberapa kasus, masalah mungkin diharapkan dan jinak. Misalnya, jika Anda memasukkan database pengujian ke beban DB yang ekstrem, DevOps Guru untuk RDS melaporkan beban sebagai anomali kinerja. Namun, Anda tidak perlu memperbaiki anomali ini karena ini adalah hasil yang diharapkan dari pengujian Anda.

   Jika Anda menentukan bahwa masalah memerlukan tanggapan, lanjutkan ke langkah berikutnya.
2. Putuskan apakah akan menerapkan rekomendasi.

   Dalam tabel rekomendasi, kolom menunjukkan tindakan yang disarankan. Untuk wawasan reaktif, ini adalah kolom Apa yang kami rekomendasikan pada halaman detail anomali reaktif. Untuk wawasan proaktif, ini adalah kolom Perubahan kustom yang disarankan pada halaman wawasan proaktif.

   DevOpsGuru untuk RDS menawarkan daftar rekomendasi yang mencakup beberapa skenario bermasalah potensial. Setelah meninjau daftar ini, tentukan rekomendasi mana yang lebih relevan dengan situasi Anda saat ini dan pertimbangkan untuk menerapkannya. Jika rekomendasi berhasil untuk situasi Anda, lanjutkan ke langkah berikutnya. Jika tidak, lewati langkah yang tersisa dan pecahkan masalah menggunakan teknik manual.
3. Lakukan tindakan yang disarankan.

   DevOpsGuru untuk RDS merekomendasikan agar Anda melakukan salah satu dari hal berikut:

   - Lakukan tindakan korektif tertentu.

     Misalnya, DevOps Guru untuk RDS mungkin menyarankan Anda meningkatkan kapasitas CPU, menyetel pengaturan kumpulan aplikasi, atau mengaktifkan Skema Kinerja.
   - Selidiki penyebab masalah.

     Biasanya, DevOps Guru untuk RDS merekomendasikan agar Anda menyelidiki pernyataan SQL tertentu atau menunggu peristiwa. Misalnya, rekomendasi mungkin untuk menyelidiki peristiwa tunggu`io/table/sql/handler`. Cari acara tunggu yang terdaftar di Menyetel dengan acara tunggu untuk Aurora PostgreSQL atau Tuning dengan acara tunggu untuk Aurora MySQL di Panduan Pengguna Amazon Aurora, atau di Menyetel dengan acara tunggu untuk RDS

untuk PostgreSQL di Panduan Pengguna Amazon RDS. Kemudian lakukan tindakan yang disarankan.

> **Important**
>
> Sebaiknya uji setiap perubahan pada instans uji sebelum diterapkan pada instans produksi. Dengan cara ini, Anda memahami dampak perubahan.

Memantau database non-relasional menggunakan Guru DevOps

DevOpsGuru mampu menghasilkan wawasan untuk database non-relasional atau NoSQL Anda yang membantu Anda menjaga sumber daya Anda dikonfigurasi sesuai dengan praktik terbaik. Misalnya, DevOps Guru dapat membantu Anda tetap di atas perencanaan kapasitas dengan meramalkan kebutuhan masa depan berdasarkan lalu lintas yang ada. DevOpsGuru dapat mengidentifikasi apakah Anda menggunakan lebih sedikit sumber daya daripada yang Anda konfigurasi dan memberikan rekomendasi untuk meningkatkan ketersediaan aplikasi berdasarkan penggunaan historis Anda. Ini dapat membantu Anda mengurangi biaya yang tidak perlu.

Di luar perencanaan kapasitas, DevOps Guru mendeteksi dan membantu Anda memecahkan masalah operasional seperti pembatasan, konflik transaksi, kegagalan pemeriksaan bersyarat, dan area untuk perbaikan parameter SDK. Database biasanya terhubung dengan beberapa layanan dan sumber daya, dan DevOps Guru dapat mengkorelasikan struktur aplikasi Anda untuk analisis menggunakan grup berdasarkan penandaan atau agregasi. CloudFormation Anomali dapat melibatkan banyak sumber daya yang semuanya dipengaruhi oleh solusi yang sama. DevOps Guru mampu berkorelasi di berbagai metrik sumber daya, konfigurasi, log, dan peristiwa. Misalnya, DevOps Guru dapat menganalisis dan menghubungkan data dari fungsi Lambda yang mungkin membaca atau menulis data dari tabel. Amazon DynamoDB Dengan cara ini, DevOps Guru memantau beberapa sumber daya terkait untuk mendeteksi anomali dan memberikan wawasan yang berguna untuk solusi database Anda.

Memantau operasi database di Amazon DynamoDB

Tabel di bawah ini menunjukkan contoh skenario dan wawasan yang dipantau DevOps Guru. Amazon DynamoDB

Amazon DynamoDB kasus penggunaan	Contoh	Metrik-metrik
Mendeteksi ketika persentase besar AccountProvisioned ReadCapacityUtilization dan AccountProvisioned WriteCapacityUtilization sedang digunakan, karena sejumlah besar permintaan baca dan tulis.	Amazon DynamoDB kapasitas konsumsi tabel untuk permintaan baca atau tulis mencapai batas tingkat tabel.	AccountProvisioned ReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
Mendeteksi kegagalan pemeriksaan bersyarat dalam Amazon DynamoDB permintaan yang disebabkan oleh ekspresi kondisi yang disediakan tidak cocok dengan apa yang diharapkan dalam database.	Kegagalan pemeriksaan bersyarat disebabkan oleh data buruk di tabel Anda, ekspresi kondisi yang ketat, atau kondisi balapan.	ConditionalCheckFailedRequests

Memantau operasi database di Amazon ElastiCache

Tabel di bawah ini menunjukkan contoh skenario dan wawasan yang dipantau DevOps Guru. Amazon ElastiCache

Skenario yang diidentifikasi DevOps Guru	CloudWatch metrik dipantau
Deteksi saat Amazon ElastiCache klaster mencapai batas komputasi untuk Redis atau Memcached karena perubahan permintaan pada cluster Anda.	CPUUtilization, MesinCPUUtilization, Penggusuran

Integrasi dengan Profiler CodeGuru

Bagian ini memberikan ikhtisar tentang bagaimana Amazon DevOps Guru terintegrasi dengan Amazon CodeGuru Profiler. Anda dapat melihat rekomendasi dari CodeGuru Profiler sebagai wawasan di konsol DevOps Guru.

Amazon DevOps Guru terintegrasi dengan Amazon CodeGuru Profiler dengan aturan EventBridge terkelola. CodeGuru Profiler mengirimkan acara ke EventBridge. Aturan terkelola merutekan peristiwa yang dikirim dengan bus acara default. Setiap peristiwa masuk dari CodeGuru Profiler adalah laporan anomali proaktif. Untuk informasi selengkapnya, lihat Bekerja EventBridge dengan CodeGuru Profiler.

DevOpsGuru mendukung acara masuk dengan EventBridge. Suatu peristiwa menunjukkan perubahan dalam rekomendasi yang diidentifikasi DevOps Guru. CodeGuru Profiler mengirimkan acara detak jantung setiap 24 jam untuk menunjukkan kelangsungan acara. Acara membawa informasi rekomendasi CodeGuru Profiler serta metadata untuk sumber daya komputasi Anda. Untuk informasi tentang siklus hidup acara, lihat Acara Amazon EventBridge .

Saat Anda mengatur DevOps Guru, DevOps Guru membuat Aturan EventBridge Terkelola di akun Anda yang merutekan peristiwa dari layanan lain. Aturan ini rute ke DevOps Guru. Pemberitahuan dikirim ketika ada acara masuk.

Bus acara menerima acara dari sumber seperti DevOps Guru dan mengarahkan mereka ke aturan yang terkait dengan bus acara itu. Untuk informasi lebih lanjut tentang bus acara, lihat Bus acara.

Untuk informasi tentang beberapa parameter, lihat EventBridgeperistiwa Amazon.

Untuk menerima wawasan CodeGuru Profiler di DevOps Guru, Anda harus memiliki yang berikut ini.

- CodeGuru Profiler harus diaktifkan. Untuk informasi tentang mengaktifkan CodeGuru Profiler, lihat CodeGuru Menyiapkan Profiler.
- DevOpsGuru harus diaktifkan. Untuk informasi tentang mengaktifkan DevOps Guru, lihat Mengaktifkan DevOps Guru.
- Sumber daya yang sama harus dipantau di Wilayah yang sama di CodeGuru Profiler dan DevOps Guru.

Mendefinisikan aplikasi menggunakan sumber daya AWS

Amazon DevOps Guru mengelompokkan sumber daya yang berada dalam batas cakupan yang menentukan sumber daya mana yang dianalisis untuk wawasan operasional. Sumber daya dikelompokkan berdasarkan sumber daya dalam CloudFormation tumpukan atau sumber daya dengan tag. Anda memilih tumpukan atau tag ketika Anda mengatur DevOps Guru. Anda juga dapat memperbarui tumpukan atau tag nanti. Kami menyarankan Anda menganggap grup sumber daya Anda sebagai aplikasi. Misalnya, Anda mungkin memiliki semua sumber daya yang Anda gunakan untuk aplikasi pemantauan yang ditentukan dalam satu tumpukan. Atau Anda dapat menambahkan tag yang sama ke semua sumber daya yang Anda gunakan dalam aplikasi database. batas yang menentukan sumber daya mana yang dianalisis Guru. DevOps Semua sumber daya dalam koleksi berada di dalam batas ini. Sumber daya apa pun di akun Anda yang tidak ada dalam pengumpulan sumber daya Anda berada di luar batas dan tidak dianalisis. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

Anda dapat menentukan batas cakupan Anda yang berisi sumber daya dalam aplikasi Anda dengan tiga cara.

- Tentukan bahwa semua AWS sumber daya yang didukung di AWS akun dan Wilayah Anda. Ini menjadikan akun dan Wilayah Anda menjadi batas sumber daya Anda. Dengan opsi ini, DevOps Guru menganalisis setiap sumber daya yang didukung di akun dan Wilayah Anda. Semua sumber daya yang ada dalam satu tumpukan dikelompokkan ke dalam aplikasi. Setiap sumber daya yang tidak ada dalam tumpukan dikelompokkan ke dalam aplikasi mereka sendiri.
- Gunakan CloudFormation tumpukan untuk menentukan sumber daya dalam aplikasi Anda. Tumpukan berisi sumber daya yang dihasilkan menggunakan CloudFormation. Di DevOps Guru, Anda memilih tumpukan di akun Anda. Sumber daya yang Anda miliki di setiap tumpukan yang Anda pilih dikelompokkan ke dalam aplikasi. Semua sumber daya dalam tumpukan dianalisis oleh DevOps Guru untuk wawasan.
- Gunakan AWS tag untuk menentukan sumber daya dalam aplikasi Anda. AWS Tag berisi kunci dan nilai. Di DevOps Guru, pilih satu kunci tag dan secara opsional pilih satu atau lebih nilai yang dipasangkan dengan kunci itu. Anda dapat menggunakan nilai untuk mengelompokkan sumber daya Anda ke dalam aplikasi.

Lihat informasi yang lebih lengkap di Memperbarui cakupan AWS analisis Anda di DevOps Guru.

Topik

- Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda
- Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda

Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda

Anda dapat menggunakan tag untuk mengidentifikasi AWS sumber daya yang dianalisis Amazon DevOps Guru dan untuk menentukan sumber daya mana yang dikelompokkan untuk pemantauan dengan kunci tag dan nilai tag yang dipilih. Anda dapat mengedit konfigurasi ini saat mengatur DevOps Guru atau ketika Anda memilih Edit sumber daya yang dianalisis dari halaman sumber daya yang dianalisis. Setelah memilih Tag, Anda memilih kunci tag tertentu yang ingin Anda pantau DevOps oleh Amazon Guru. Untuk menganalisis semua sumber daya di akun dan menggunakan nilai tag untuk mengelompokkan sumber daya, pilih Semua Sumber Daya Akun. Untuk menggunakan nilai tag untuk menentukan sumber daya untuk DevOps dianalisis Guru, pilih Pilih nilai tag tertentu.

> **Note**
>
> Ketika Semua Sumber Daya Akun dipilih dan tidak ada nilai tag, sumber daya tanpa kunci tag dikelompokkan dan dianalisis secara terpisah.

Anda menggunakan kunci tag untuk mengidentifikasi sumber daya, lalu menggunakan nilai dengan kunci itu untuk mengelompokkan sumber daya ke dalam aplikasi Anda. Misalnya, Anda dapat menandai sumber daya Anda dengan kunci `devops-guru-applications`, lalu gunakan kunci tersebut dengan nilai yang berbeda untuk setiap aplikasi Anda. Anda dapat menggunakan kunci tag - pasangan nilai`devops-guru-applications/database`,`devops-guru-applications/cicd`, dan `devops-guru-applications/monitoring` untuk mengidentifikasi tiga aplikasi di akun Anda. Setiap aplikasi terdiri dari sumber daya terkait yang berisi kunci tag yang sama - pasangan nilai. Anda menambahkan tag ke sumber daya Anda menggunakan AWS layanan tempat mereka berada. Untuk informasi selengkapnya, lihat Menambahkan AWS tag ke AWS sumber daya.

Setelah menambahkan tag ke sumber daya di aplikasi, Anda dapat memfilter wawasan berdasarkan tag pada sumber daya yang menghasilkannya. Untuk informasi selengkapnya tentang cara memfilter wawasan menggunakan tag, lihatMelihat wawasan DevOps Guru.

Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

Topik

- Apa itu AWS tag?
- Mendefinisikan aplikasi DevOps Guru menggunakan tag
- Menggunakan tag dengan DevOps Guru
- Menambahkan AWS tag ke AWS sumber daya

Apa itu AWS tag?

Tag membantu Anda mengidentifikasi dan mengatur AWS sumber daya Anda. Banyak AWS layanan mendukung penandaan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya terkait. Misalnya, Anda dapat menetapkan tag yang sama ke sumber daya tabel Amazon DynamoDB yang Anda tetapkan ke suatu AWS Lambda fungsi. Untuk informasi lebih lanjut tentang penggunaan tanda, lihat laporan resmi Praktik terbaik.

Setiap AWS tag memiliki dua bagian.

- Kunci tag (misalnya, `CostCenter`, `Environment`, `Project`, atau `Secret`). K unci tag peka huruf besar/kecil.
- Bidang opsional yang dikenal sebagai nilai tag (misalnya, `111122223333`, `Production`, atau nama tim). Menghilangkan nilai tag sama dengan menggunakan string kosong. Seperti kunci tag, nilai tag peka huruf besar-kecil.

Bersama-sama ini dikenal sebagai pasangan nilai kunci.

