aws

Panduan Pengguna

AWS Health

AWS Health: Panduan Pengguna

Table of Contents

Apakah AWS Health itu?

AWS Healthmemberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan akun AndaLayanan AWS. Anda dapat menggunakan peristiwa AWS Health untuk mempelajari bagaimana perubahan layanan dan sumber daya dapat memengaruhi aplikasi yang berjalan di AWS. AWS Health menyediakan informasi yang relevan dan tepat waktu untuk membantu Anda mengelola peristiwa yang sedang berlangsung. AWS Health juga membantu Anda menyadari dan mempersiapkan kegiatan yang direncanakan. Layanan ini memberikan peringatan dan notifikasi yang dipicu oleh perubahan kesehatan dari sumber daya AWS, sehingga Anda mendapatkan visibilitas dan panduan peristiwa mendekati instan untuk membantu mempercepat pemecahan masalah.

Semua pelanggan dapat menggunakan AWS HealthDashboard AWS , yang didukung oleh AWS Health API. Dasbor tidak memerlukan pengaturan, dan siap digunakan untuk pengguna AWS terautentikasi. Untuk sorotan layanan lainnya, lihat halaman detail AWS Health Dashboard halaman .

Untuk memahami dasar-dasar AWS Health dan bagaimana Anda dapat menggunakan layanan ini, lihatApakah Anda pengguna AWS Health baru?.

Untuk daftar istilah yang akan Anda lihat saat Anda menggunakanAWS Health, lihatKonsep untuk AWS Health.

> **Catatan**
>
> - AWS HealthDasbor tersedia untuk semua AWS pelanggan tanpa biaya tambahan.
> - Semua AWS pelanggan dapat menerima AWS Health acara melalui Amazon tanpa EventBridge biaya tambahan.
> - Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda dapat menggunakan AWS Health API untuk berintegrasi dengan sistem internal dan pihak ketiga. Untuk informasi lebih lanjut, lihat Referensi API AWS Health.
> - Untuk informasi selengkapnya tentang AWS Support paket yang tersedia, lihat AWS Support.

Apakah Anda pengguna AWS Health baru?

Jika Anda pengguna baru AWS Health, mulailah dengan membaca bagian berikut:

- Apakah AWS Health itu?Bagian ini menjelaskan model data yang mendasarinya, operasi yang didukungnya, dan AWS SDK yang dapat Anda gunakan untuk berinteraksi dengan layanan.
- Konsep untuk AWS Health— Pelajari dasar-dasar tentang AWS Health dan istilah yang akan Anda temui saat Anda menggunakan layanan ini.
- Memulai AWS Health Dashboard Anda — Kesehatan akun Anda— Pelajari cara melihat peristiwa dan entitas yang terpengaruh dan melakukan pemfilteran lanjutan. Dasbor ini mencakup acara yang khusus untuk akun dan organisasi Anda.
- AWS Health Dashboard — Layanan kesehatan— Jika Anda tidak memilikiAkun AWS, Anda dapat melihat informasi tentang kesehatan dan status masing-masing Layanan AWSWilayah AWS.
- Memantau AWS Health peristiwa dengan Amazon EventBridge— Anda dapat menggunakan Amazon EventBridge untuk menerima pemberitahuan push dariAWS Health.
- Mengakses API AWS Health— Bagian AWS Health API menjelaskan operasi yang mengambil informasi tentang peristiwa dan entitas.

AWS Healthmenyediakan konsol, yang disebut AWS Health Dashboard, untuk semua pelanggan. Anda tidak perlu menulis kode atau melakukan tindakan apapun untuk mengatur dasbor.

Anda dapat mengatur EventBridge aturan untuk menerima AWS Health acara di Amazon EventBridge. Ini menyediakan cara untuk menggunakan pemberitahuan push untuk mengotomatiskan manajemen AWS Health acara dengan membuat EventBridge aturan Amazon untuk mengambil tindakan.

Jika Anda memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda dapat mengakses informasi yang disajikan di dasbor secara terprogram. Anda dapat menggunakan AWS Command Line Interface (AWS CLI) atau menulis kode untuk membuat permintaan, dengan menggunakan REST API langsung atau SDK AWS.

Untuk informasi selengkapnya tentang menggunakan AWS Health acara di Amazon EventBridge, lihatMemantau AWS Health peristiwa dengan Amazon EventBridge. Untuk informasi lebih lanjut tentang penggunaan AWS Health dengan AWS CLI, lihat Referensi AWS CLI untuk AWS Health. Untuk petunjuk pemasangan AWS CLI, lihat Menginstal AWS Command Line Interface.

Konsep untuk AWS Health

Pelajari tentang AWS Health konsep dan pahami bagaimana Anda dapat menggunakan layanan ini untuk menjaga kesehatan aplikasi, layanan, dan sumber daya Anda Akun AWS.

Topik

AWS Health acara

AWS Health Acara, juga dikenal sebagai acara Kesehatan, adalah pemberitahuan yang AWS Health dikirim atas nama AWS layanan lain. Anda dapat menggunakan acara ini untuk mempelajari tentang perubahan mendatang atau terjadwal yang mungkin memengaruhi akun Anda. Misalnya, AWS Health dapat mengirim peristiwa jika AWS Identity and Access Management (IAM) berencana untuk menghentikan kebijakan terkelola atau AWS Config berencana untuk menghentikan aturan terkelola. AWS Health juga mengirimkan acara ketika ada masalah ketersediaan layanan di file Wilayah AWS. Anda dapat meninjau deskripsi acara untuk memahami masalah, mengidentifikasi sumber daya yang terpengaruh, dan mengambil tindakan yang disarankan.

Ada dua jenis acara Kesehatan:

Daftar Isi

Acara khusus akun

Acara khusus akun bersifat lokal untuk akun Anda Akun AWS atau akun di organisasi Anda AWS . Misalnya, jika ada masalah dengan jenis instans Amazon Elastic Compute Cloud (Amazon EC2) di Wilayah yang Anda gunakan AWS Health , berikan informasi tentang peristiwa dan nama sumber daya yang terpengaruh.

Anda dapat menemukan peristiwa khusus akun dari AWS Health Dasbor, AWS Health API, atau menggunakan CloudWatch Acara Amazon untuk menerima pemberitahuan.

Acara publik

Acara publik adalah peristiwa layanan yang dilaporkan yang tidak spesifik untuk akun. Misalnya, jika ada masalah layanan untuk Amazon Simple Storage Service (Amazon S3) di Wilayah Timur AS (Ohio) AWS Health , berikan informasi tentang acara tersebut, meskipun Anda tidak menggunakan layanan tersebut atau memiliki bucket S3 di Wilayah tersebut. Kami menyarankan Anda meninjau pemberitahuan publik sebelum Anda mengambil tindakan terhadapnya.

Anda dapat menemukan acara publik dari AWS Health Dasbor dan AWS Health Dasbor — Kesehatan layanan.

Jika Anda memiliki akun, lihatMemulai AWS Health Dashboard Anda — Kesehatan akun Anda.

Jika Anda tidak memiliki akun, lihatAWS Health Dashboard — Layanan kesehatan.

AWS Health Dasbor

Jika Anda memiliki Akun AWS, AWS Health Dasbor Anda menampilkan acara publik dan acara khusus akun.

Kami menyarankan Anda menggunakan AWS Health Dasbor Anda untuk mempelajari tentang acara yang memberikan kesadaran umum, seperti masalah pemeliharaan yang akan datang untuk layanan di Wilayah. Anda juga dapat menggunakan AWS Health Dasbor untuk mempelajari peristiwa yang mungkin memengaruhi Anda secara langsung, seperti sumber daya yang tidak digunakan lagi di akun Anda.

Anda dapat masuk ke AWS Management Console untuk melihat AWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.

Untuk informasi selengkapnya, lihat Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.

AWS Health Dashboard — Layanan kesehatan

Jika Anda tidak memiliki akun, Anda dapat menggunakan AWS Health Dasbor — Layanan kesehatan di https://health.aws.amazon.com/health/status untuk melihat acara publik. Acara publik dilaporkan masalah layanan AWS yang memberikan informasi tentang ketersediaan layanan. Situs web ini hanya menampilkan acara publik, yang tidak spesifik untuk akun apa pun. Anda tidak perlu masuk atau memiliki akun untuk melihat halaman ini.

Untuk informasi selengkapnya, lihat AWS Health Dashboard — Layanan kesehatan.

Kode jenis acara

Kode jenis acara yang ditampilkan dalam acara Kesehatan mencakup layanan yang terpengaruh dan jenis acara. Misalnya, jika Anda menerima acara Kesehatan yang memiliki kode jenis `AWS_EC2_SYSTEM_MAINTENANCE_EVENT` acara, ini berarti bahwa layanan menjadwalkan acara pemeliharaan yang mungkin memengaruhi Anda. Gunakan informasi ini untuk merencanakan ke depan atau mengambil tindakan untuk akun Anda.

Kategori jenis acara

Semua acara Kesehatan memiliki kategori jenis acara terkait. Untuk beberapa peristiwa, kategori jenis acara mungkin muncul dalam kode tipe acara, seperti `AWS_RDS_MAINTENANCE_SCHEDULED` kode. Dalam contoh ini, kategori dijadwalkan. Anda dapat menggunakan informasi ini untuk memahami kategori acara pada tingkat tinggi.

Kami menyarankan Anda memantau semua kategori jenis acara. Perhatikan bahwa setiap kategori muncul untuk berbagai jenis acara. Anda juga dapat menggunakan operasi DescribeEventTypes API untuk menemukan kategori jenis acara.

Pemberitahuan akun

Peristiwa ini memberikan informasi tentang administrasi atau keamanan akun dan layanan Anda. Peristiwa ini mungkin informatif, atau mungkin memerlukan tindakan segera dari Anda. Kami menyarankan Anda memperhatikan jenis acara ini dan meninjau semua tindakan yang disarankan.

Berikut ini adalah contoh kode jenis acara untuk pemberitahuan akun:

- `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`— Anda memiliki bucket Amazon S3 yang memungkinkan akses publik.

- AWS_BILLING_SUSPENSION_NOTICE— Akun Anda memiliki biaya terutang dan telah ditangguhkan, atau Anda menonaktifkan akun Anda.
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION— Ada masalah layanan untuk Amazon WorkSpaces.

Isu

Peristiwa ini adalah peristiwa tak terduga yang memengaruhi AWS layanan atau sumber daya. Peristiwa umum dalam kategori ini termasuk komunikasi tentang masalah operasional yang menyebabkan degradasi layanan, atau masalah tingkat sumber daya lokal untuk kesadaran Anda.

Berikut ini adalah contoh kode jenis acara untuk masalah:

- AWS_EC2_OPERATIONAL_ISSUEMasalah operasional untuk suatu layanan, seperti keterlambatan dalam menggunakan layanan.
- AWS_EC2_API_ISSUE— Masalah operasional untuk API layanan, seperti peningkatan latensi untuk operasi API.
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE— Masalah tingkat sumber daya lokal yang mungkin memengaruhi sumber daya Amazon Elastic Block Store (Amazon EBS) Anda.
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT— Acara ini berarti bahwa akun Anda mungkin ditangguhkan jika Anda tidak mengambil tindakan.

Perubahan terjadwal

Acara ini memberikan informasi tentang perubahan yang akan datang pada layanan dan sumber daya Anda. Peristiwa ini mencakup peristiwa siklus hidup yang direncanakan seperti end-of-support pemberitahuan dan peningkatan otomatis untuk versi yang berbeda. Beberapa peristiwa mungkin menyarankan Anda mengambil tindakan untuk menghindari gangguan layanan, sementara yang lain akan terjadi secara otomatis tanpa tindakan apa pun dari pihak Anda. Sumber daya Anda mungkin tidak tersedia untuk sementara selama aktivitas perubahan terjadwal. Semua acara dalam kategori ini adalah acara khusus akun.

Berikut ini adalah contoh kode jenis acara untuk perubahan terjadwal:

- AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED- Instans Amazon EC2 memerlukan reboot.
- AWS_SAGEMAKER_SCHEDULED_MAINTENANCE— SageMaker membutuhkan acara pemeliharaan, seperti memperbaiki masalah layanan.
- AWS_RDS_PLANNED_LIFECYCLE_EVENTAmazon RDS menjadwalkan acara siklus hidup yang direncanakan, seperti end-of-support acara untuk salah satu versinya, yang memerlukan tindakan pelanggan.

> **Tip**
>
> Jika Anda menggunakan AWS Health API atau AWS Command Line Interface (AWS CLI) untuk menampilkan detail peristiwa, `Event` objek berisi `eventScopeCode` bidang dengan `ACCOUNT_SPECIFIC` nilai. Untuk informasi lebih lanjut, lihat Referensi API AWS Health.

Status acara

Status acara memberi tahu Anda jika acara Kesehatan terbuka, ditutup, atau akan datang. Anda dapat melihat peristiwa Kesehatan di AWS Health Dasbor atau AWS Health API hingga 90 hari.

Entitas terpengaruh

Entitas yang terpengaruh adalah AWS sumber daya yang mungkin terpengaruh oleh peristiwa tersebut. Misalnya, jika Anda menerima acara terjadwal untuk pemeliharaan Amazon EC2 untuk jenis instans tertentu yang Anda gunakan di akun, Anda dapat menggunakan peristiwa Health untuk menentukan ID instans yang terpengaruh. Gunakan informasi ini untuk mengatasi masalah layanan potensial, seperti membuat atau menghentikan sumber daya.

AWS Health acara di Amazon EventBridge

Anda dapat mengatur EventBridge aturan Amazon untuk akun Anda untuk mengotomatiskan tindakan setelah AWS Health peristiwa yang sesuai diterima oleh akun. Ini bisa berupa tindakan umum, seperti mengirim semua pesan peristiwa siklus hidup yang direncanakan ke antarmuka obrolan. Atau, mereka bisa berupa tindakan spesifik, seperti memicu alur kerja di alat manajemen layanan TI.

Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.

AWS Health API

Anda dapat menggunakan AWS Health API untuk mengakses informasi yang muncul di AWS Health Dasbor secara terprogram, seperti berikut ini:

- Dapatkan informasi tentang acara yang dapat memengaruhi AWS layanan dan sumber daya Anda

- Mengaktifkan atau menonaktifkan fitur tampilan organisasi untuk AWS organisasi Anda
- Filter acara Anda berdasarkan layanan tertentu, kategori jenis acara, dan kode jenis acara

Untuk informasi lebih lanjut, lihat Referensi API AWS Health.

> **Note**
>
> Anda harus memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support AWS Supportuntuk menggunakan API. AWS Health Jika Anda memanggil AWS Health API dari akun yang tidak memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, Anda akan menerima error. `SubscriptionRequiredException`

Tampilan organisasi

Anda dapat menggunakan fitur ini untuk menggabungkan semua peristiwa kesehatan untuk AWS akun di AWS Organizations dalam satu tampilan di AWS Health Dasbor. Anda kemudian dapat masuk ke akun manajemen organisasi Anda atau menggunakan AWS Health API untuk melihat semua peristiwa yang mungkin memengaruhi akun dan sumber daya yang berbeda. Anda dapat mengaktifkan fitur ini dari AWS Health konsol atau API. Untuk informasi selengkapnya, lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.

AWS Health Dashboard — Layanan kesehatan

Anda dapat menggunakan AWS Health Dasbor — Layanan kesehatan untuk melihat kesehatan semua Layanan AWS. Halaman ini menampilkan peristiwa layanan yang dilaporkan untuk seluruh layanan Wilayah AWS. Anda tidak perlu masuk atau memiliki Akun AWS untuk mengakses halaman AWS Health Dashboard — Layanan kesehatan.

> **Tip**
>
> Situs web ini hanya menampilkan acara-acara publik, yang tidak spesifik untuk sebuah Akun AWS. Jika Anda sudah memiliki akun, kami sarankan Anda masuk untuk melihat AWS Health Dasbor Anda dan tetap mendapat informasi tentang peristiwa yang dapat memengaruhi akun dan layanan Anda. Untuk informasi selengkapnya, lihat Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.

Untuk melihat AWS Health Dasbor — Layanan kesehatan

1. Arahkan ke halaman https://health.aws.amazon.com/health/status.

   > **Note**
   >
   > Jika Anda sudah masuk ke halaman Akun AWS, Anda akan diarahkan ke AWS Health Dasbor — halaman kesehatan akun Anda.