Mendefinisikan aplikasi DevOps Guru menggunakan tag

Untuk menentukan aplikasi Amazon DevOps Guru menggunakan tag, tambahkan tag itu ke AWS sumber daya di akun Anda yang membentuk aplikasi Anda. Tag Anda berisi kunci dan nilai. Kami menyarankan Anda menambahkan tag ke setiap AWS sumber daya Anda yang dianalisis oleh DevOps Guru yang memiliki kunci yang sama. Gunakan nilai yang berbeda dalam tag untuk mengelompokkan sumber daya ke dalam aplikasi Anda. Misalnya, Anda dapat menetapkan tag dengan kunci `devops-guru-analysis-boundary` ke semua AWS sumber daya di batas cakupan Anda. Gunakan nilai yang berbeda dengan kunci itu untuk mengidentifikasi aplikasi di

akun Anda. Anda dapat menggunakan nilai `containers`,`database`, dan `monitoring` untuk tiga aplikasi. Untuk informasi selengkapnya, lihat Memperbarui cakupan AWS analisis Anda di DevOps Guru.

Jika Anda menggunakan AWS tag untuk menentukan sumber daya mana yang akan dianalisis, Anda dapat menggunakan tag hanya dengan satu kunci. Anda dapat memas angkan kunci tag Anda dipasangkan dengan nilai apa pun. Gunakan nilai untuk mengelompokkan sumber daya yang berisi kunci Anda ke dalam aplikasi operasional Anda.

> **Important**
>
> Saat Anda membuat kunci, kasus karakter dalam kunci dapat menjadi apa pun yang Anda pilih. Setelah Anda membuat kunci, kunci tersebut peka huruf besar/kecil. Misalnya, DevOps Guru bekerja dengan kunci bernama `devops-guru-rds` dan kunci bernama`DevOps-Guru-RDS`, dan ini bertindak sebagai dua kunci yang berbeda. Kem ungkinan pasangan kunci /nilai dalam aplikasi Anda mungkin `Devops-Guru-production-application/RDS` atau`Devops-Guru-production-application/containers`.

Menggunakan tag dengan DevOps Guru

Tentukan AWS tag yang mengidentifikasi AWS sumber daya yang ingin Anda analisis oleh Amazon DevOps Guru, atau tentukan nilai tag yang mengidentifikasi sumber daya mana yang akan dikelompokkan. Sumber daya ini adalah batas cakupan sumber daya Anda. Anda dapat memilih satu kunci dan nol atau lebih nilai.

Untuk memilih tag Anda

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Buka panel navigasi, lalu perluas Peng aturan.
3. Di Sumber daya yang dianalisis, pilih Edit.
4. Pilih Tag jika Anda ingin DevOps Guru menganalisis semua sumber daya yang berisi tag yang Anda pilih. Pilih kunci, lalu pilih salah satu opsi berikut.

   - Semua sumber daya akun — Analisis semua AWS sumber daya di Wilayah dan akun saat ini. Sumber daya dengan kunci tag yang dipilih dikelompokkan berdasarkan nilai tag, jika ada. Sumber daya tanpa kunci tag ini dikelompokkan dan dianalisis secara terpisah.

- Pilih nilai tag tertentu — Semua sumber daya yang berisi tag dengan kunci yang Anda pilih dianalisis. DevOpsGuru mengelompokkan sumber daya Anda ke dalam aplikasi berdasarkan nilai tag Anda.

5. Pilih Simpan.

Menambahkan AWS tag ke AWS sumber daya

Saat Anda menentukan AWS tag yang mengidentifikasi AWS sumber daya yang ingin Anda analisis DevOps oleh Guru, pilih tag yang memiliki sumber daya yang terkait dengannya. Anda dapat menambahkan tag ke sumber daya menggunakan AWS layanan yang dimiliki setiap sumber daya, atau menggunakan Editor AWS Tag.

- Untuk mengelola tag menggunakan layanan sumber daya Anda, gunakan konsol AWS Command Line Interface, atau SDK layanan yang dimiliki sumber daya. Misalnya, Anda dapat menandai sumber daya aliran Amazon Kinesis atau sumber daya CloudFront distribusi Amazon. Ini adalah dua contoh layanan dengan sumber daya yang dapat ditandai. Sebagian besar sumber daya yang dapat dianalisis DevOps Guru mendukung tag. Untuk informasi selengkapnya, lihat Menandai streaming Anda di Panduan Pengembang Amazon Kinesis dan Men andai distribusi di Panduan Pengembang Amazon CloudFront . Untuk mempelajari cara menambahkan tag ke jenis sumber daya lain, lihat panduan pengguna atau panduan pengembang untuk AWS layanan yang menjadi miliknya.

  > **Note**
  >
  > Saat menandai sumber daya Amazon RDS, Anda harus menandai instance database dan bukan cluster.

- Anda dapat menggunakan Editor AWS Tag untuk mengelola tag berdasarkan sumber daya di Wilayah Anda dan berdasarkan sumber daya di AWS layanan tertentu. Untuk informasi selengkapnya, lihat Editor tag di AWS Panduan Pengguna Grup Sumber Daya dan Tag.

Saat menambahkan tag ke sumber daya, Anda dapat menambahkan kunci saja, atau kunci dan nilai. Misalnya, Anda dapat membuat tag dengan kunci `devops-guru-` untuk semua sumber daya yang merupakan bagian dari DevOps aplikasi Anda. Anda juga dapat menambahkan tag dengan kunci `devops-guru-` dan nilainya *`RDS`*, lalu menambahkan pasangan kunci - nilai itu hanya ke

sumber daya Amazon RDS di aplikasi Anda. Ini berguna jika Anda ingin melihat wawasan di konsol yang dihasilkan hanya dari sumber daya Amazon RDS di aplikasi Anda.

Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda

Anda dapat menggunakan AWS CloudFormation tumpukan untuk menentukan AWS sumber daya mana yang ingin dianalisis DevOps Guru. Stack adalah kumpulan sumber AWS daya yang dikelola sebagai satu unit. Sumber daya di tumpukan yang Anda pilih membentuk batas cakupan DevOps Guru Anda. Untuk setiap tumpukan yang Anda pilih, data operasional dalam sumber daya yang didukung dianalisis untuk perilaku anomali. Masalah-masalah tersebut kemudian dikelompokkan ke dalam anomali terkait untuk menciptakan wawasan. Setiap wawasan mencakup satu atau lebih rekomendasi untuk membantu Anda mengatasinya. Jumlah maksimum tumpukan yang dapat Anda tentukan adalah 1000. Untuk informasi selengkapnya, lihat Bekerja dengan tumpukan di Panduan AWS CloudFormation Pengguna danMemperbarui cakupan AWS analisis Anda di DevOps Guru.

Setelah Anda memilih tumpukan, DevOps Guru segera mulai menganalisis sumber daya apa pun yang Anda tambahkan ke dalamnya. Jika Anda menghapus sumber daya dari tumpukan, itu tidak lagi dianalisis.

Jika Anda memilih agar DevOps Guru menganalisis semua sumber daya yang didukung di akun Anda (ini berarti AWS akun dan Wilayah Anda adalah batas cakupan DevOps Guru Anda), DevOps Guru menganalisis dan membuat wawasan untuk setiap sumber daya yang didukung di akun Anda, termasuk yang ada di tumpukan. Wawasan yang dibuat dari anomali dalam sumber daya yang tidak ada dalam tumpukan dikelompokkan di tingkat akun. Jika wawasan dibuat dari anomali dalam sumber daya yang ada di tumpukan, maka itu dikelompokkan pada tingkat tumpukan. Untuk informasi selengkapnya, lihat Memahami bagaimana perilaku anomali dikelompokkan ke dalam wawasan.

Memilih tumpukan untuk DevOps dianalisis Guru

Tentukan sumber daya yang ingin Anda analisis Amazon DevOps Guru dengan memilih CloudFormation tumpukan yang membuatnya. Anda dapat melakukan ini menggunakan Konsol Manajemen AWS atau SDK.

Topik

- Memilih tumpukan untuk dianalisis DevOps Guru (konsol)

- Memilih tumpukan untuk dianalisis DevOps Guru (DevOpsGuru SDK)

Memilih tumpukan untuk dianalisis DevOps Guru (konsol)

Anda dapat menambahkan AWS CloudFormation tumpukan menggunakan konsol.

Untuk memilih tumpukan yang berisi sumber daya untuk dianalisis

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Buka panel navigasi, lalu pilih Pengaturan.
3. Dalam cakupan analisis DevOps Guru, pilih Kelola.
4. Pilih CloudFormation tumpukan jika Anda ingin DevOps Guru menganalisis sumber daya yang ada di tumpukan yang Anda pilih, lalu pilih salah satu opsi berikut.
   - Semua sumber daya — Semua sumber daya yang ada di tumpukan di akun Anda dianalisis. Sumber daya di setiap tumpukan dikelompokkan ke dalam aplikasi mereka sendiri. Sumber daya apa pun di akun Anda yang tidak ada dalam tumpukan tidak dianalisis.
   - Pilih tumpukan — Pilih tumpukan yang ingin dianalisis DevOps Guru. Sumber daya di setiap tumpukan yang Anda pilih dikelompokkan ke dalam aplikasi mereka sendiri. Anda dapat memasukkan nama tumpukan di Temukan tumpukan untuk menemukan tumpukan tertentu dengan cepat. Anda dapat memilih hingga 1.000 tumpukan.
5. Pilih Simpan.

Memilih tumpukan untuk dianalisis DevOps Guru (DevOpsGuru SDK)

Untuk menentukan CloudFormation tumpukan menggunakan Amazon DevOps Guru SDK, gunakan metode ini`UpdateResourceCollection`. Untuk informasi selengkapnya, lihat UpdateResourceCollectiondi Referensi API Amazon DevOps Guru.

Bekerja dengan Amazon EventBridge

Amazon DevOps Guru terintegrasi dengan Amazon EventBridge untuk memberi tahu Anda tentang peristiwa tertentu yang berkaitan dengan wawasan dan pembaruan wawasan terkait. Acara dari AWS Layanan disampaikan ke EventBridge hampir secara real time. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Tindakan yang dapat dimulai secara otomatis mencakup contoh-contoh berikut:

- Memanggil AWS Lambda fungsi
- Memanggil perintah run Amazon Elastic Compute Cloud
- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin status Fungsi Langkah
- Memberi tahu Amazon SNS atau Amazon SQS

Anda dapat memilih salah satu pola yang telah ditentukan berikut untuk memfilter peristiwa atau membuat aturan pola khusus untuk memulai tindakan di yang didukung AWS sumber daya.

- DevOps Guru New Insight Terbuka
- DevOps Asosiasi Anomali Baru Guru
- DevOps Tingkat keparahan Guru Insight Ditingkatkan
- DevOps Guru Rekomendasi Baru Dibuat
- DevOps Guru Insight Ditutup

Acara untuk DevOps Guru

Berikut ini adalah contoh peristiwa dari DevOps Guru. Peristiwa dipancarkan atas dasar upaya terbaik. Untuk mempelajari lebih lanjut tentang pola acara, lihat Memulai dengan Amazon EventBridge atau Amazon EventBridge pola acara.

DevOps Acara Terbuka Guru New Insight

Kapan DevOps Guru membuka wawasan baru, ia mengirimkan peristiwa berikut.

```
{
```

```
    "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"
    }
  },
```

Pola peristiwa sampel khusus untuk Insight baru dengan tingkat keparahan tinggi

Aturan menggunakan pola kejadian untuk memilih kejadian dan merutekannya ke target. Berikut ini adalah contoh DevOps Pola acara Guru.

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

Memperbarui pengaturan DevOps Guru

Anda dapat memperbarui pengaturan Amazon DevOps Guru berikut:

- Cakupan DevOps Guru Anda. Ini menentukan sumber daya mana di akun Anda yang dianalisis.
- Pemberitahuan Anda. Ini menentukan topik Layanan Pemberitahuan Sederhana Amazon mana yang digunakan untuk memberi tahu Anda tentang peristiwa DevOps Guru penting.
- Fitur untuk wawasan yang disempurnakan. Ini termasuk deteksi anomali log, enkripsi, dan pengaturan AWS Systems Manager integrasi Anda. Ini menentukan apakah DevOps Guru menampilkan data log, apakah Anda menggunakan kunci keamanan tambahan, dan apakah sebuah OpsItem dibuat di Systems Manager OpsCenter untuk setiap wawasan baru.

Topik

- Memperbarui pengaturan akun manajemen Anda
- Memperbarui cakupan AWS analisis Anda di DevOps Guru
- Memperbarui notifikasi Anda di DevOps Guru
- Memfilter notifikasi DevOps Guru Anda
- Memperbarui AWS Systems Manager integrasi di DevOps Guru
- Memperbarui deteksi anomali log di Guru DevOps
- Memperbarui pengaturan enkripsi di DevOps Guru

Memperbarui pengaturan akun manajemen Anda

Anda dapat mengonfigurasi DevOps Guru untuk akun di organisasi Anda. Jika Anda belum mendaftarkan administrator yang didelegasikan, Anda dapat melakukannya dengan memilih Daftarkan administrator yang didelegasikan. Untuk informasi selengkapnya tentang mendaftarkan administrator yang didelegasikan, lihat Mengaktifkan DevOps Guru.

Memperbarui cakupan AWS analisis Anda di DevOps Guru

Anda dapat memperbarui AWS sumber daya mana yang ada di analisis DevOps Guru akun Anda. Untuk melakukan ini, navigasikan ke halaman Sumber daya yang dianalisis di konsol dan kemudian pilih Edit. Untuk informasi selengkapnya, lihat Melihat sumber daya yang dianalisis.

Memperbarui notifikasi Anda di DevOps Guru

Siapkan topik Layanan Pemberitahuan Sederhana Amazon yang digunakan untuk memberi tahu Anda tentang peristiwa penting Amazon DevOps Guru. Anda dapat memilih dari daftar nama topik yang sudah ada di AWS akun Anda, masukkan nama untuk topik baru yang dibuat DevOps Guru di akun Anda, atau masukkan Nama Sumber Daya Amazon (ARN) dari topik yang ada di AWS akun mana pun di Wilayah Anda. Jika Anda menentukan ARN dari topik yang tidak ada di akun Anda, Anda harus memberikan izin kepada DevOps Guru untuk mengakses topik tersebut dengan menambahkan kebijakan IAM ke dalamnya. Untuk informasi selengkapnya, lihat Izin untuk topik Amazon SNS. Anda dapat menentukan hingga dua topik.

DevOpsGuru mengirimkan pemberitahuan untuk pembaruan berikut:

- Wawasan baru dibuat.
- Anomali baru ditambahkan ke wawasan.
- Tingkat keparahan wawasan ditingkatkan dari `Low` atau `Medium` ke`High`.
- Status wawasan berubah dari yang sedang berlangsung menjadi diselesaikan.
- Rekomendasi untuk wawasan diidentifikasi.