2. Di bawah Kesehatan layanan, pilih Terbuka dan masalah terbaru untuk melihat peristiwa yang baru-baru ini dilaporkan. Anda dapat melihat informasi berikut tentang acara tersebut:

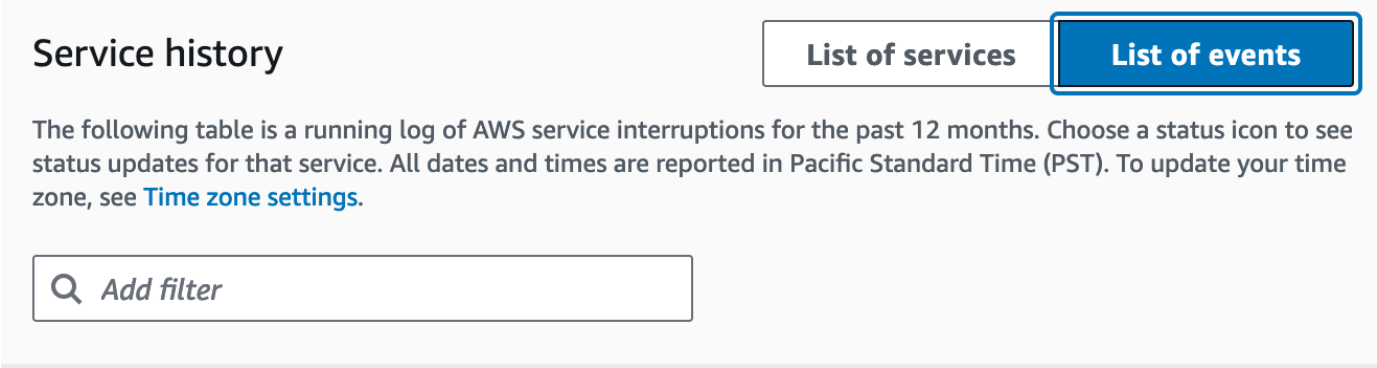
   - Nama acara dan Wilayah yang terpengaruh. Misalnya, Masalah operasional — Amazon Elastic Compute Cloud (Virginia N.)
   - Nama layanan
   - Tingkat keparahan acara, seperti Informasi atau Degradasi
   - Garis waktu pembaruan terbaru untuk acara tersebut
   - Daftar Layanan AWS yang juga terpengaruh oleh peristiwa ini

> **Note**
>
> Anda dapat melihat acara di zona waktu lokal Anda atau di UTC. Untuk informasi selengkapnya, lihat Pengaturan zona waktu.

3. (Opsional) Di samping acara, pilih RSS untuk berlangganan umpan RSS untuk acara ini. Anda akan menerima pemberitahuan tentang layanan khusus ini dalam yang ditentukan Wilayah AWS.
4. Pilih Riwayat layanan untuk melihat tabel Riwayat layanan. Tabel ini menunjukkan semua Layanan AWS gangguan selama 12 bulan terakhir.

> **Tip**
>
> Anda dapat memfilter berdasarkan Layanan, Wilayah AWS, dan tanggal.

5. Di samping acara layanan yang sedang berlangsung, pilih ikon status ( ) untuk melihat informasi selengkapnya tentang acara tersebut.
6. (Opsional) Untuk melihat ini sebagai daftar peristiwa bersejarah, pilih tombol daftar acara. Pilih acara apa pun di kolom acara untuk melihat informasi selengkapnya tentang peristiwa tertentu di panel samping pop-up.



> **Note**
>
> Memilih acara publik apa pun setelah September 2023 akan mengisi URL di browser dengan tautan ke acara publik AWS Health tersebut. Setelah memilih tautan ini, Anda menavigasi ke daftar tampilan acara dengan pop-up acara tersebut.

7. (Opsional) Pilih RSS untuk berlangganan RSS feed. Anda akan menerima pemberitahuan tentang layanan khusus ini dalam yang ditentukan Wilayah AWS.
8. (Opsional) Anda dapat melihat acara di zona waktu lokal atau UTC. Untuk informasi selengkapnya, lihat Pengaturan zona waktu.
9. (Opsional) Jika Anda memiliki akun, pilih Buka kesehatan akun Anda untuk masuk. Setelah masuk, Anda dapat melihat acara yang spesifik untuk akun Anda. Lihat informasi yang lebih lengkap di Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.

Acara siklus hidup yang direncanakan untuk AWS Health

Pelajari tentang peristiwa siklus hidup yang direncanakan untuk. AWS Health

Topik

Apa acara siklus hidup yang direncanakan?

AWS Health mengkomunikasikan perubahan penting yang dapat memengaruhi ketersediaan aplikasi Anda. Dalam model tanggung jawab AWS bersama, AWS ambil tindakan untuk menjaga perangkat keras dan infrastruktur yang mendasari yang mendukung sumber daya Anda tetap mutakhir dan aman. Namun, beberapa perubahan memerlukan tindakan atau koordinasi pelanggan untuk menghindari dampak pada aplikasi Anda. AWS Health memberi tahu Anda sebelumnya tentang perubahan penting seperti:

- Akhir dukungan perangkat lunak sumber terbuka - Beberapa Layanan AWS menjalankan versi perangkat lunak open source. Jika komunitas open source mengakhiri dukungan untuk versi perangkat lunak, maka AWS memberi tahu Anda kapan Anda perlu mengambil tindakan untuk meningkatkan dan menghindari dampak pada aplikasi Anda.
  - Amazon RDS for MySQL engine versi akhir dukungan
  - Versi Amazon EKS Kubernetes akhir dari dukungan
- Perubahan yang memengaruhi sumber AWS daya milik yang mungkin memerlukan tindakan Anda.
  - Kedaluwarsa sertifikat Otoritas Sertifikat Amazon RDS.
  - Amazon WorkDocs Companion mencapai akhir hayat dan tidak lagi tersedia.

> **Note**
>
> Semua pemberitahuan yang sesuai dengan kriteria ini akan dilaporkan melalui AWS Health Peristiwa Siklus Hidup yang Direncanakan.

- Burndown sumber daya dinamis dan metadata yang ditingkatkan: Dari saat Anda menerima notifikasi selama masa pakai AWS Health acara, sumber daya yang terpengaruh dikaitkan dengan AWS Health peristiwa sebagai entitas yang terpengaruh dengan status entitas tertentu. Sumber daya yang terpengaruh ditentukan dalam format ARN, jika berlaku. Jika sumber daya Anda yang terpengaruh memerlukan tindakan pelanggan, maka mereka terdaftar dengan status “PENDING”. Jika sumber daya Anda yang terpengaruh telah melakukan tindakan yang diperlukan atau sumber daya dihapus, maka status diperbarui ke “DISELESAIKAN”.

> **Note**
>
> - Pembaruan status sumber daya dilakukan secara asinkron dan berkala dan dapat mengalami penundaan hingga 72 jam dalam kesempatan langka.
> - Dalam pengecualian di mana pembaruan dinamis tidak disediakan, daripada sumber daya yang memiliki status “PENDING” atau “DISELESAIKAN”, sumber daya tidak akan diberikan status apa pun.
> - Pembaruan status sumber daya tidak didukung di Wilayah AWS GovCloud (US) dan China.

Apa yang harus saya harapkan ketika saya menerima pemberitahuan peristiwa siklus hidup yang direncanakan?

AWS Health Pengalaman untuk acara siklus hidup yang direncanakan membantu tim Anda mempelajari tentang perubahan siklus hidup yang akan datang dan melacak penyelesaian tindakan.

Jenis kategori: Perubahan terjadwal

Kode jenis acara: AWS _ {SERVICE} _PLANNED_LIFECYCLE_EVENT

Waktu mulai acara: Waktu mulai acara adalah tanggal tercepat di mana sumber daya Anda dipengaruhi oleh perubahan.

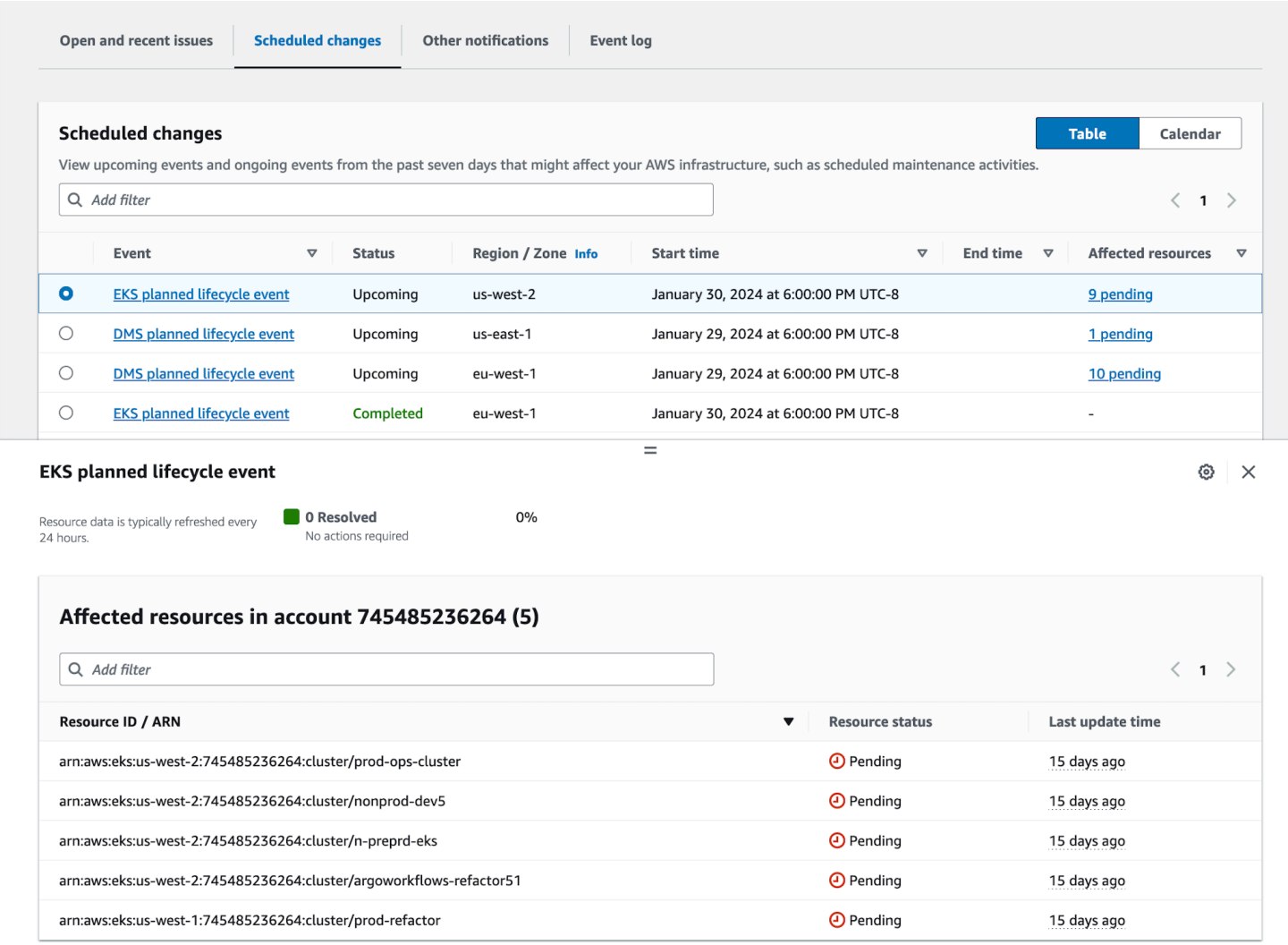
Waktu akhir acara: Waktu akhir acara adalah tanggal perubahan selesai di semua AWS sumber daya. Perhatikan bahwa waktu akhir tidak selalu ditentukan. Penting untuk memperlakukan waktu mulai sebagai tanggal perubahan.

> **Note**
>
> Organizations dapat mengharapkan untuk menerima satu acara ARN untuk setiap peristiwa siklus hidup yang direncanakan dikelompokkan berdasarkan Wilayah di mana ada sumber daya yang terpengaruh. Tetapi mereka mungkin menerima beberapa ARN jika organisasi memiliki sejumlah besar sumber daya Akun AWS atau terpengaruh.

Visibilitas awal ke peristiwa siklus hidup yang direncanakan: Peristiwa siklus hidup yang direncanakan dirancang untuk memiliki waktu tunggu minimum 180 hari untuk versi/perubahan utama dan 90 hari untuk versi/perubahan kecil, jika memungkinkan.

Burndown sumber daya dinamis dan metadata yang ditingkatkan: Dari saat Anda menerima notifikasi selama masa pakai AWS Health acara, sumber daya yang terpengaruh dikaitkan dengan AWS Health peristiwa sebagai entitas yang terpengaruh dengan status entitas tertentu. Sumber daya yang terpengaruh ditentukan dalam format ARN, jika berlaku. Jika sumber daya Anda yang terpengaruh memerlukan tindakan pelanggan, maka mereka terdaftar dengan status “PENDING”. Jika sumber daya Anda yang terpengaruh telah melakukan tindakan yang diperlukan atau sumber daya dihapus, maka status diperbarui ke “DISELESAIKAN”.

> **Note**
>
> - AWS Health pemberitahuan memberikan pembaruan status dari waktu ke waktu jika memungkinkan, kecuali untuk Wilayah AWS GovCloud (US) dan China.
> - Pembaruan status sumber daya dilakukan secara asinkron dan berkala dan dapat mengalami penundaan hingga 72 jam dalam kesempatan langka.

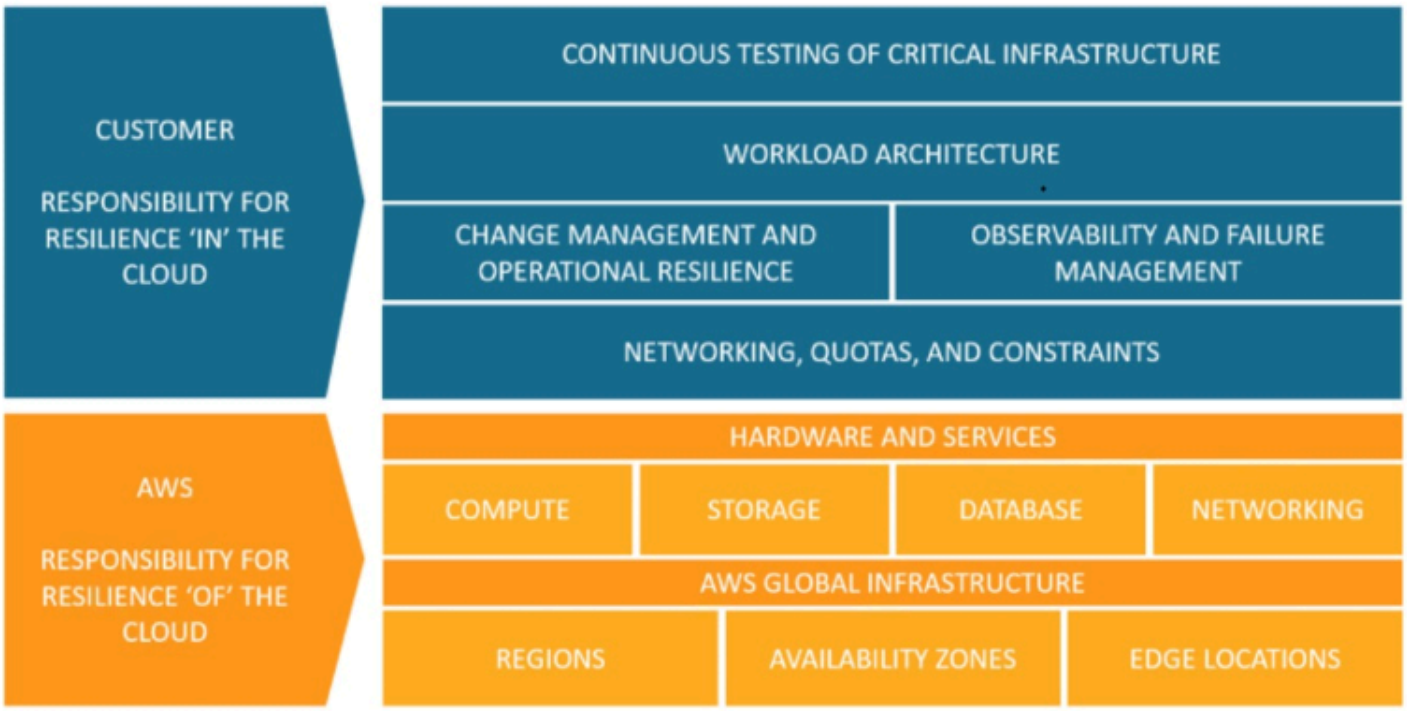


Setelah tanggal acara yang direncanakan berlalu:

1. Jika berlaku, layanan dapat menerapkan perubahan yang dijelaskan pada sumber daya Anda kapan saja setelah tanggal mulai acara.
2. Jika Anda menyelesaikan semua sumber daya sebelum akhir tanggal dukungan, maka AWS Health acara Anda berubah menjadi status “Ditutup”.
3. Jika Anda memiliki sumber daya yang luar biasa setelah tanggal yang tidak terselesaikan, maka AWS Health acara tetap terbuka selama 90 hari setelah tanggal mulai atau berakhir. Kemudian acara tersebut dihapus.