DevOpsGuru juga mengirimkan pemberitahuan jika CloudFormation tumpukan atau kunci tag yang dipilih tidak valid saat Anda mencoba menambahkan sumber daya ke akun Guru Anda DevOps.

Anda dapat memilih untuk menerima pemberitahuan Amazon SNS untuk semua jenis pembaruan pada suatu masalah atau untuk menerima pemberitahuan Amazon SNS hanya ketika masalah dibuka, ditutup, atau memiliki perubahan tingkat keparahan. Secara default, Anda menerima pemberitahuan untuk semua pembaruan.

Untuk memperbarui notifikasi, pertama-tama navigasikan ke halaman notifikasi, lalu pilih apakah akan menambahkan, menghapus, atau memperbarui konfigurasi untuk topik notifikasi Amazon SNS.

Topik

- Arahkan ke pengaturan notifikasi di konsol DevOps Guru
- Menambahkan topik notifikasi Amazon SNS di konsol Guru DevOps
- Menghapus topik notifikasi Amazon SNS di konsol Guru DevOps
- Memperbarui konfigurasi notifikasi Amazon SNS
- Izin ditambahkan ke topik Amazon SNS Anda

Arahkan ke pengaturan notifikasi di konsol DevOps Guru

Untuk memperbarui notifikasi, Anda harus terlebih dahulu menavigasi ke bagian pengaturan notifikasi.

Untuk menavigasi ke bagian pengaturan notifikasi

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Pilih Pengaturan di panel navigasi.

   Halaman Pengaturan menyertakan bagian Pemberitahuan, dengan informasi tentang topik Amazon SNS yang dikonfigurasi.

Menambahkan topik notifikasi Amazon SNS di konsol Guru DevOps

Untuk menambahkan topik notifikasi Amazon SNS di konsol Guru DevOps

1. the section called “Arahkan ke pengaturan notifikasi di konsol DevOps Guru”.
2. Pilih Tambahkan notifikasi.
3. Untuk menambahkan topik Amazon SNS, lakukan salah satu hal berikut.

   - Pilih Hasilkan topik SNS baru menggunakan email. Kemudian, dari Tentukan alamat email, masukkan alamat email yang ingin Anda terima notifikasi. Untuk memasukkan alamat email tambahan, pilih Tambahkan email baru.
   - Pilih Gunakan topik SNS yang ada. Kemudian, dari Pilih topik di AWS akun Anda, pilih topik yang ingin Anda gunakan.
   - Pilih Gunakan ARN topik SNS yang ada untuk menentukan topik yang ada dari akun lain. Kemudian, di Masukkan ARN untuk suatu topik, masukkan topik ARN. ARN adalah Nama Sumber Daya Amazon topik. Anda dapat menentukan topik di akun yang berbeda. Jika Anda menggunakan topik di akun lain, Anda harus menambahkan kebijakan sumber daya ke topik tersebut. Untuk informasi selengkapnya, lihat Izin untuk topik Amazon SNS.
4. Pilih Simpan.

Menghapus topik notifikasi Amazon SNS di konsol Guru DevOps

Untuk menghapus topik Amazon SNS di konsol Guru DevOps

1. the section called “Arahkan ke pengaturan notifikasi di konsol DevOps Guru”.
2. Pilih Pilih topik yang ada.
3. Dari menu tarik-turun, pilih topik yang ingin Anda hapus.
4. Pilih Hapus.
5. Pilih Simpan.

Memperbarui konfigurasi notifikasi Amazon SNS

Ada dua jenis konfigurasi notifikasi untuk topik DevOps notifikasi Amazon SNS di Guru. Anda dapat memilih untuk menerima pemberitahuan dari semua tingkat keparahan atau hanya pemberitahuan dengan tingkat keparahan Tinggi dan Menengah. Anda juga dapat memilih untuk menerima pemberitahuan untuk semua jenis pembaruan atau hanya beberapa jenis pembaruan.

Saat Anda memilih untuk menerima notifikasi Amazon SNS untuk semua jenis pembaruan masalah ini, DevOps Guru mengirimkan pemberitahuan untuk pembaruan berikut:

- Wawasan baru dibuat.
- Anomali baru ditambahkan ke wawasan.
- Tingkat keparahan wawasan ditingkatkan dari `Low` atau `Medium` ke`High`.
- Status wawasan berubah dari yang sedang berlangsung menjadi diselesaikan.
- Rekomendasi untuk wawasan diidentifikasi.

Secara default, Anda hanya menerima pemberitahuan tingkat keparahan Tinggi dan Menengah, dan Anda menerima pemberitahuan untuk semua jenis pembaruan.

Untuk memperbarui konfigurasi notifikasi untuk topik notifikasi Amazon SNS

1. the section called “Arahkan ke pengaturan notifikasi di konsol DevOps Guru”.
2. Pilih Pilih topik yang ada.
3. Dari menu tarik-turun, pilih topik yang ingin Anda update.

4. Pilih Semua tingkat keparahan untuk menerima pemberitahuan dengan tingkat keparahan Tinggi, Sedang, dan Rendah, atau pilih Hanya Tinggi dan Sedang untuk menerima pemberitahuan dengan tingkat keparahan Tinggi dan Sedang.
5. Pilih Beri tahu saya tentang semua pembaruan wawasan, atau pilih Beri tahu saya saat wawasan dibuka atau ditutup, atau tingkat keparahan berubah dari Rendah atau Sedang ke Tinggi.
6. Pilih Simpan.

Izin ditambahkan ke topik Amazon SNS Anda

Topik Amazon SNS adalah sumber daya yang berisi kebijakan sumber daya AWS Identity and Access Management (IAM). Saat Anda menentukan topik di sini, DevOps Guru menambahkan izin berikut ke kebijakan sumber dayanya.

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

Izin ini diperlukan agar DevOps Guru mempublikasikan notifikasi menggunakan topik. Jika Anda memilih untuk tidak memiliki izin ini pada topik tersebut, Anda dapat menghapusnya dengan aman dan topik akan terus berfungsi seperti sebelum Anda memilihnya. Namun, jika izin yang ditambahkan ini dihapus, DevOps Guru tidak dapat menggunakan topik tersebut untuk menghasilkan notifikasi.

Memfilter notifikasi DevOps Guru Anda

Anda dapat memfilter notifikasi DevOps Guru Anda dengan the section called “Memperbarui konfigurasi notifikasi Amazon SNS” atau dengan menggunakan kebijakan filter langganan Amazon SNS.

Topik

- Memfilter notifikasi dengan kebijakan filter langganan Amazon SNS
- Contoh notifikasi Amazon SNS yang difilter untuk Amazon Guru DevOps

Memfilter notifikasi dengan kebijakan filter langganan Amazon SNS

Anda dapat membuat kebijakan filter langganan Amazon Simple Notification Service (Amazon SNS) untuk mengurangi jumlah notifikasi yang Anda terima dari Amazon Guru. DevOps

Gunakan kebijakan filter untuk menentukan jenis notifikasi yang Anda terima. Anda dapat memfilter pesan Amazon SNS Anda menggunakan kata kunci berikut.

- `NEW_INSIGHT`— Menerima pemberitahuan saat wawasan baru dibuat.
- `CLOSED_INSIGHT`— Menerima pemberitahuan saat wawasan yang ada ditutup.
- `NEW_RECOMMENDATION`— Menerima pemberitahuan ketika rekomendasi baru dibuat dari wawasan.
- `NEW_ASSOCIATION`— Menerima pemberitahuan ketika anomali baru terdeteksi dari wawasan.
- `CLOSED_ASSOCIATION`— Menerima pemberitahuan ketika anomali yang ada ditutup.
- `SEVERITY_UPGRADED`— Menerima pemberitahuan saat tingkat keparahan wawasan ditingkatkan

Untuk informasi tentang cara membuat kebijakan filter langganan Amazon SNS, lihat kebijakan filter langganan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Dalam kebijakan filter Anda, Anda menentukan salah satu kata kunci dengan kebijakan tersebut`MessageType`. Misalnya, berikut ini akan muncul di filter yang menentukan topik Amazon SNS hanya mengirimkan pemberitahuan ketika anomali baru terdeteksi dari wawasan.

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

Contoh notifikasi Amazon SNS yang difilter untuk Amazon Guru DevOps

Berikut ini adalah contoh notifikasi Amazon Simple Notification Service (Amazon SNS) dari topik Amazon SNS dengan kebijakan filter. `MessageType`Ini diatur ke`NEW_ASSOCIATION`, sehingga mengirimkan pemberitahuan hanya ketika anomali baru terdeteksi dari wawasan.

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

Memperbarui AWS Systems Manager integrasi di DevOps Guru

Anda dapat mengaktifkan pembuatan OpsItem untuk setiap wawasan baru di AWS Systems Manager OpsCenter. OpsCenter adalah sistem terpusat di mana Anda dapat melihat, menyelidiki, dan meninjau item pekerjaan operasional (OpsItems). The OpsItems for your insights dapat membantu Anda mengelola pekerjaan yang membahas perilaku anomali yang memicu penciptaan setiap wawasan. Untuk informasi selengkapnya, lihat AWS Systems Manager OpsCenterdan Bekerja dengan OpsItem di Panduan AWS Systems Manager Pengguna.

> **Note**
>
> Jika Anda mengubah kunci atau nilai bidang tag OpsItem, maka DevOps Guru tidak dapat memperbaruinya OpsItem. Misalnya, jika Anda mengubah tag OpsItem dari dari `"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` ke sesuatu yang lain, maka DevOps Guru tidak dapat memperbaruinya OpsItem.

Untuk mengelola integrasi Systems Manager

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Pilih Pengaturan di panel navigasi.
3. Dalam AWS Systems Manager integrasi, pilih Aktifkan DevOps Guru untuk membuat AWS OpstItem in OpsCenter untuk setiap wawasan yang OpsItem dibuat untuk setiap wawasan baru. Hapus pilihannya untuk berhenti OpsItem membuat untuk setiap wawasan baru.

Anda dikenakan biaya untuk OpsItems dibuat di akun Anda. Untuk informasi selengkapnya, lihat harga AWS Systems Manager.

Memperbarui deteksi anomali log di Guru DevOps

Untuk mengelola pengaturan deteksi anomali log

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Pilih Pengaturan di panel navigasi.
3. Dalam deteksi anomali Log, pilih Aktifkan deteksi anomali log dengan memberikan izin DevOps Guru untuk menampilkan data log yang terkait dengan wawasan. agar DevOps Guru menampilkan data log yang terkait dengan wawasan.

Memperbarui pengaturan enkripsi di DevOps Guru

Anda dapat memperbarui pengaturan enkripsi untuk menggunakan kunci yang AWS dimiliki atau kunci yang dikelola AWS KMS pelanggan. Saat beralih ke AWS KMS kunci terkelola pelanggan baru dari kunci terkelola pelanggan yang sudah ada, DevOps Guru secara otomatis mulai mengenkripsi metadata yang baru dicerna menggunakan AWS KMS kunci baru. Data historis akan tetap dienkripsi dengan kunci terkelola AWS KMS pelanggan yang dikonfigurasi sebelumnya.

> **Note**
>
> Jika Anda mencabut hibah, atau menonaktifkan atau menghapus AWS KMS kunci sebelumnya, DevOps Guru tidak akan dapat mengakses data apa pun yang dienkripsi oleh kunci ini dan Anda mungkin melihat `AccessDeniedException` saat melakukan operasi baca.

Untuk mengelola pengaturan enkripsi

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Pilih Pengaturan di panel navigasi.
3. Di bagian Enkripsi, pilih Edit enkripsi.

4. Pilih jenis encrpytion yang ingin Anda gunakan untuk melindungi data Anda. Anda dapat menggunakan kunci bawaan yang AWS dimiliki, memilih kunci terkelola pelanggan yang sudah ada, atau membuat AWS KMS kunci terkelola pelanggan baru.
5. Pilih Simpan.

Enkripsi adalah bagian penting dari keamanan DevOps Guru. Lihat informasi yang lebih lengkap di the section called “Perlindungan Data”.

Melihat notifikasi

Ada berbagai jenis notifikasi di DevOps Guru.

Topik

- Wawasan baru
- Wawasan tertutup
- Asosiasi baru
- Rekomendasi baru
- Tingkat keparahan ditingkatkan
- Kegagalan validasi sumber daya

Bagian pada halaman ini menunjukkan contoh dari setiap jenis notifikasi.

Wawasan baru

Pemberitahuan untuk wawasan baru berisi informasi berikut:


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

Wawasan tertutup

Pemberitahuan untuk wawasan tertutup berisi informasi berikut:

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

Asosiasi baru

Pemberitahuan untuk asosiasi baru berisi informasi berikut:

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

Rekomendasi baru

Pemberitahuan untuk rekomendasi baru berisi informasi berikut:

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

Tingkat keparahan ditingkatkan

Pemberitahuan untuk peningkatan tingkat keparahan berisi informasi berikut:

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

Kegagalan validasi sumber daya

Anda dapat menggunakan CloudFormation tumpukan dan AWS tag untuk memfilter dan mengidentifikasi AWS sumber daya yang ingin dianalisis DevOps Guru. Saat Anda memilih tumpukan atau tag yang tidak valid untuk DevOps Guru untuk mengidentifikasi sumber daya, DevOps Guru akan membuat `SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE` notifikasi. Ini dapat terjadi ketika tag atau nama tumpukan yang Anda tentukan tidak memiliki sumber daya yang terkait dengannya. Untuk mendapatkan hasil maksimal dari metode penyaringan DevOps Guru, pilih tumpukan dan tag yang memiliki sumber daya yang terkait dengannya.

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

Melihat sumber daya yang dianalisis oleh DevOps Guru

DevOpsGuru menyediakan daftar nama sumber daya dan batas aplikasi mereka di bawah analisis menggunakan `ListMonitoredResources` tindakan. Informasi ini dikumpulkan dari Amazon CloudWatch, AWS CloudTrail, dan AWS layanan lainnya menggunakan peran terkait layanan DevOps Guru.

Perhatikan bahwa meskipun pengguna tidak memiliki izin eksplisit untuk mengakses layanan lain seperti AWS Lambda atau Amazon RDS, DevOps Guru tetap menyediakan daftar sumber daya dari layanan tersebut selama `ListMonitoredResources` tindakan tersebut diizinkan. APIs

Topik

- Memperbarui cakupan AWS analisis Anda di DevOps Guru
- Menghapus tampilan sumber daya yang dianalisis untuk pengguna

Memperbarui cakupan AWS analisis Anda di DevOps Guru

Anda dapat memperbarui AWS sumber daya mana yang ada di analisis DevOps Guru akun Anda. Sumber daya yang dianalisis membentuk batas cakupan DevOps Guru Anda. Ketika Anda menentukan batas Anda, sumber daya Anda dikelompokkan dalam aplikasi. Anda memiliki empat opsi cakupan batas.