Model tanggung jawab bersama untuk ketahanan

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. Bergantung pada layanan yang digunakan, model bersama ini dapat membantu meringankan beban operasional pelanggan. Ini karena AWS mengoperasikan, mengelola, dan mengontrol komponen dari sistem operasi host dan lapisan virtualisasi hingga keamanan fisik fasilitas di mana layanan beroperasi. Pelanggan memikul tanggung jawab dan pengelolaan sistem operasi tamu (termasuk pembaruan dan patch keamanan) dan perangkat lunak aplikasi terkait lainnya, selain konfigurasi firewall grup keamanan AWS yang disediakan. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.



Mengakses acara siklus hidup yang direncanakan

Acara siklus hidup yang direncanakan dapat diakses dan dipantau menggunakan beberapa saluran:

- Gunakan Amazon EventBridge
- Gunakan AWS Health dasbor
  - Tampilan kalender
  - Tampilan sumber daya yang terpengaruh
- Gunakan AWS Health API

Memulai AWS Health Dashboard Anda — Kesehatan akun Anda

Anda dapat menggunakan AWS Health Dasbor Anda untuk mempelajari tentang AWS Health acara. Peristiwa ini dapat memengaruhi Anda Layanan AWS atauAkun AWS. Setelah Anda masuk ke akun Anda, AWS Health Dasbor menampilkan informasi dengan cara berikut:

- Acara akun Anda — Halaman ini menampilkan acara yang spesifik untuk akun Anda. Anda dapat melihat perubahan terbuka, terbaru, dan terjadwal. Anda juga dapat melihat notifikasi dan log peristiwa yang menampilkan semua peristiwa dari 90 hari terakhir.
- Acara organisasi Anda — Halaman ini menampilkan acara yang khusus untuk organisasi AndaAWS Organizations. Anda dapat melihat perubahan terbuka, terbaru, dan terjadwal untuk organisasi Anda. Anda juga dapat melihat notifikasi, serta log peristiwa yang menampilkan semua acara organisasi dari 90 hari terakhir.

> **Note**
>
> Jika Anda tidak memilikiAkun AWS, Anda dapat menggunakan AWS Health Dashboard — Layanan kesehatan untuk mempelajari tentang ketersediaan layanan umum.
> Jika Anda memiliki akun, kami sarankan Anda masuk ke AWS Health Dasbor untuk mendapatkan wawasan lebih dalam tentang acara dan perubahan mendatang yang mungkin memengaruhi layanan dan sumber daya Anda.

Daftar Isi

- Tampilan sumber daya yang terpengaruh
- Pengaturan zona waktu
- Kesehatan organisasi Anda
- Konfigurasikan Amazon EventBridge
- AWS HealthSadar
- Pemberitahuan untuk peristiwa AWS Health

Melihat peristiwa akun Anda di AWS Health Dasbor

Anda dapat masuk ke akun Anda untuk mendapatkan acara dan rekomendasi yang dipersonalisasi.

Untuk melihat peristiwa akun di AWS Health Dasbor

1. Buka AWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di panel navigasi, untuk kesehatan akun Anda, Anda dapat memilih opsi berikut:
    a. Terbitan terbuka dan terbaru — Lihat acara yang baru dibuka dan ditutup.
    b. Perubahan terjadwal — Lihat acara mendatang yang mungkin memengaruhi layanan dan sumber daya Anda.
    c. Notifikasi lainnya — Lihat semua pemberitahuan lain dan acara yang sedang berlangsung dari tujuh hari terakhir yang mungkin memengaruhi akun Anda.
    d. Log acara — Lihat semua acara dari 90 hari terakhir.

Terbuka dan masalah terbaru

Gunakan tab Terbuka dan masalah terbaru untuk melihat semua peristiwa yang sedang berlangsung dari tujuh hari terakhir yang mungkin memengaruhi akun Anda.

Saat Anda memilih acara dari dasbor, panel Detail akan muncul dengan informasi tentang peristiwa dan daftar sumber daya yang terpengaruh. Untuk informasi selengkapnya, lihat Detail acara.

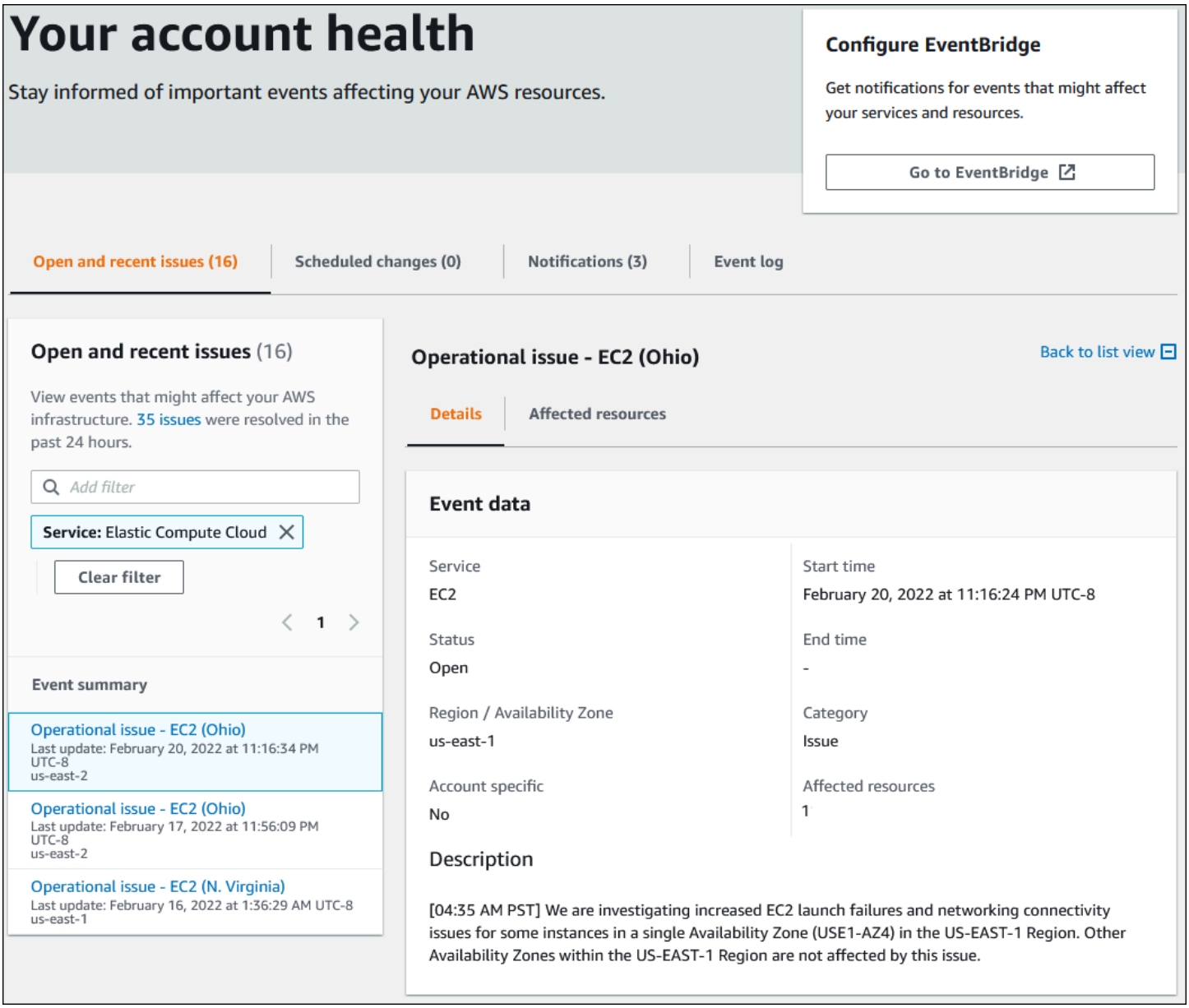
Anda dapat memfilter peristiwa yang muncul di tab apa pun dengan memilih opsi dari daftar filter. Misalnya, Anda dapat mempersempit hasil berdasarkan Availability Zone, Region, event end time atau update time terakhirLayanan AWS, dan sebagainya.