- Pilih agar DevOps Guru menganalisis semua sumber daya yang didukung di akun Anda. Semua sumber daya di akun Anda yang ada di tumpukan dikelompokkan ke dalam aplikasi. Jika Anda memiliki beberapa tumpukan di akun Anda, maka sumber daya di setiap tumpukan membuat aplikasi mereka sendiri. Jika ada sumber daya di akun Anda tidak dalam tumpukan, mereka dikelompokkan ke dalam aplikasi mereka sendiri.
- Tentukan sumber daya dengan memilih AWS CloudFormation tumpukan yang menentukan sumber daya tersebut. Jika Anda melakukan ini, DevOps Guru menganalisis setiap sumber daya yang ditentukan dalam tumpukan yang Anda pilih. Jika sumber daya di akun Anda tidak ditentukan oleh tumpukan yang Anda pilih, itu tidak dianalisis. Untuk informasi selengkapnya, lihat Bekerja dengan tumpukan di Panduan CloudFormation Pengguna danTentukan cakupan untuk DevOps Guru.
- Tentukan sumber daya dengan menggunakan AWS tag. DevOpsGuru menganalisis semua sumber daya di akun dan Wilayah Anda atau semua sumber daya yang berisi kunci tag yang Anda pilih. Sumber daya dikelompokkan berdasarkan nilai tag yang dipilih. Untuk informasi

selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

- Tentukan untuk tidak memiliki sumber daya yang dianalisis sehingga Anda berhenti menimbulkan biaya dari analisis sumber daya.

> **Note**
>
> Jika Anda memperbarui cakupan Anda untuk berhenti menganalisis sumber daya, Anda mungkin terus dikenakan biaya kecil jika Anda meninjau wawasan yang ada yang dihasilkan oleh DevOps Guru di masa lalu. Biaya ini terkait dengan panggilan API yang digunakan untuk mengambil dan menampilkan informasi wawasan. Untuk informasi selengkapnya, lihat harga Amazon DevOps Guru.

DevOpsGuru mendukung semua sumber daya yang terkait dengan layanan yang didukung. Untuk informasi selengkapnya tentang layanan dan sumber daya yang didukung, lihat harga Amazon DevOps Guru.

Untuk mengelola cakupan analisis DevOps Guru Anda

1. Buka konsol Amazon DevOps Guru di https://console.aws.amazon.com/devops-guru/.
2. Perluas sumber daya yang dianalisis di panel navigasi.
3. Pilih Edit.
4. Pilih salah satu opsi cakupan berikut.

   - Pilih Semua sumber daya akun jika Anda ingin DevOps Guru menganalisis semua sumber daya yang didukung di AWS akun dan Wilayah Anda. Jika Anda memilih opsi ini, AWS akun Anda adalah batas cakupan analisis sumber daya Anda. Semua sumber daya di setiap tumpukan di akun Anda dikelompokkan ke dalam aplikasi mereka sendiri. Sumber daya yang tersisa yang tidak ada dalam tumpukan dikelompokkan ke dalam aplikasi mereka sendiri.
   - Pilih CloudFormation tumpukan jika Anda ingin DevOps Guru menganalisis sumber daya yang ada di tumpukan yang Anda pilih, lalu pilih salah satu opsi berikut.
     - Semua sumber daya — Semua sumber daya yang ada di tumpukan di akun Anda dianalisis. Sumber daya di setiap tumpukan dikelompokkan ke dalam aplikasi mereka sendiri. Sumber daya apa pun di akun Anda yang tidak ada dalam tumpukan tidak dianalisis.

- Pilih tumpukan — Pilih tumpukan yang ingin dianalisis DevOps Guru. Sumber daya di setiap tumpukan yang Anda pilih dikelompokkan ke dalam aplikasi mereka sendiri. Anda dapat memasukkan nama tumpukan di Temukan tumpukan untuk menemukan tumpukan tertentu dengan cepat. Anda dapat memilih hingga 1.000 tumpukan.

  Untuk informasi selengkapnya, lihat Menggunakan CloudFormation tumpukan untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

- Pilih Tag jika Anda ingin DevOps Guru menganalisis semua sumber daya yang berisi tag yang Anda pilih. Pilih kunci, lalu pilih salah satu opsi berikut.
  - Semua sumber daya akun —Analisis semua sumber daya AWS di Wilayah dan akun saat ini. Sumber daya dengan kunci tag yang dipilih dikelompokkan berdasarkan nilai tag, jika ada. Sumber daya tanpa kunci tag ini dikelompokkan dan dianalisis secara terpisah.
  - Pilih nilai tag tertentu — Semua sumber daya yang berisi tag dengan kunci yang Anda pilih dianalisis. DevOpsGuru mengelompokkan sumber daya Anda ke dalam aplikasi berdasarkan nilai tag Anda.

  Untuk informasi selengkapnya, lihat Menggunakan tag untuk mengidentifikasi sumber daya dalam aplikasi DevOps Guru Anda.

- Pilih Tidak Ada jika Anda tidak ingin DevOps Guru menganalisis sumber daya apa pun. Opsi ini menonaktifkan DevOps Guru sehingga Anda berhenti menimbulkan biaya dari analisis sumber daya.

5. Pilih Simpan.

Menghapus tampilan sumber daya yang dianalisis untuk pengguna

Bahkan jika pengguna tidak memiliki izin eksplisit untuk mengakses layanan lain seperti Lambda atau Amazon RDS DevOps, Guru masih menyediakan daftar sumber daya dari layanan itu selama `ListMonitoredResources` tindakan diizinkan. APIs Untuk mengubah perilaku ini, Anda dapat memperbarui kebijakan AWS IAM untuk menolak tindakan ini.

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

Praktik terbaik di DevOps Guru

Praktik terbaik berikut dapat membantu Anda memahami, mendiagnosis, dan memperbaiki perilaku anomali yang terdeteksi oleh Amazon DevOps Guru. Gunakan praktik terbaik Memahami wawasan di konsol DevOps Guru untuk mengatasi masalah operasional yang terdeteksi oleh DevOps Guru.

- Dalam tampilan garis waktu wawasan, lihat metrik yang disorot terlebih dahulu. Mereka sering menjadi indikator utama masalah.
- Gunakan Amazon CloudWatch untuk melihat metrik yang terjadi tepat sebelum metrik pertama yang disorot dalam wawasan untuk menentukan kapan dan bagaimana perilaku berubah. Ini dapat membantu Anda mendiagnosis dan memperbaiki masalah.
- Untuk sumber daya Amazon RDS, lihat metrik Performance Insights. Dengan mengkorelasikan metrik penghitung dengan pemuatan basis data, Anda bisa mendapatkan informasi terperinci tentang masalah kinerja. Untuk informasi selengkapnya, lihat Menganalisis anomali kinerja dengan DevOps Gurufor Amazon RDS.
- Beberapa dimensi dari metrik yang sama seringkali bisa anomali. Lihatlah dimensi dalam tampilan grafik untuk mendapatkan pemahaman yang lebih dalam tentang masalah.
- Lihat di bagian peristiwa wawasan untuk penyebaran atau peristiwa infrastruktur yang terjadi sekitar waktu wawasan dibuat. Mengetahui peristiwa mana yang terjadi ketika perilaku anomali wawasan terjadi dapat membantu Anda memahami dan mendiagnosis masalah.
- Cari tiket di sistem operasional Anda yang terjadi sekitar waktu yang sama sebagai wawasan untuk petunjuk.
- Dalam wawasan, baca rekomendasi dan kunjungi tautan dalam rekomendasi. Ini sering memiliki langkah-langkah pemecahan masalah yang dapat membantu Anda mendiagnosis dan memecahkan masalah dengan cepat.
- Jangan abaikan wawasan yang diselesaikan kecuali Anda telah memecahkan masalah. Sekali sehari, lihat wawasan baru, bahkan jika mereka telah diselesaikan. Cobalah untuk memahami akar penyebab di balik sebanyak mungkin wawasan yang Anda bisa. Carilah pola yang mungkin menjadi tanda masalah sistemik. Jika masalah sistemik dibiarkan tidak terselesaikan, itu bisa menyebabkan masalah yang lebih serius di masa depan. Memperbaiki masalah sementara sekarang dapat membantu mencegah insiden masa depan yang lebih serius.

Keamanan di Amazon DevOps Guru

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud -- AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan AWS layanan di AWS Awan. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS Program Kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon DevOps Guru, lihat Layanan AWS dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan DevOps Guru. Topik berikut menunjukkan cara mengkonfigurasi DevOps Guru untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan DevOps Sumber daya Guru.

Topik

- Perlindungan data di Amazon DevOps Guru
- Manajemen Identitas dan Akses untuk Amazon DevOps Guru
- Pencatatan dan pemantauan DevOps Guru
- DevOps Guru dan antarmuka titik akhir VPC (AWS PrivateLink)
- Keamanan infrastruktur di DevOps Guru
- Ketahanan di Amazon DevOps Guru

Perlindungan data di Amazon DevOps Guru

The AWS model tanggung jawab bersama berlaku untuk perlindungan data di Amazon DevOps Guru. Seperti yang dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi DataKetentuan. Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami sarankan Anda melindungi Akun AWS kredensional dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (SEKARANG). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jalur untuk ditangkap AWS kegiatan, lihat Bekerja dengan CloudTrail jalan setapak di AWS CloudTrail Panduan Pengguna.
- Gunakan AWS solusi enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan DevOps Guru atau lainnya Layanan AWS menggunakan konsol, API, AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi data di DevOps Guru

Enkripsi adalah bagian penting dari DevOps Keamanan Guru. Beberapa enkripsi, seperti untuk data dalam transit, disediakan secara default dan Anda tidak perlu melakukan apa pun. Enkripsi lain, seperti untuk data at rest, Anda dapat mengonfigurasi ketika Anda membuat proyek atau build.

- Enkripsi data dalam transit: Semua komunikasi antara pelanggan dan DevOps Guru dan antara DevOps Guru dan dependensi hilirnya dilindungi menggunakan TLS dan diautentikasi menggunakan proses penandatanganan Signature Version 4. Semua DevOps Titik akhir Guru menggunakan sertifikat yang dikelola oleh AWS Private Certificate Authority. Untuk informasi selengkapnya, lihat Proses penandatanganan Signature Version 4 dan Tentang ACM PCA.
- Enkripsi data saat istirahat: Untuk semua AWS sumber daya dianalisis oleh DevOps Guru, Amazon CloudWatch metrik dan data, ID sumber daya, dan AWS CloudTrail peristiwa disimpan menggunakan Amazon S3, Amazon DynamoDB, dan Amazon Kinesis. Jika CloudFormation tumpukan digunakan untuk menentukan sumber daya yang dianalisis, kemudian data tumpukan juga dikumpulkan. DevOps Guru menggunakan kebijakan penyimpanan data Amazon S3, DynamoDB, dan Kinesis. Data yang disimpan di Kinesis dapat disimpan hingga satu tahun dan tergantung pada kebijakan yang ditetapkan. Data yang disimpan di Amazon S3 dan DynamoDB disimpan selama satu tahun.

  Data yang disimpan dienkripsi menggunakan kemampuan enkripsi data-at-rest dari Amazon S3, DynamoDB, dan Kinesis.

  Kunci yang dikelola pelanggan: DevOps Guru mendukung mengenkripsi konten pelanggan dan metadata sensitif seperti anomali log yang dihasilkan dari CloudWatch Log dengan kunci yang dikelola pelanggan. Fitur ini memberi Anda opsi untuk menambahkan lapisan keamanan yang dikelola sendiri untuk membantu Anda memenuhi persyaratan kepatuhan dan peraturan organisasi Anda. Untuk informasi tentang mengaktifkan kunci yang dikelola pelanggan di DevOps Pengaturan Guru, lihat the section called “Memperbarui enkripsi”.

  Karena Anda memiliki kontrol penuh atas lapisan enkripsi ini, Anda dapat melakukan tugas-tugas seperti:

  - Menetapkan dan memelihara kebijakan utama
  - Menetapkan dan memelihara kebijakan dan hibah IAM
  - Mengaktifkan dan menonaktifkan kebijakan utama

- Memutar materi kriptografi kunci
- Menambahkan tanda
- Membuat alias kunci
- Kunci penjadwalan untuk penghapusan

Untuk informasi lebih lanjut, lihat Kunci yang dikelola pelanggan di AWS Key Management Service Panduan Pengembang.

> **Note**
>
> DevOps Guru secara otomatis mengaktifkan enkripsi saat istirahat menggunakan AWS kunci yang dimiliki untuk melindungi metadata sensitif tanpa biaya. Namun, AWS KMS biaya berlaku untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat AWS Key Management Service harga.

Bagaimana DevOps Guru menggunakan hibah di AWS KMS

DevOps Guru membutuhkan hibah untuk menggunakan kunci yang dikelola pelanggan Anda.

Saat Anda memilih untuk mengaktifkan enkripsi dengan kunci yang dikelola pelanggan, DevOps Guru membuat hibah atas nama Anda dengan mengirimkan CreateGrant meminta untuk AWS KMS. Hibah di AWS KMS Digunakan untuk memberi DevOps Akses Guru ke a AWS KMS kunci di akun pelanggan.

DevOps Guru memerlukan hibah untuk menggunakan kunci yang dikelola pelanggan Anda untuk operasi internal berikut:

- Kirim DescribeKey permintaan untuk AWS KMS untuk memverifikasi bahwa ID kunci KMS yang dikelola pelanggan simetris yang dimasukkan saat membuat pelacak atau koleksi geofence valid.
- Kirim GenerateDataKey permintaan untuk AWS KMS untuk menghasilkan kunci data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.
- Kirim permintaan Decrypt ke AWS KMS untuk mendekripsi kunci data terenkripsi sehingga mereka dapat digunakan untuk mengenkripsi data Anda.

Anda dapat mencabut akses ke hibah, atau menghapus akses layanan ke kunci yang dikelola pelanggan kapan saja. Jika Anda melakukannya, DevOps Guru tidak akan dapat mengakses

data apa pun yang dienkripsi oleh kunci yang dikelola pelanggan, yang memengaruhi operasi yang bergantung pada data tersebut. Misalnya, jika Anda mencoba untuk mendapatkan informasi anomali log terenkripsi DevOps Guru tidak dapat mengakses, maka operasi akan mengembalikan AccessDeniedException kesalahan.

Memantau kunci enkripsi Anda di DevOps Guru

Ketika Anda menggunakan AWS KMS kunci yang dikelola pelanggan dengan Anda DevOps Sumber daya Guru, Anda dapat menggunakan AWS CloudTrail atau CloudWatch Log untuk melacak permintaan yang DevOps Guru mengirim ke AWS KMS.

Membuat kunci yang dikelola pelanggan

Anda dapat membuat kunci yang dikelola pelanggan simetris dengan menggunakan Konsol Manajemen AWS atau AWS KMS API.

Untuk membuat kunci yang dikelola pelanggan simetris, lihat Membuat kunci KMS enkripsi simetris.

Kebijakan kunci

Kebijakan utama mengontrol akses ke kunci yang dikelola pelanggan Anda. Setiap kunci yang dikelola pelanggan harus memiliki tepat satu kebijakan kunci, yang berisi pernyataan yang menentukan siapa yang dapat menggunakan kunci dan bagaimana mereka dapat menggunakannya. Saat membuat kunci yang dikelola pelanggan, Anda dapat menentukan kebijakan kunci. Untuk informasi lebih lanjut, lihat Otentikasi dan kontrol akses untuk AWS KMS di AWS Key Management Service Panduan Pengembang.

Untuk menggunakan kunci yang dikelola pelanggan dengan DevOps Sumber daya Guru, operasi API berikut harus diizinkan dalam kebijakan utama:

- `kms:CreateGrant` — Menambahkan hibah ke kunci yang dikelola pelanggan. Memberikan akses kontrol ke yang ditentukan AWS KMS kunci, yang memungkinkan akses ke operasi hibah DevOps Guru membutuhkan. Untuk informasi lebih lanjut tentang menggunakan hibah, lihat AWS Key Management Service Panduan Pengembang.

Hal ini memungkinkan DevOps Guru untuk melakukan hal berikut:

- Panggilan GenerateDataKey untuk menghasilkan kunci data terenkripsi dan menyimpannya, karena kunci data tidak segera digunakan untuk mengenkripsi.

- Panggil Decrypt untuk menggunakan kunci data terenkripsi yang disimpan untuk mengakses data terenkripsi.
- Siapkan prinsipal yang pensiun untuk memungkinkan layanan RetireGrant.
- Gunakan kms:DescribeKey untuk memberikan rincian kunci yang dikelola pelanggan untuk memungkinkan DevOps Guru untuk memvalidasi kunci.

Pernyataan berikut mencakup contoh pernyataan kebijakan yang dapat Anda tambahkan DevOps Guru:

```
"Statement" : [
  {
    "Sid" : "Allow access to principals authorized to use DevOps Guru",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [
      "kms:DescribeKey",
      "kms:CreateGrant"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "kms:ViaService" : "devops-guru.Region.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
  },
  {
    "Sid": "Allow access for key administrators",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:root"
     },
    "Action" : [
      "kms:*"
     ],
    "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
  },
  {
    "Sid" : "Allow read-only access to key metadata to the account",
    "Effect" : "Allow",
```

```
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

Privasi lalu lintas

Anda dapat meningkatkan keamanan analisis sumber daya dan pembuatan wawasan dengan mengonfigurasi DevOps Guru untuk menggunakan antarmuka titik akhir VPC. Untuk melakukan ini, Anda tidak memerlukan gateway internet, perangkat NAT, atau gateway pribadi virtual. Hal ini juga tidak diperlukan untuk mengkonfigurasi PrivateLink, meskipun dianjurkan. Untuk informasi selengkapnya, lihat DevOps Guru dan antarmuka titik akhir VPC (AWS PrivateLink). Untuk informasi lebih lanjut tentang PrivateLink dan titik akhir VPC, lihat AWS PrivateLink dan Mengakses layanan AWS melalui PrivateLink.

Manajemen Identitas dan Akses untuk Amazon DevOps Guru

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses dengan aman ke AWS sumber daya. Administrator IAM mengontrol siapa yang bisa mengonfirmasi (masuk) dan resmi (memiliki izin) untuk menggunakan DevOps Sumber daya Guru. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan Identitas
- Mengelola Akses menggunakan Kebijakan
- DevOps Guru memperbarui ke AWS kebijakan terkelola dan peran terkait layanan
- Bagaimana Amazon DevOps Guru bekerja dengan IAM
- Identity-based Kebijakan untuk Amazon DevOps Guru

- Menggunakan peran terkait layanan untuk DevOps Guru
- Amazon DevOps Referensi izin Guru
- Izin untuk topik Amazon SNS
- Izin untuk AWS KMS Topik Amazon SNS yang dienkripsi
- Pemecahan masalah Amazon DevOps Identitas dan akses guru

Audiens

Bagaimana Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan masalah Amazon DevOps Identitas dan akses guru)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana Amazon DevOps Guru bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based Kebijakan untuk Amazon DevOps Guru)

Mengautentikasi dengan Identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau Google/Facebook kredenSIAL. Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Ketika Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut Akun AWS pengguna root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat

menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas Terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredenSIAL sementara.

SEBUAH Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredenSIAL dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi lebih lanjut, lihat Memerlukan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredenSIAL sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan menelepon AWS CLI atau AWS Operasi API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola Akses menggunakan Kebijakan

Anda mengontrol akses di AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based Kebijakan bisa kebijakan sebaris (tertanam langsung ke dalam satu identitas) atau kebijakan yang dikelola (kebijakan mandiri yang melekat pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan sebaris yang terletak di layanan tersebut. Anda tidak dapat menggunakan AWS kebijakan yang dikelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis Kebijakan Lain

AWS mendukung jenis kebijakan tambahan yang dapat mengatur izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai Jenis Kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari caranya AWS menentukan apakah akan mengizinkan permintaan ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

DevOps Guru memperbarui ke AWS kebijakan terkelola dan peran terkait layanan

Lihat detail tentang pembaruan ke AWS kebijakan terkelola dan peran terkait layanan untuk DevOps Guru sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di DevOps Guru Amazon DevOps Sejarah dokumen Guru.

Ubah	Deskripsi	Date
AmazonDevOpsGuruConsoleFullAccess Memperbarui kebijakan yang ada.	`AmazonDevOpsGuruFullAccess` kebijakan terkelola sekarang mendukung langganan Amazon SNS.	9 Agustus 2023
AmazonDevOpsGuruReadOnlyAccess – Pembaruan ke kebijakan yang ada	`AmazonDevOpsGuruReadOnlyAccess` kebijakan terkelola sekarang mendukung akses baca-saja ke daftar langganan Amazon SNS.	9 Agustus 2023
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung akses ke tindakan GET API Gateway pada REST API.	11 Januari 2023
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung beberapa tindakan Layanan Penyimpanan Sederhana Amazon dan Kuota Layanan.	Oktober 19, 2022
AmazonDevOpsGuruFullAccess – Pembaruan ke kebijakan yang ada	Yang `AmazonDevOpsGuruFullAccess` kebijakan yang dikelola sekarang mendukung akses ke CloudWatch `FilterLogEvents` tindakan.	30 Agustus 2022
AmazonDevOpsGuruConsoleFullAccess – Pembaruan ke kebijakan yang ada	`AmazonDevOpsGuruConsoleFullAccess` kebijakan yang dikelola sekarang mendukung akses	30 Agustus 2022

Ubah	Deskripsi	Date
	ke CloudWatch `FilterLogEvents` tindakan.	
AmazonDevOpsGuruReadOnlyAccess – Pembaruan ke kebijakan yang ada	`AmazonDevOpsGuruReadOnlyAccess` kebijakan terkelola sekarang mendukung akses baca-saja ke CloudWatch `FilterLogEvents` tindakan.	30 Agustus 2022
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung CloudWatch mencatat tindakan `FilterLogEvents` , `DescribeLogGroups` , dan `DescribeLogStreams` .	12 Juli 2022
Identity-based kebijakan untuk DevOps Guru Kebijakan baru yang dikelola.	Yang `AmazonDevOpsGuruConsoleFullAccess` kebijakan telah ditambahkan.	Desember 16, 2021
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung Performance Insights `DescribeMetricsKeys` , dan Amazon RDS `DescribeDBInstances` tindakan.	1 Desember 2021

Ubah	Deskripsi	Date
AmazonDevOpsGuruReadOnlyAccess – Pembaruan ke kebijakan yang ada	Yang `AmazonDevOpsGuruReadOnlyAccess` kebijakan terkelola sekarang mendukung akses read-only ke Amazon RDS `DescribeDBInstances` tindakan.	1 Desember 2021
AmazonDevOpsGuruFullAccess – Pembaruan ke kebijakan yang ada	Yang `AmazonDevOpsGuruFullAccess` kebijakan terkelola sekarang mendukung akses ke Amazon RDS `DescribeDBInstances` tindakan.	1 Desember 2021
Identity-based Kebijakan untuk Amazon DevOps Guru Kebijakan baru ditambahkan.	Yang `AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung akses ke Amazon RDS `DescribeDBInstances` dan Wawasan Kinerja `GetResourceMetrics` tindakan. Yang `AmazonDevOpsGuruOrganizationsAccess` kebijakan yang dikelola menyediakan akses ke DevOps Guru dalam suatu organisasi.	November 16, 2021

Ubah	Deskripsi	Date
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang mendukung Organisasi AWS.	4 November 2021
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang berisi kondisi baru di `ssm:CreateOpsItem` dan `ssm:AddTagsToResource` tindakan.	11 Oktober 2021
Service-linked izin peran untuk DevOps Guru Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran terkait layanan sekarang berisi kondisi baru di `ssm:CreateOpsItem` dan `ssm:AddTagsToResource` tindakan.	14 Juni 2021
AmazonDevOpsGuruReadOnlyAccess – Pembaruan ke kebijakan yang ada	Yang `AmazonDevOpsGuruReadOnlyAccess` kebijakan terkelola sekarang memungkinkan akses baca-saja ke AWS Identity and Access Management `GetRole` dan DevOps Guru `DescribeFeedback` tindakan.	14 Juni 2021

Ubah	Deskripsi	Date
AmazonDevOpsGuruReadOnlyAccess – Pembaruan ke kebijakan yang ada	Yang `AmazonDevOpsGuruReadOnlyAccess` kebijakan terkelola sekarang memungkinkan akses baca-saja ke DevOps Guru `GetCostEstimation` dan `StartCostEstimation` tindakan.	27 April 2021
AmazonDevOpsGuruServiceRolePolicy Memperbarui kebijakan yang ada.	`AWSServiceRoleForDevOpsGuru` peran sekarang memungkinkan akses ke AWS Systems Manager `AddTagsToResource` dan Penskalaan Otomatis Amazon EC2 `DescribeAutoScalingGroups` tindakan.	27 April 2021
DevOps Guru mulai melacak perubahan	DevOps Guru mulai melacak perubahan untuknya AWS kebijakan yang dikelola.	10 Desember 2020

Bagaimana Amazon DevOps Guru bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke DevOps Guru, pelajari fitur IAM apa yang tersedia untuk digunakan DevOps Guru.

Fitur IAM yang dapat Anda gunakan dengan Amazon DevOps Guru

Fitur IAM	DevOps Dukungan Guru
Identity-based kebijakan	Ya

Fitur IAM	DevOps Dukungan Guru
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Ya

Untuk mendapatkan pandangan tingkat tinggi tentang bagaimana DevOps Guru dan lainnya AWS layanan bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk DevOps Guru

Mendukung kebijakan berbasis identitas: ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based Contoh kebijakan untuk DevOps Guru

Untuk melihat contoh DevOps Kebijakan berbasis identitas Guru, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.

Resource-based kebijakan di dalam DevOps Guru

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk DevOps Guru

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS Kebijakan JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar DevOps Tindakan Guru, lihat Tindakan yang ditentukan oleh Amazon DevOps Guru di Referensi Otorisasi Layanan.

Tindakan kebijakan di DevOps Guru menggunakan awalan berikut sebelum tindakan:

```
aws
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh DevOps Kebijakan berbasis identitas Guru, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.

Sumber daya kebijakan untuk DevOps Guru

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS Kebijakan JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar DevOps Jenis sumber daya Guru dan ARN-nya, lihat Sumber daya yang ditentukan oleh Amazon DevOps Guru di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana Anda dapat menentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh Amazon DevOps Guru.

Untuk melihat contoh DevOps Kebijakan berbasis identitas Guru, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.

Kunci kondisi kebijakan untuk DevOps Guru

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan AWS Kebijakan JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua AWS kunci kondisi global, lihat AWS kunci konteks kondisi global di Panduan Pengguna IAM.

Untuk melihat daftar DevOps Kunci kondisi Guru, lihat Kunci kondisi untuk Amazon DevOps Guru di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana Anda dapat menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Amazon DevOps Guru.

Untuk melihat contoh DevOps Kebijakan berbasis identitas Guru, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.

Daftar kontrol akses (ACL) di DevOps Guru

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses (ABAC) dengan DevOps Guru

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas IAM dan AWS sumber daya, lalu rancang kebijakan ABAC untuk memungkinkan operasi ketika tag kepala sekolah cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensional sementara dengan DevOps Guru

Mendukung kredensial sementara: Ya

KredenSIAL sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis membuat kredenSIAL sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Cross-service izin utama untuk DevOps Guru

Mendukung sesi akses terusan (FAS): Ya

Sesi akses teruskan (FAS) menggunakan izin dari kepala sekolah yang memanggil Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk DevOps Guru

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan mungkin rusak DevOps Fungsionalitas Guru. Edit peran layanan hanya bila DevOps Guru memberikan bimbingan untuk melakukannya.

Service-linked peran untuk DevOps Guru

Mendukung peran terkait layanan: ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke Layanan AWS. Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked Peran muncul di Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Temukan layanan di tabel yang mencakup `Yes` di Service-linked peran kolom. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based Kebijakan untuk Amazon DevOps Guru

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi DevOps Sumber daya Guru. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Buat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh DevOps Guru, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon DevOps Guru di Referensi Otorisasi Layanan.

Topik

- Praktik Terbaik Kebijakan
- Menggunakan DevOps Konsol Guru
- Mengizinkan pengguna melihat izin mereka sendiri
- Kebijakan AWS yang dikelola (telah ditentukan sebelumnya) untuk DevOps Guru

Praktik Terbaik Kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus DevOps Sumber daya Guru di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai dengan AWS kebijakan terkelola dan bergerak menuju izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan AWS kebijakan yang dikelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan mendefinisikan AWS kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang membutuhkan pengguna IAM atau pengguna root di Anda Akun AWS, nyalakan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan DevOps Konsol Guru

Untuk mengakses Amazon DevOps Konsol Guru, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang DevOps Sumber daya Guru di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan DevOps Konsol Guru, pasang juga DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` atau `AmazonDevOpsGuruFullAccess` AWS kebijakan yang dikelola untuk entitas. Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan AWS CLI atau AWS API.