Untuk melihat semua peristiwa, bukan yang terbaru yang muncul di dasbor, pilih Log peristiwatab.

> **Note**
>
> Saat ini, Anda tidak dapat menghapus notifikasi untuk acara yang muncul di AWS Health Dasbor Anda. Setelah Layanan AWS menyelesaikan suatu peristiwa, notifikasi akan dihapus dari tampilan dasbor Anda.

Example : Peristiwa masalah operasional untuk Amazon Elastic Compute Cloud (Amazon EC2)

Gambar berikut menunjukkan peristiwa untuk kegagalan peluncuran dan masalah konektivitas untuk instans Amazon EC2.



Perubahan terjadwal

Gunakan tab Perubahan terjadwal untuk melihat acara mendatang yang mungkin memengaruhi akun Anda. Peristiwa ini dapat mencakup aktivitas pemeliharaan terjadwal untuk layanan dan peristiwa siklus hidup terencana yang memerlukan tindakan untuk diselesaikan. Untuk membantu Anda merencanakan aktivitas ini, tampilan kalender disediakan sehingga Anda dapat memetakan perubahan terjadwal ini ke dalam kalender bulanan. Filter tersedia. Untuk informasi selengkapnya tentang peristiwa siklus hidup yang direncanakan, lihat. Acara siklus hidup yang direncanakan untuk AWS Health

Pemberitahuan lainnya

Gunakan tab Notifikasi untuk melihat semua notifikasi lain dan acara yang sedang berlangsung dari tujuh hari terakhir yang mungkin memengaruhi akun Anda. Ini dapat mencakup peristiwa, seperti rotasi sertifikat, pemberitahuan penagihan, dan kerentanan keamanan.

Log peristiwa

Gunakan tab log Peristiwa untuk melihat semua AWS Health peristiwa. Tabel log menyertakan kolom tambahan sehingga Anda dapat memfilter berdasarkan Status dan waktu Mulai.

Bila Anda memilih peristiwa di tabel log peristiwa, panel Detail akan muncul dengan informasi tentang peristiwa dan daftar sumber daya yang terpengaruh. Untuk informasi selengkapnya, lihat Detail acara.

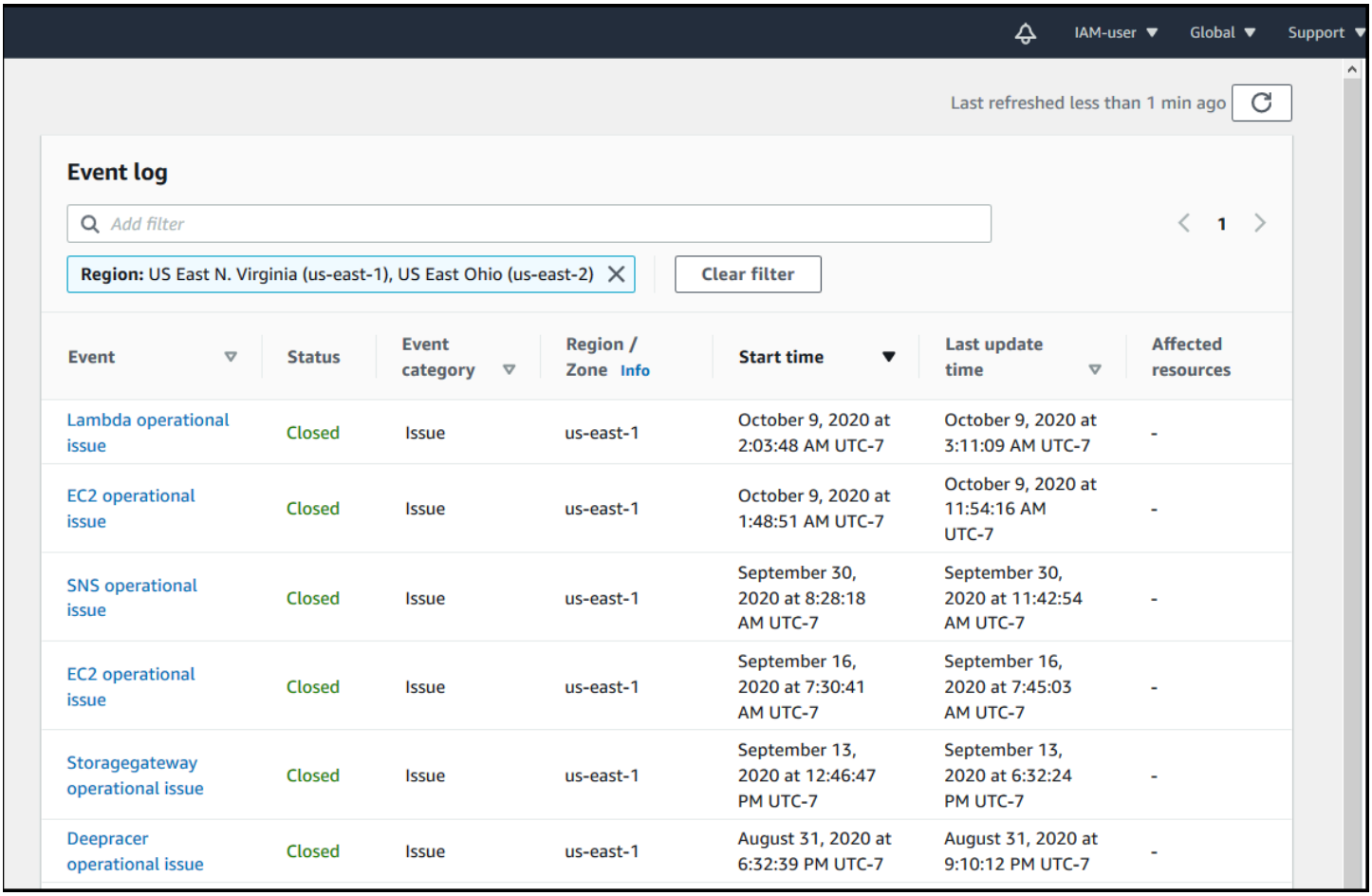
Anda dapat memilih opsi filter berikut untuk mempersempit hasil Anda:

- Availability Zone
- Waktu akhir
- Peristiwa
- Acara ARN
- Kategori acara
- Waktu pembaruan terakhir
- Wilayah
- ID Sumber Daya/ARN
- Layanan
- Waktu mulai

- Status

Example : Log Peristiwa

Gambar berikut menunjukkan peristiwa terbaru untuk Wilayah Timur AS (Virginia N.) dan Timur AS (Ohio).