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

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

Kebijakan AWS yang dikelola (telah ditentukan sebelumnya) untuk DevOps Guru

AWS mengatasi banyak kasus penggunaan umum dengan menyediakan kebijakan IAM mandiri yang dibuat dan dikelola oleh AWS. Ini AWS-kebijakan yang dikelola memberikan izin yang diperlukan untuk kasus penggunaan umum sehingga Anda dapat menghindari keharusan menyelidiki izin apa yang diperlukan. Untuk informasi selengkapnya, lihat Kebijakan yang Dikelola AWS dalam Panduan Pengguna IAM.

Untuk membuat dan mengelola DevOps Peran layanan Guru, Anda juga harus melampirkan AWS-kebijakan yang dikelola bernama `IAMFullAccess`.

Anda juga dapat membuat kebijakan IAM kustom Anda sendiri untuk mengizinkan izin DevOps Tindakan dan sumber daya guru. Anda dapat menyematkan kebijakan khusus ini untuk pengguna atau grup yang memerlukan izin tersebut.

Berikut ini AWS-kebijakan terkelola, yang dapat Anda lampirkan ke pengguna di akun Anda, khusus untuk DevOps Guru.

Topik

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

`AmazonDevOpsGuruFullAccess` - Menyediakan akses penuh ke DevOps Guru, termasuk izin untuk membuat topik Amazon SNS, mengakses Amazon CloudWatch metrik, dan akses AWS CloudFormation tumpukan. Terapkan ini hanya untuk pengguna tingkat administratif yang ingin Anda berikan kontrol penuh DevOps Guru.

`AmazonDevOpsGuruFullAccess` kebijakan berisi pernyataan berikut.

JSON

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

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

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

AmazonDevOpsGuruConsoleFullAccess

`AmazonDevOpsGuruConsoleFullAccess` - Menyediakan akses penuh ke DevOps Guru, termasuk izin untuk membuat topik Amazon SNS, mengakses Amazon CloudWatch metrik, dan akses AWS CloudFormation tumpukan. Kebijakan ini memiliki izin wawasan kinerja tambahan sehingga Anda dapat melihat analisis terperinci terkait instans Amazon RDS Aurora DB yang tidak normal di konsol. Terapkan ini hanya untuk pengguna tingkat administratif yang ingin Anda berikan kontrol penuh DevOps Guru.

`AmazonDevOpsGuruConsoleFullAccess` kebijakan berisi pernyataan berikut.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
```

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

```
            "StringEquals": {
                "aws:ResourceTag/DevOps-Guru-Analysis": "true"
            }
        }
    }
  ]
}
```

AmazonDevOpsGuruReadOnlyAccess

`AmazonDevOpsGuruReadOnlyAccess` — Memberikan akses baca-saja ke DevOps Guru dan sumber daya terkait di lainnya AWS layanan. Terapkan kebijakan ini ke pengguna yang ingin Anda berikan kemampuan untuk melihat wawasan, tetapi tidak untuk membuat pembaruan apa pun DevOps Batas cakupan analisis Guru, topik Amazon SNS, atau Manajer Sistem OpsCenter integrasi.

`AmazonDevOpsGuruReadOnlyAccess` kebijakan berisi pernyataan berikut.

JSON

```
{
"Version":"2012-10-17",
"Statement": [
    {
        "Sid": "DevOpsGuruReadOnlyAccess",
        "Effect": "Allow",
        "Action": [
            "devops-guru:DescribeAccountHealth",
            "devops-guru:DescribeAccountOverview",
            "devops-guru:DescribeAnomaly",
            "devops-guru:DescribeEventSourcesConfig",
            "devops-guru:DescribeFeedback",
            "devops-guru:DescribeInsight",
            "devops-guru:DescribeResourceCollectionHealth",
            "devops-guru:DescribeServiceIntegration",
            "devops-guru:GetCostEstimation",
            "devops-guru:GetResourceCollection",
            "devops-guru:ListAnomaliesForInsight",
            "devops-guru:ListEvents",
            "devops-guru:ListInsights",
            "devops-guru:ListAnomalousLogGroups",
```

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

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

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess` - Menyediakan akses administrator Organisasi ke DevOps Tampilan multi-akun Guru dalam organisasi. Terapkan kebijakan ini ke pengguna tingkat administrator organisasi Anda yang ingin Anda berikan akses penuh DevOps Guru dalam suatu organisasi. Anda dapat menerapkan kebijakan ini di akun manajemen organisasi Anda dan akun administrator yang didelegasikan untuk DevOps Guru. Anda bisa melamar `AmazonDevOpsGuruReadOnlyAccess` atau `AmazonDevOpsGuruFullAccess` selain kebijakan ini untuk menyediakan akses baca-saja atau penuh ke DevOps Guru.

`AmazonDevOpsGuruOrganizationsAccess` kebijakan berisi pernyataan berikut.

Menggunakan peran terkait layanan untuk DevOps Guru

Amazon DevOps Guru menggunakan AWS Identity and Access Management (SUDAH) peran terkait layanan. Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke DevOps Guru. Service-linked peran telah ditentukan oleh DevOps Guru dan sertakan semua izin yang diperlukan layanan untuk menelepon AWS CloudTrail, Amazon CloudWatch, AWS CodeDeploy, AWS X-Ray, dan Organisasi AWS atas nama Anda.

Peran terkait layanan membuat pengaturan DevOps Guru lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. DevOps Guru mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya DevOps Guru dapat mengambil perannya. Izin-izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah terlebih dahulu menghapus sumber dayanya yang terkait. Ini melindungi Anda DevOps Sumber daya Guru karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Service-linked izin peran untuk DevOps Guru

DevOps Guru menggunakan peran terkait layanan bernama `AWSServiceRoleForDevOpsGuru`. Ini adalah AWS kebijakan terkelola dengan izin cakupan yang DevOps Guru harus berjalan di akun Anda.

Peran terkait layanan `AWSServiceRoleForDevOpsGuru` memercayai layanan berikut untuk mengambil peran tersebut:

- `devops-guru.amazonaws.com`

Kebijakan izin peran, `AmazonDevOpsGuruServiceRolePolicy` memungkinkan DevOps Guru untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan.

JSON

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

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

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

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

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

Membuat peran terkait layanan untuk DevOps Guru

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda membuat wawasan dalam Konsol Manajemen AWS, AWS CLI, atau AWS API, DevOps Guru menciptakan peran terkait layanan untuk Anda.

> **Important**
>
> Peran terkait layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang didukung oleh peran ini; misalnya, peran tersebut dapat muncul jika Anda menambahkan DevOps Guru ke repositori dari AWS CodeCommit.

Mengedit peran terkait layanan untuk DevOps Guru

DevOps Guru tidak mengizinkan Anda untuk mengedit `AWSServiceRoleForDevOpsGuru` peran terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit a Service-Linked Peran di Panduan Pengguna IAM.

Menghapus peran yang ditautkan layanan untuk DevOps Guru

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak perlu lagi memantau atau memelihara entitas yang tidak digunakan. Namun, Anda harus memutuskan hubungan dari semua repositori sebelum Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika DevOps Layanan Guru menggunakan peran ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus `AWSServiceRoleForDevOpsGuru` peran terkait layanan. Untuk informasi lebih lanjut, lihat Menghapus a Service-Linked Peran di Panduan Pengguna IAM.

Amazon DevOps Referensi izin Guru

Anda dapat menggunakan AWS-kunci kondisi lebar di Anda DevOps Kebijakan Guru untuk mengekspresikan kondisi. Untuk daftarnya, lihat IAM JSON Policy Elements Reference dalam Panduan Pengguna IAM.

Anda menentukan tindakan di bidang `Action` kebijakan. Untuk menentukan tindakan, gunakan prefiks `devops-guru:` diikuti dengan nama operasi API (misalnya `devops-`

`guru:SearchInsights` dan `devops-guru:ListAnomalies`). Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma (misalnya, `"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`).

Menggunakan karakter wildcard

Anda menentukan Nama Sumber Daya Amazon (ARN), dengan atau tanpa karakter wildcard (*), sebagai nilai sumber daya di kebijakan `Resource` bidang. Anda dapat menggunakan wildcard untuk menentukan beberapa tindakan atau sumber daya. Sebagai contoh, `devops-guru:*` menentukan semua DevOps Tindakan Guru dan `devops-guru:List*` menentukan semua DevOps Tindakan Guru yang dimulai dengan kata `List`. Contoh berikut mengacu pada semua wawasan dengan pengidentifikasi unik universal (UUID) yang dimulai dengan `12345`.

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

Anda dapat menggunakan tabel berikut sebagai referensi ketika menyiapkan Mengautentikasi dengan Identitas dan menulis kebijakan izin yang dapat Anda lampirkan ke identitas IAM (kebijakan berbasis identitas).

DevOps Operasi API Guru dan izin yang diperlukan untuk tindakan

`AddNotificationChannel`

Tindakan: `devops-guru:AddNotificationChannel`

Diperlukan untuk menambahkan saluran notifikasi dari DevOps Guru. Saluran notifikasi digunakan untuk memberi tahu Anda kapan DevOps Guru menghasilkan wawasan yang berisi informasi tentang cara meningkatkan operasi Anda.

Sumber daya: *

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

Diperlukan untuk menghapus saluran notifikasi dari DevOps Guru. Saluran notifikasi digunakan untuk memberi tahu Anda kapan DevOps Guru menghasilkan wawasan yang berisi informasi tentang cara meningkatkan operasi Anda.

Sumber daya: *

`ListNotificationChannels`

Tindakan: `devops-guru:ListNotificationChannels`

Diperlukan untuk mengembalikan daftar saluran notifikasi yang dikonfigurasi untuk DevOps Guru. Setiap saluran notifikasi digunakan untuk memberi tahu Anda kapan DevOps Guru menghasilkan wawasan yang berisi informasi tentang cara meningkatkan operasi Anda. Salah satu jenis notifikasi yang didukung adalah Amazon Simple Notification Service.

Sumber daya: *

`UpdateResourceCollectionFilter`

Tindakan: `devops-guru:UpdateResourceCollectionFilter`

Diperlukan untuk memperbarui daftar CloudFormation tumpukan yang digunakan untuk menentukan mana AWS sumber daya di akun Anda dianalisis oleh DevOps Guru. Analisis menghasilkan wawasan yang mencakup rekomendasi, metrik operasional, dan peristiwa operasional yang dapat Anda gunakan untuk meningkatkan kinerja operasi Anda. Metode ini juga membuat peran IAM yang diperlukan untuk Anda gunakan CodeGuru OpsAdvisor.

Sumber daya: *

`GetResourceCollectionFilter`

Tindakan: `devops-guru:GetResourceCollectionFilter`

Diperlukan untuk mengembalikan daftar AWS CloudFormation tumpukan yang digunakan untuk menentukan mana AWS sumber daya di akun Anda dianalisis oleh DevOps Guru. Analisis menghasilkan wawasan yang mencakup rekomendasi, metrik operasional, dan peristiwa operasional yang dapat Anda gunakan untuk meningkatkan kinerja operasi Anda.

Sumber daya: *

`ListInsights`

Tindakan: `devops-guru:ListInsights`

Diperlukan untuk mengembalikan daftar wawasan di AWS akun. Anda dapat menentukan wawasan mana yang dikembalikan berdasarkan waktu mulai, status (`ongoing` atau `any`), dan ketik (`reactive` atau `predictive`).

Sumber daya: *

`DescribeInsight`

Aksi: `devops-guru:DescribeInsight`

Diperlukan untuk mengembalikan detail tentang wawasan yang Anda tentukan menggunakan ID-nya.

Sumber daya: *

`SearchInsights`

Aksi: `devops-guru:SearchInsights`

Diperlukan untuk mengembalikan daftar wawasan di AWS akun. Anda dapat menentukan wawasan mana yang dikembalikan berdasarkan waktu mulai, filter, dan jenisnya (`reactive` atau `predictive`).

Sumber daya: *

`ListAnomalies`

Aksi: `devops-guru:ListAnomalies`

Diperlukan untuk mengembalikan daftar anomali yang termasuk dalam wawasan yang Anda tentukan menggunakan ID-nya.

Sumber daya: *

`DescribeAnomaly`

Aksi: `devops-guru:DescribeAnomaly`

Diperlukan untuk mengembalikan detail tentang anomali yang Anda tentukan menggunakan ID-nya.

Sumber daya: *

`ListEvents`

Aksi: `devops-guru:ListEvents`

Diperlukan untuk mengembalikan daftar peristiwa yang dipancarkan oleh sumber daya yang dievaluasi oleh DevOps Guru. Anda dapat menggunakan filter untuk menentukan peristiwa mana yang dikembalikan.

Sumber daya: *

`ListRecommendations`

Aksi: `devops-guru:ListRecommendations`

Diperlukan untuk mengembalikan daftar rekomendasi wawasan tertentu. Setiap rekomendasi menyertakan daftar metrik dan daftar peristiwa yang terkait dengan rekomendasi.

Sumber daya: *

`DescribeAccountHealth`

Aksi: `devops-guru:DescribeAccountHealth`

Diperlukan untuk mengembalikan jumlah wawasan reaktif terbuka, jumlah wawasan prediktif terbuka, dan jumlah metrik yang dianalisis di AWS akun. Gunakan angka-angka ini untuk mengukur kesehatan operasi di Anda AWS akun.

Sumber daya: *

`DescribeAccountOverview`

Aksi: `devops-guru:DescribeAccountOverview`

Diperlukan untuk mengembalikan hal-hal berikut yang terjadi selama rentang waktu: jumlah wawasan reaktif terbuka yang dibuat, jumlah wawasan prediktif terbuka yang dibuat, dan waktu rata-rata pemulihan (MTTR) untuk semua wawasan reaktif yang ditutup.

Sumber daya: *

`DescribeResourceCollectionHealthOverview`

Aksi: `devops-guru:DescribeResourceCollectionHealthOverview`

Diperlukan untuk mengembalikan jumlah wawasan prediktif terbuka, wawasan reaktif terbuka, dan waktu rata-rata pemulihan (MTTR) untuk semua wawasan untuk masing-masing CloudFormation tumpukan ditentukan dalam DevOps Guru.

Sumber daya: *

`DescribeIntegratedService`

Aksi: `devops-guru:DescribeIntegratedService`

Diperlukan untuk mengembalikan status integrasi layanan yang dapat diintegrasikan dengan DevOps Guru. Satu layanan yang dapat diintegrasikan dengan DevOps Guru adalah AWS Systems Manager, yang dapat digunakan untuk membuat OpsItem untuk setiap wawasan yang dihasilkan.

Sumber daya: *

`UpdateIntegratedServiceConfig`

Aksi: `devops-guru:UpdateIntegratedServiceConfig`

Diperlukan untuk mengaktifkan atau menonaktifkan integrasi dengan layanan yang dapat diintegrasikan DevOps Guru. Satu layanan yang dapat diintegrasikan dengan DevOps Guru adalah Manajer Sistem, yang dapat digunakan untuk membuat OpsItem untuk setiap wawasan yang dihasilkan.

Sumber daya: *

Izin untuk topik Amazon SNS

Gunakan informasi dalam topik ini hanya jika Anda ingin mengonfigurasi Amazon DevOps Guru mengirimkan notifikasi ke topik Amazon SNS yang dimiliki oleh orang lain AWS akun.

Untuk DevOps Guru untuk mengirimkan pemberitahuan ke topik Amazon SNS yang dimiliki oleh akun lain, Anda harus melampirkan kebijakan ke topik Amazon SNS yang memberikan DevOps Izin Guru untuk mengirim pemberitahuan ke sana. Jika Anda mengkonfigurasi DevOps Guru untuk mengirimkan notifikasi ke topik Amazon SNS yang dimiliki oleh akun yang sama dengan yang Anda gunakan DevOps Guru, maka DevOps Guru menambahkan kebijakan ke topik untuk Anda.

Setelah melampirkan kebijakan untuk mengonfigurasi izin untuk topik Amazon SNS di akun lain, Anda dapat menambahkan topik Amazon SNS di DevOps Guru. Anda juga dapat memperbarui kebijakan Amazon SNS Anda dengan saluran notifikasi untuk membuatnya lebih aman.

> **Note**
>
> DevOps Guru saat ini hanya mendukung akses lintas akun di Wilayah yang sama.

Topik

- Mengkonfigurasi izin untuk topik Amazon SNS di akun lain
- Menambahkan topik Amazon SNS dari akun lain
- Memperbarui kebijakan Amazon SNS Anda dengan saluran notifikasi (disarankan)

Mengkonfigurasi izin untuk topik Amazon SNS di akun lain

Menambahkan izin sebagai peran IAM

Untuk menggunakan topik Amazon SNS dari akun lain setelah masuk dengan peran IAM, Anda harus melampirkan kebijakan ke topik Amazon SNS yang ingin Anda gunakan. Untuk melampirkan kebijakan ke topik Amazon SNS dari akun lain saat menggunakan peran IAM, Anda harus memiliki izin berikut untuk sumber daya akun tersebut sebagai bagian dari peran IAM Anda:

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

Lampirkan kebijakan berikut ke topik Amazon SNS yang ingin Anda gunakan. Untuk `Resource` kunci, *`topic-owner-account-id`* adalah ID akun pemilik topik, *`topic-sender-account-id`* adalah ID akun pengguna yang mengatur DevOps Guru, dan *`devops-guru-role`* adalah peran IAM dari pengguna individu yang terlibat. Anda harus mengganti nilai yang sesuai untuk *`region-id`* (contohnya, `us-west-2`), dan *`my-topic-name`*.

Menambahkan izin sebagai pengguna IAM

Untuk menggunakan topik Amazon SNS dari akun lain sebagai pengguna IAM, lampirkan kebijakan berikut ke topik Amazon SNS yang ingin Anda gunakan. Untuk `Resource` kunci, *`topic-owner-account-id`* adalah ID akun pemilik topik, *`topic-sender-account-id`* adalah ID akun pengguna yang mengatur DevOps Guru, dan *`devops-guru-user-name`* adalah pengguna IAM individu yang terlibat. Anda harus mengganti nilai yang sesuai untuk *`region-id`* (contohnya, `us-west-2`) dan *`my-topic-name`*.

> **Note**
>
> Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi

dan kunci akses. Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menambahkan topik Amazon SNS dari akun lain

Setelah mengonfigurasi izin untuk topik Amazon SNS di akun lain, Anda dapat menambahkan topik Amazon SNS tersebut ke DevOps Pengaturan pemberitahuan Guru. Anda dapat menambahkan topik Amazon SNS menggunakan AWS CLI atau DevOps Konsol Guru.

- Saat Anda menggunakan konsol, Anda harus memilih opsi Menggunakan topik SNS ARN untuk menentukan topik yang ada untuk menggunakan topik dari akun lain.
- Saat Anda menggunakan AWS CLI operasi tambahkan saluran notifikasi, Anda harus menentukan `TopicArn` di dalam `NotificationChannelConfig` objek.

Tambahkan topik Amazon SNS dari akun lain menggunakan konsol

1. Buka Amazon DevOps Konsol Guru di https://console.aws.amazon.com/devops-guru/.
2. Buka panel navigasi, lalu pilih Pengaturan.
3. Pergi ke Pemberitahuan bagian dan pilih Sunting.
4. Memilih Tambahkan topik SNS.
5. Memilih Menggunakan topik SNS ARN untuk menentukan topik yang ada.
6. Masukkan ARN topik Amazon SNS yang ingin Anda gunakan. Anda seharusnya sudah mengonfigurasi izin untuk topik ini dengan melampirkan kebijakan ke topik ini.
7. (Opsional) Pilih Konfigurasi notifikasi untuk mengedit pengaturan frekuensi notifikasi.
8. Pilih Simpan.

Setelah menambahkan topik Amazon SNS ke pengaturan notifikasi, DevOps Guru menggunakan topik itu untuk memberi tahu Anda tentang peristiwa penting, seperti ketika wawasan baru dibuat.

Memperbarui kebijakan Amazon SNS Anda dengan saluran notifikasi (disarankan)

Setelah menambahkan topik, sebaiknya Anda membuat kebijakan Anda lebih aman dengan menetapkan izin hanya untuk DevOps Saluran notifikasi Guru yang berisi topik Anda.

Perbarui kebijakan topik Amazon SNS Anda dengan saluran notifikasi (disarankan)

1. Jalankan `list-notification-channels` DevOps Guru AWS CLI perintah di akun Anda tempat Anda ingin mengirim notifikasi.

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

2. Dalam `list-notification-channels` respon, catat ID saluran yang berisi ARN topik Amazon SNS Anda. ID saluran adalah panduan.

   Misalnya, dalam respons berikut, ID saluran untuk topik dengan ARN `arn:aws:sns:`*`region-id`*`:`*`111122223333`*`:`*`topic-name`* adalah *`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. Buka kebijakan yang Anda buat di akun lain menggunakan ID pemilik topik di the section called “Mengkonfigurasi izin untuk topik Amazon SNS di akun lain”. Di `Condition` pernyataan kebijakan, tambahkan baris yang menentukan `SourceArn`. ARN berisi ID Wilayah Anda (misalnya, `us-east-1`), itu AWS nomor akun pengirim topik, dan ID saluran yang Anda catat.

   Anda diperbarui `Condition` pernyataan terlihat seperti berikut ini.

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

```
    }
  }
```

Jika `AddNotificationChannel` tidak dapat menambahkan Topik SNS Anda, periksa apakah kebijakan IAM Anda memiliki izin berikut.

Izin untuk AWS KMS Topik Amazon SNS yang dienkripsi

Topik Amazon SNS yang Anda tentukan mungkin dienkripsi oleh AWS Key Management Service. Untuk mengizinkan DevOps Guru untuk bekerja dengan topik terenkripsi, Anda harus terlebih dahulu membuat AWS KMS key dan kemudian tambahkan pernyataan berikut ke kebijakan kunci KMS. Untuk informasi lebih lanjut, lihat Mengenkripsi pesan yang dipublikasikan ke Amazon SNS dengan AWS KMS, Pengidentifikasi kunci (KeyId) di AWS KMS Panduan Pengguna, dan Enkripsi data di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> DevOps Guru saat ini mendukung topik terenkripsi untuk digunakan dalam satu akun. Menggunakan topik terenkripsi di beberapa akun tidak didukung saat ini.

Pemecahan masalah Amazon DevOps Identitas dan akses guru

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan DevOps Guru dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di DevOps Guru
- Saya ingin memberi pengguna akses terprogram
- Saya tidak berwenang untuk melakukan iam:PassRole
- Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses saya DevOps Sumber daya Guru

Saya tidak berwenang untuk melakukan tindakan di DevOps Guru

Jika Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang fiksi *`my-example-widget`* sumber daya tetapi tidak memiliki fiksi `aws:`*`GetWidget`* izin.

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

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `aws:`*`GetWidget`*.

Saya ingin memberi pengguna akses terprogram

Pengguna memerlukan akses terprogram jika mereka ingin berinteraksi AWS di luar Konsol Manajemen AWS. Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredenSIAL konsol sebagai kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Login untuk AWS pembangun an lokal di AWS Command Line Interface Panduan Pengguna. • Untuk AWS SDK, lihat Login untuk AWS pembangun

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		an lokal di AWS Panduan Referensi SDK dan Alat.
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi AWS CLI untuk menggunakan AWS IAM Identity Center di AWS Command Line Interface Panduan Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat Otentikasi Pusat Identitas IAM di AWS Panduan Referensi SDK dan Alat.
IAM	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti instruksi di Menggunakan kredenSIAL sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredenSIAL jangka panjang untuk menandata ngani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengotentikasi menggunakan kredentif pengguna IAM di AWS Command Line Interface Panduan Pengguna. • Untuk AWS SDK dan alat, lihat Otentikasi menggunakan kredensional jangka panjang di AWS Panduan Referensi SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Saya tidak berwenang untuk melakukan iam:PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui untuk memungkinkan Anda meneruskan peran DevOps Guru.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di DevOps Guru. Namun, tindakan tersebut memerlukan

layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

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

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda membutuhkan bantuan, hubungi AWS administrator. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya AWS akun untuk mengakses saya DevOps Sumber daya Guru

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah DevOps Guru mendukung fitur-fitur ini, lihat Bagaimana Amazon DevOps Guru bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di yang lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses ke Akun AWS dimiliki oleh pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Pencatatan dan pemantauan DevOps Guru

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja DevOps Guru dan solusi AWS Anda yang lain. AWS menyediakan alat pemantauan berikut untuk ditonton DevOps Guru, laporkan ketika ada sesuatu yang salah, dan ambil tindakan otomatis jika sesuai:

- Amazon CloudWatch memonitor Anda AWS sumber daya dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat memiliki CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi lebih lanjut, lihat Amazon CloudWatch Panduan Pengguna.
- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dilakukan oleh atau atas nama Anda AWS akun dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

- Pemantauan DevOps Guru dengan Amazon CloudWatch
- Pencatatan Amazon DevOps Panggilan API Guru dengan AWS CloudTrail

Pemantauan DevOps Guru dengan Amazon CloudWatch

Anda dapat memantau DevOps Guru menggunakan CloudWatch, yang mengumpulkan data mentah dan memprosesnya menjadi metrik yang dapat dibaca dan hampir real-time. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang performa aplikasi atau layanan web Anda. Anda juga dapat mengatur alarm yang mengawasi ambang batas tertentu dan mengirim pemberitahuan atau mengambil tindakan ketika ambang batas tersebut terpenuhi. Untuk informasi lebih lanjut, lihat Amazon CloudWatch Panduan Pengguna.

Untuk DevOps Guru, Anda dapat melacak metrik untuk wawasan dan metrik untuk Anda DevOps Penggunaan Guru. Anda mungkin ingin menonton sejumlah besar yang dibuat `Insights` untuk

membantu Anda menentukan apakah solusi operasional Anda mengalami perilaku anomali. Atau Anda mungkin ingin menonton DevOps Penggunaan Guru untuk membantu melacak biaya Anda.

Yang DevOps Layanan Guru melaporkan metrik berikut di `AWS/DevOps-Guru` ruang nama.

Topik

- Metrik wawasan
- DevOps Metrik penggunaan Guru

Metrik wawasan

Anda dapat menggunakan CloudWatch untuk melacak metrik untuk menunjukkan berapa banyak wawasan yang dibuat di AWS akun. Anda dapat menentukan `Type` dimensi untuk dilacak `proactive` atau `reactive` wawasan. Jangan tentukan dimensi jika Anda ingin melacak semua wawasan.

Metrik-metrik

Metrik	Deskripsi
`Insight`	Jumlah wawasan yang dibuat dalam AWS akun. Dimensi yang valid: `Type` Statistik yang valid: Jumlah sampel, Jumlah Unit: Hitungan

Dimensi berikut didukung untuk DevOps Guru `Insight` metrik.

Dimensi

Dimensi	Deskripsi
`Type`	Ini adalah jenis wawasan. Jangan menentukan dimensi untuk `Insights` metrik jika Anda ingin melacak semua wawasan. Nilai yang valid adalah: `proactive` , `reactive`.

DevOps Metrik penggunaan Guru

Anda dapat menggunakan CloudWatch untuk melacak Amazon Anda DevOps Penggunaan Guru.

Metrik-metrik

Metrik	Deskripsi
`CallCount`	Jumlah panggilan yang dilakukan oleh salah satu dari berikut DevOps Metode Guru. • `ListInsights` • `ListAnomaliesForInsight` • `ListRecommendations` • `ListEvents` • `SearchInsights` • `DescribeInsight` • `DescribeAnomaly` Dimensi yang valid: `Service`, `Class`, `Type`, `Resource` Statistik yang valid: Jumlah sampel, Jumlah Unit: Hitungan

Dimensi berikut didukung untuk DevOps Metrik penggunaan Guru.

Dimensi

Dimensi	Deskripsi

Dimensi	Deskripsi
`Service`	Ini adalah nama layanan AWS yang berisi sumber daya. Misalnya, untuk DevOps Guru, nilai ini `DevOps-Guru` .
`Class`	Ini adalah kelas sumber daya yang dilacak. DevOps Guru menggunakan dimensi ini dengan nilai `None`.
`Type`	Ini adalah jenis sumber daya yang dilacak. DevOps Guru menggunakan dimensi ini dengan nilai `API`.
`Resource`	Ini adalah nama DevOps Operasi Guru. Nilai yang valid adalah: `ListInsights` , `ListAnomaliesForInsight` , `ListRecommendations` , `ListEvents` , `SearchInsights` , `DescribeInsight` , `DescribeAnomaly` .

Pencatatan Amazon DevOps Panggilan API Guru dengan AWS CloudTrail

Amazon DevOps Guru terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di DevOps Guru. CloudTrail menangkap panggilan API untuk DevOps Guru sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari DevOps Konsol Guru dan panggilan kode ke DevOps Operasi API Guru. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan CloudTrail acara ke bucket Amazon S3, termasuk acara untuk DevOps Guru. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol masuk Sejarah acara. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk DevOps Guru, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan itu dibuat, dan detail tambahan.

Untuk mempelajari lebih lanjut tentang CloudTrail, lihat AWS CloudTrail Panduan Pengguna.

DevOps Informasi Guru di CloudTrail

CloudTrail diaktifkan pada Anda AWS akun saat Anda membuat akun. Ketika aktivitas terjadi di DevOps Guru, aktivitas itu dicatat dalam CloudTrail Acara bersama dengan lainnya AWS acara layanan di Sejarah acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun. Untuk informasi lebih lanjut, lihat Melihat acara dengan CloudTrail Sejarah acara.

Untuk catatan peristiwa yang berkelanjutan di Anda AWS akun, termasuk acara untuk DevOps Guru, buat jejak. SEBUAH jejak menyalakan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak di konsol tersebut, jejak tersebut diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengkonfigurasi lainnya AWS layanan untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima CloudTrail file log dari beberapa wilayah dan Menerima CloudTrail log file dari beberapa akun

DevOps Guru mendukung pencatatan semua tindakannya sebagai peristiwa di CloudTrail file log. Untuk informasi lebih lanjut, lihat Tindakan di DevOps Referensi API Guru.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Baik permintaan tersebut dibuat dengan kredensial pengguna atau root.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh orang lain AWS layanan.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami DevOps Entri file log Guru

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan a CloudTrail entri log yang menunjukkan `UpdateResourceCollection` tindakan.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
```

```
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

DevOps Guru dan antarmuka titik akhir VPC (AWS PrivateLink)

Anda dapat menggunakan titik akhir VPC saat memanggil Amazon DevOps API Guru. Saat Anda menggunakan titik akhir VPC, panggilan API Anda lebih aman karena terdapat di dalam VPC Anda dan tidak mengakses internet. Untuk informasi lebih lanjut, lihat Tindakan di Amazon DevOps Referensi API Guru.

Anda membuat koneksi pribadi antara VPC Anda dan DevOps Guru dengan menciptakan antarmuka titik akhir VPC. Titik akhir antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda untuk mengakses secara pribadi DevOps API Guru tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi DevOps API Guru. Lalu lintas antara VPC Anda dan DevOps Guru tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda.

Untuk informasi lebih lanjut, lihat Antarmuka titik akhir VPC (AWS PrivateLink) di Panduan Pengguna Amazon VPC.

Pertimbangan untuk DevOps Titik akhir Guru VPC

Sebelum Anda menyiapkan titik akhir VPC antarmuka untuk DevOps Guru, pastikan Anda mengulas Properti dan batasan titik akhir antarmuka di Panduan Pengguna Amazon VPC.

DevOps Guru mendukung membuat panggilan ke semua tindakan API dari VPC Anda.