Event	Status	Event category	Region / Zone Info	Start time	Last update time	Affected resources
Lambda operational issue	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
SNS operational issue	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
Storagegateway operational issue	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
Deepracer operational issue	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

Detail acara

Saat Anda memilih acara, dua tab muncul tentang acara tersebut. Tab Detail menampilkan informasi berikut:

- Layanan
- Status
- Wilayah atau Availability Zone
- Apakah acara tersebut spesifik akun atau tidak

- Waktu mulai dan berakhir
- Kategori
- Jumlah sumber daya yang terpengaruh
- Deskripsi dan garis waktu pembaruan tentang acara

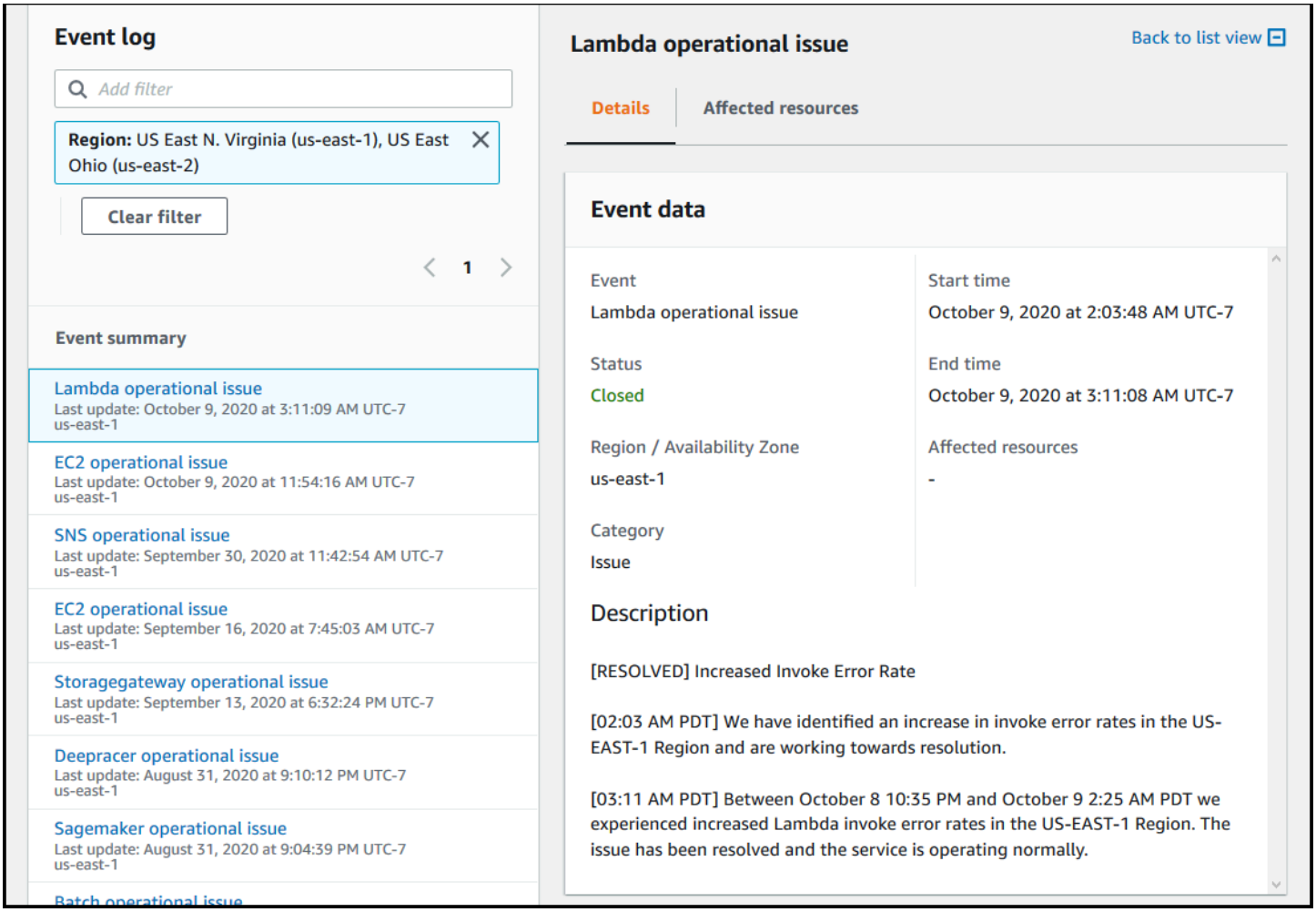
Tab Sumber daya yang terpengaruh menampilkan informasi berikut tentang AWS sumber daya apa pun yang terpengaruh oleh peristiwa:

- ID sumber daya (misalnya, ID volume Amazon EBS seperti `vol-a1b2c34f`) atau Amazon Resource Name (ARN), jika tersedia atau relevan.
- Untuk peristiwa siklus hidup yang direncanakan, daftar sumber daya yang terpengaruh ini juga berisi status sumber daya terbaru (Tertunda, Tidak Diketahui, atau Terselesaikan. Daftar ini biasanya menyegarkan setiap 24 jam sekali.

Anda dapat memfilter item yang muncul di sumber daya. Anda dapat mempersempit hasil Anda dengan ID sumber daya atau ARN.

Example : peristiwa AWS Health untuk AWS Lambda

Tangkapan layar berikut menunjukkan contoh acara untuk Lambda.



Tipe peristiwa

Ada dua jenis peristiwa AWS Health:

- Acara publik adalah acara layanan yang tidak spesifik untuk akun. Misalnya, jika ada masalah dengan Amazon EC2 di sebuahWilayah AWS, AWS Health berikan informasi tentang peristiwa tersebut, meskipun Anda tidak menggunakan layanan atau sumber daya di Wilayah tersebut.
- Acara khusus akun khusus untuk akun Anda atau akun di organisasi Anda. Misalnya, jika ada masalah dengan instans Amazon EC2 di Wilayah yang Anda gunakan, AWS Health berikan informasi tentang peristiwa dan daftar instans Amazon EC2 yang terpengaruh.

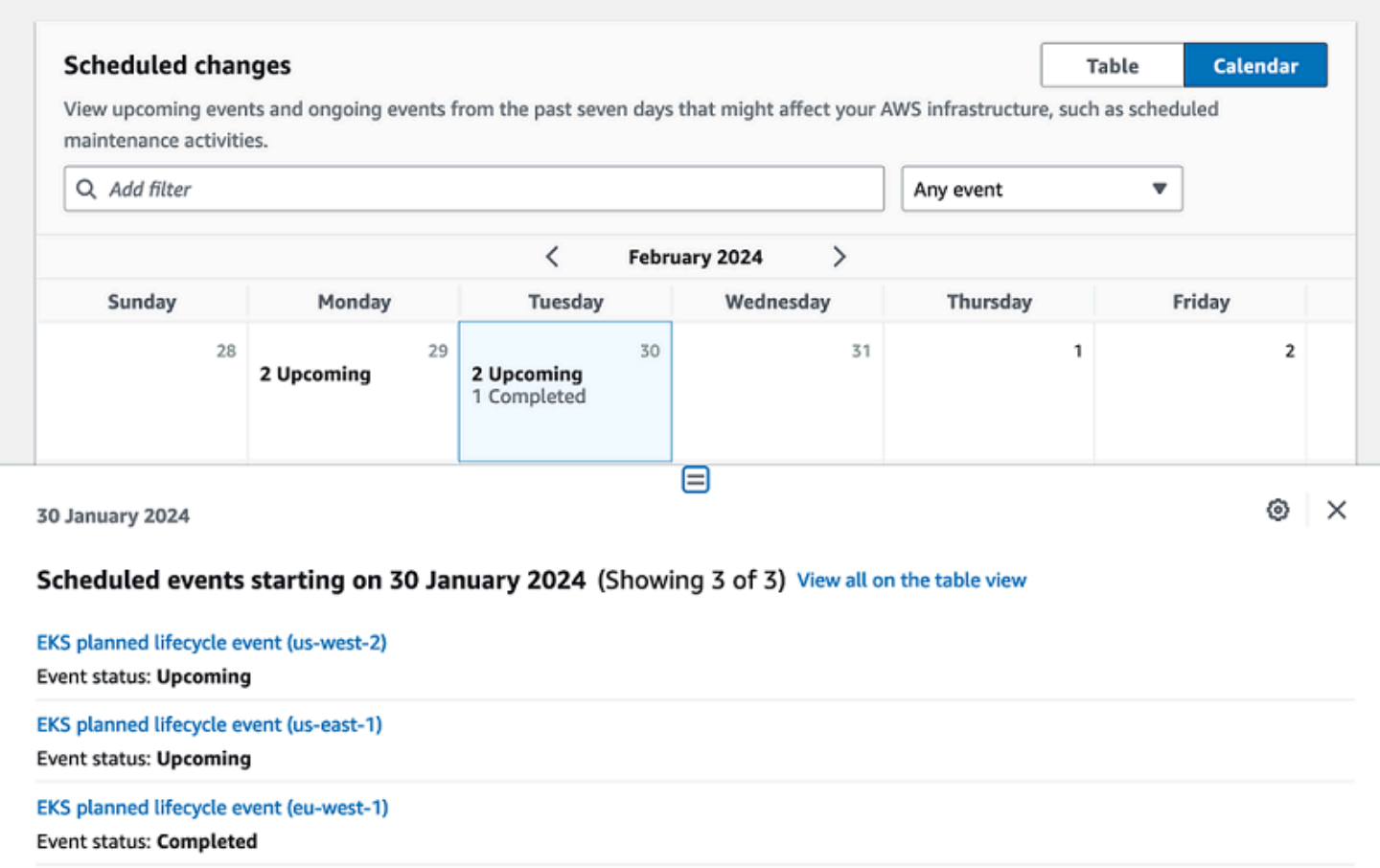
Anda dapat menggunakan opsi berikut untuk mengidentifikasi jika suatu peristiwa bersifat publik atau akun-spesifik:

- Di AWS Health Dasbor, pilih tab Sumber daya yang terpengaruh untuk suatu peristiwa. Peristiwa dengan sumber daya spesifik untuk akun Anda. Peristiwa tanpa sumber daya bersifat publik dan tidak spesifik untuk akun Anda. Untuk informasi selengkapnya, lihat Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.
- Gunakan API AWS Health untuk mengembalikan parameter `eventScopeCode`. Peristiwa dapat memiliki nilai `PUBLIC`, `ACCOUNT_SPECIFIC`, atau `NONE`. Untuk informasi selengkapnya, lihat DescribeEventDetailsoperasi di Referensi AWS Health API.

Tampilan kalender

Tampilan kalender tersedia di tab perubahan terjadwal untuk memproyeksikan AWS Health acara ke dalam kalender bulanan. Tampilan ini memungkinkan Anda untuk melihat perubahan terjadwal hingga 3 bulan ke masa lalu dan satu tahun ke depan.

AWS Healthacara ditampilkan berdasarkan tanggal. Pilih tanggal untuk menampilkan panel samping yang berisi rincian lebih lanjut tentang AWS Health acara tersebut. Acara mendatang dan yang sedang berlangsung ditampilkan dalam warna hitam. Acara yang sudah selesai ditampilkan dalam warna abu-abu. Jika ada lebih dari dua peristiwa dalam satu tanggal, hanya jumlah peristiwa hitam dan abu-abu yang ditampilkan. Pilih tanggal untuk menampilkan daftar AWS Health acara di panel samping. Anda dapat memilih acara di panel samping untuk menampilkan informasi tentang acara tersebut. Panel samping memiliki remah roti untuk menavigasi ke tampilan sebelumnya.



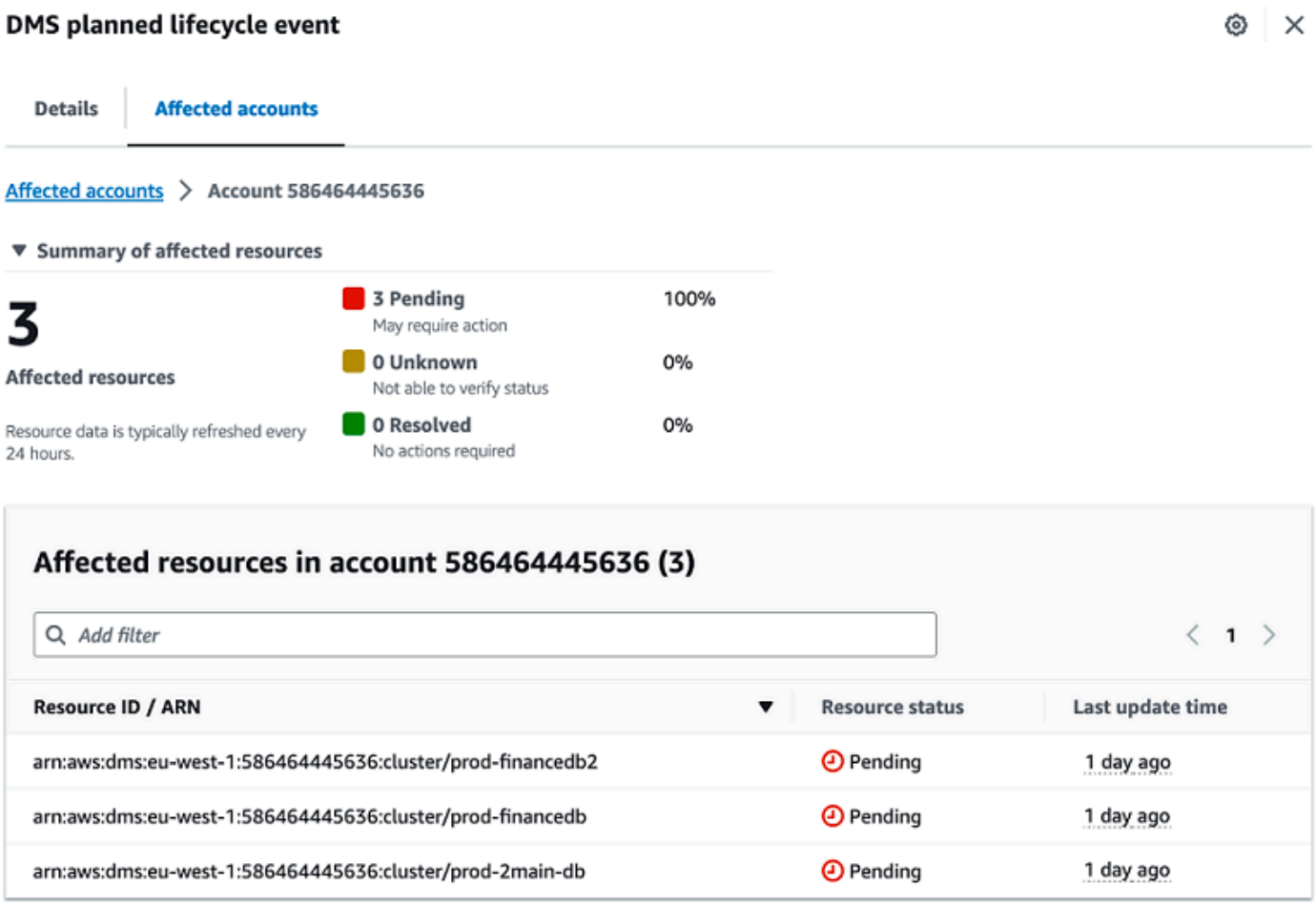
Tampilan sumber daya yang terpengaruh

Untuk peristiwa siklus hidup yang direncanakan, AWS Health acara biasanya menyediakan pembaruan harian status sumber daya yang terpengaruh. Untuk melihat status, pilih AWS Health acara. Status ditampilkan di tab sumber daya yang terpengaruh di panel samping.

AWS HealthPeristiwa tingkat akun menampilkan ringkasan status sumber daya yang terpengaruh di bagian atas tab sumber daya yang terpengaruh. Daftar sumber daya yang terpengaruh ditampilkan dalam tabel bersama dengan status yang sesuai. Peristiwa siklus hidup yang direncanakan adalah contoh jenis peristiwa yang menggunakan bidang status sumber daya. Untuk mempelajari lebih lanjut tentang peristiwa siklus hidup yang direncanakan, lihat. Acara siklus hidup yang direncanakan untuk AWS Health

Jika mengakses tampilan organisasi, AWS Health acara menampilkan ringkasan status semua sumber daya yang terpengaruh untuk semua akun yang disertakan. Berikut ringkasan adalah daftar akun yang terpengaruh dan jumlah sumber daya yang tertunda untuk akun itu. Pilih nomor akun atau

jumlah sumber daya yang tertunda untuk menampilkan ringkasan tampilan akun. Ringkasan tampilan akun memiliki remah roti untuk menavigasi kembali ke daftar organisasi akun yang terpengaruh. Ringkasan status sumber daya yang terpengaruh ditampilkan di bagian atas panel split.



Pengaturan zona waktu

Anda dapat melihat peristiwa di AWS Health Dasbor di zona waktu lokal Anda atau di UTC. Jika Anda mengubah zona waktu di AWS Health Dasbor, semua stempel waktu di dasbor dan acara publik akan diperbarui ke zona waktu yang Anda tentukan.

Untuk memperbarui pengaturan zona waktu