Membuat titik akhir antarmuka VPC untuk DevOps Guru

Anda dapat membuat titik akhir VPC untuk DevOps Layanan Guru menggunakan konsol Amazon VPC atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Buat titik akhir VPC untuk DevOps Guru menggunakan nama layanan berikut:

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

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke DevOps Guru menggunakan nama DNS default untuk Wilayah, misalnya, `devops-guru.us-east-1.amazonaws.com`.

Untuk informasi selengkapnya, lihat Mengakses layanan melalui titik akhir antarmuka dalam Panduan Pengguna Amazon VPC.

Membuat kebijakan titik akhir VPC untuk DevOps Guru

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke DevOps Guru. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan titik akhir VPC dalam Panduan Pengguna Amazon VPC.

Contoh: Kebijakan titik akhir VPC untuk DevOps Tindakan Guru

Berikut ini adalah contoh kebijakan titik akhir untuk DevOps Guru. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke yang terdaftar DevOps Tindakan Guru untuk semua kepala sekolah di semua sumber daya.

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

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

Keamanan infrastruktur di DevOps Guru

Sebagai layanan terkelola, Amazon DevOps Guru dilindungi oleh AWS keamanan jaringan global. Untuk informasi tentang AWS layanan keamanan dan bagaimana AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk mendesain Anda AWS lingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur di Pilar Keamanan AWS Kerangka Kerja yang Didesain dengan Baik.

Anda menggunakan AWS panggilan API yang diterbitkan untuk mengakses DevOps Guru melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Kurva Elliptik Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Ketahanan di Amazon DevOps Guru

The AWS Infrastruktur global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Zona Ketersediaan yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. DevOps Guru beroperasi di beberapa Availability Zone dan menyimpan data artefak dan metadata di Amazon S3 dan Amazon DynamoDB. Data terenkripsi Anda disimpan secara berlebihan di berbagai fasilitas dan beberapa perangkat di setiap fasilitas, sehingga sangat tersedia dan sangat berdaya tahan.

Untuk informasi lebih lanjut tentang AWS Wilayah dan Zona Ketersediaan, lihat AWS Infrastruktur Global.

Kuota dan batasan untuk Amazon Guru DevOps

Tabel berikut mencantumkan kuota saat ini di Amazon DevOps Guru. Kuota ini untuk setiap AWS Region yang didukung untuk setiap AWS akun.

Notifikasi

Jumlah maksimum topik Amazon Simple Notification Service yang dapat Anda tentukan sekaligus	2

CloudFormation tumpukan

Jumlah maksimum AWS CloudFormation tumpukan yang dapat Anda tentukan	1000

DevOpsBatas pemantauan sumber daya Guru

Deskripsi sumber daya	Kuota	Dapat ditingkatkan
Batas default untuk memantau antrian Amazon Simple Queue Service (Amazon SQS)	100*	Ya**

*Untuk akun DevOps Guru baru yang dibuat pada atau setelah 29 Juni 2023, dan untuk akun yang sudah ada yang aktif pada tanggal yang sama dan memiliki kurang dari 100 antrian Amazon SQS.

**Untuk meminta perubahan batas ini, hubungi Dukungan di https://aws.amazon.com/contact-us. Anda dapat meminta batas pemantauan antrian Amazon SQS 100, 500, 1.000, 5.000, atau 10.000.

DevOpsKuota Guru untuk membuat, menerapkan, dan mengelola API

Kuota tetap berikut berlaku untuk membuat, menerapkan, dan mengelola API di DevOps Guru, menggunakan, konsol API Gateway AWS CLI, atau API Gateway REST API dan nya. SDKs

Untuk daftar semua Tindakan DevOps Guru APIs, lihat Amazon DevOps Guru Actions.

Kuota default	Dapat ditingkatkan	
20 permintaan setiap 1 detik per akun	Ya	

Amazon DevOps Sejarah dokumen Guru

Tabel berikut menjelaskan dokumentasi untuk rilis ini DevOps Guru.

- Versi API: terbaru
- Pembaruan dokumentasi terbaru: Agustus 9, 2023

Perubahan	Deskripsi	Tanggal
Panduan transisi ke Amazon CloudWatch dan Amazon DevOps Agen	Menambahkan panduan untuk transisi dari Amazon DevOps Guru ke Amazon CloudWatch dan Amazon DevOps Agen sebelum Amazon DevOps Guru mencapai akhir dukungan pada 30 September 2027. Untuk informasi lebih lanjut, lihat Transisi dari Amazon DevOps Guru ke Amazon CloudWatch dan Amazon DevOps Agen.	8 Oktober 2026
Pemberitahuan akhir dukungan	Pemberitahuan akhir dukungan: Pada 30 September 2027, AWS akan mengakhiri dukungan untuk Amazon DevOps Guru. Setelah 30 September 2027, Anda tidak akan lagi dapat mengakses Amazon DevOps Konsol Guru atau Amazon DevOps Sumber daya Guru. Untuk informasi lebih lanjut, lihat Amazon DevOps Guru berakhir dukungan.	September 29, 2026

Pembaruan kebijakan terkelola	Langganan Amazon SNS dan akses daftar berlangganan telah ditambahkan ke `AmazonDevOpsGuruConsoleFullAccess` kebijakan. Akses daftar langganan juga telah ditambahkan ke `AmazonDevOpsGuruReadOnlyAccess` kebijakan. Untuk informasi lebih lanjut, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.	9 Agustus 2023
Kunci enkripsi yang dikelola pelanggan	DevOps Guru sekarang mendukung enkripsi dengan kunci yang dikelola pelanggan menggunakan AWS KMS. Untuk informasi lebih lanjut, lihat Perlindungan data di DevOps Guru.	5 Juli 2023
DevOps Guru untuk RDS mendukung RDS PostgreSQL	DevOps Guru untuk RDS dapat mendeteksi hambatan kinerja dan wawasan lainnya di database PostgreSQL. Untuk informasi lebih lanjut, lihat Manfaat dari DevOps Guru untuk RDS.	30 Maret 2023

DevOps Guru untuk RDS mendukung wawasan proaktif	DevOps Guru untuk RDS menerbitkan wawasan proaktif dengan rekomendasi untuk membantu Anda mengatasi masalah di database Aurora Anda sebelum menjadi masalah yang lebih besar. Untuk informasi lebih lanjut, lihat Bekerja dengan anomali di DevOps Guru untuk RDS.	28 Februari 2023
Halaman sumber daya yang dianalisis	Halaman baru di DevOps Konsol Guru mencantumkan sumber daya di akun Anda yang dianalisis oleh DevOps Guru. Untuk informasi lebih lanjut, lihat Melihat sumber daya yang dianalisis oleh DevOps Guru.	20 Oktober 2022
Pengaturan konfigurasi notifikasi baru	Anda sekarang dapat memilih apakah akan menerima semua notifikasi atau hanya menerima pemberitahuan untuk tingkat keparahan dan peristiwa tertentu. Untuk informasi lebih lanjut, lihat Memperbarui konfigurasi notifikasi Amazon Amazon SNS.	30 September 2022

Penambahan analisis anomali log ke kebijakan terkelola	AWS kebijakan yang dikelola untuk DevOps Guru atelah diperbarui di konsol IAM untuk mendukung akses ke CloudWatch aksi `FilterLogEvents` . Untuk informasi lebih lanjut, lihat DevOps Guru memperbarui ke AWS kebijakan terkelola dan peran terkait layanan.	30 Agustus 2022
Analisis anomali log ditambahkan	Anda dapat melihat informasi terperinci tentang grup log yang terkait dengan wawasan di DevOps Konsol Guru. Ada juga peran terkait layanan yang diperluas yang tersedia untuk dijelaskan CloudWatch log dan aliran. Untuk informasi lebih lanjut, lihat Memahami wawasan dalam DevOps Konsol Guru dan DevOps Guru memperbarui ke AWS kebijakan terkelola dan peran terkait layanan.	12 Juli 2022
CodeGuru Integrasi Profiler	DevOps Guru sekarang terintegrasi dengan Amazon CodeGuru Profiler dengan EventBridge aturan yang dikelola. Setiap inbound event dari CodeGuru Profiler adalah laporan anomali proaktif. Untuk informasi lebih lanjut, lihat Mengintegrasikan dengan CodeGuru Profiler.	7 Maret 2022

Service-linked pembaruan peran dan kebijakan terkelola	Kebijakan yang diperluas tersedia di konsol IAM. Perubahan memungkinkan DevOps Guru untuk mendukung integrasi yang ditingkatkan dengan Amazon Relational Database Service (Amazon RDS). Untuk informasi lebih lanjut, lihat Menggunakan peran terkait layanan dan AWS kebijakan yang dikelola (telah ditentukan sebelumnya) untuk DevOps Guru.	21 Desember 2021
Kebijakan terkelola baru ditambahkan	Yang `AmazonDevOpsGuruConsoleFullAccess` kebijakan telah ditambahkan. Untuk informasi lebih lanjut, lihat Identity-based Kebijakan untuk Amazon DevOps Guru.	Desember 6, 2021
Dukungan untuk menentukan aplikasi Anda dengan AWS tag	Anda sekarang dapat menggunakan AWS tag untuk mengidentifikasi sumber daya yang Anda inginkan DevOps Guru untuk menganalisis, mengidentifikasi sumber daya di aplikasi Anda, dan memfilter wawasan di konsol. Untuk informasi lebih lanjut, lihat Gunakan tag untuk mengidentifikasi sumber daya dalam aplikasi Anda.	1 Desember 2021

Service-linked pembaruan peran dan kebijakan terkelola	Kebijakan yang diperluas tersedia di konsol IAM. Perubahan memungkin kan DevOps Guru untuk mendukung integrasi yang ditingkatkan dengan Amazon Relational Database Service (Amazon RDS). Untuk informasi lebih lanjut, lihat Menggunakan peran terkait layanan dan AWS kebijakan yang dikelola (telah ditentuka n sebelumnya) untuk DevOps Guru.	1 Desember 2021
Dukungan Amazon RDS	DevOps Guru sekarang menyediakan analisis dan wawasan komprehensif untuk sumber daya Amazon Relational Database Service (Amazon RDS) di aplikasi Anda. Untuk informasi lebih lanjut, lihat Bekerja dengan anomali di DevOps Guru untuk Amazon RDS.	1 Desember 2021
Amazon EventBridge integrasi	DevOps Guru sekarang terintegrasi dengan EventBrid ge untuk memberi tahu Anda tentang peristiwa tertentu yang berkaitan dengan Anda DevOps Wawasan guru. Untuk informasi lebih lanjut, lihat Bekerja dengan EventBridge.	18 November 2021

AWS kebijakan terkelola ditambahkan	Baru AWS kebijakan yang dikelola ditambahkan. Yang `AmazonDevOpsGuruOrganizationsAccess` Kebijakan memberikan akses ke DevOps Guru dalam suatu organisasi. Untuk informasi lebih lanjut, lihat kebijakan berbasis identitas.	November 16, 2021
Service-linked pembaruan kebijakan peran	Kebijakan yang diperluas tersedia di konsol IAM. Perubahan memungkinkan DevOps Guru untuk mendukung tampilan multi akun. Untuk informasi lebih lanjut, lihat Menggunakan peran terkait layanan.	4 November 2021
Dukungan lintas akun	Anda sekarang dapat melihat wawasan dan metrik di beberapa akun di organisasi Anda. Untuk informasi lebih lanjut, lihat Apa itu Amazon DevOps Guru.	4 November 2021
Rilis ketersediaan umum	Amazon DevOps Guru sekarang tersedia secara umum (GA).	4 Mei 2021

Topik baru	Anda sekarang dapat membuat perkiraan biaya bulanan untuk DevOps Guru untuk menganalisis sumber daya Anda. Untuk informasi lebih lanjut, lihat Perkirakan Amazon Anda DevOps Biaya Guru.	27 April 2021
Dukungan VPC Endpoint	Anda sekarang dapat menggunakan titik akhir VPC untuk meningkat kan keamanan analisis sumber daya dan pembuatan wawasan. Untuk informasi lebih lanjut, lihat DevOps Guru dan antarmuka titik akhir VPC (AWS PrivateLink).	April 15, 2021
Topik baru	Topik baru tentang cara memantau DevOps Guru dengan Amazon CloudWatc h telah ditambahkan. Untuk informasi lebih lanjut, lihat Pemantauan DevOps Guru dengan Amazon CloudWatch.	11 Desember 2020
Pratinjau rilis	Ini adalah rilis pratinjau dari Amazon DevOps Panduan Pengguna Guru.	1 Desember 2020

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS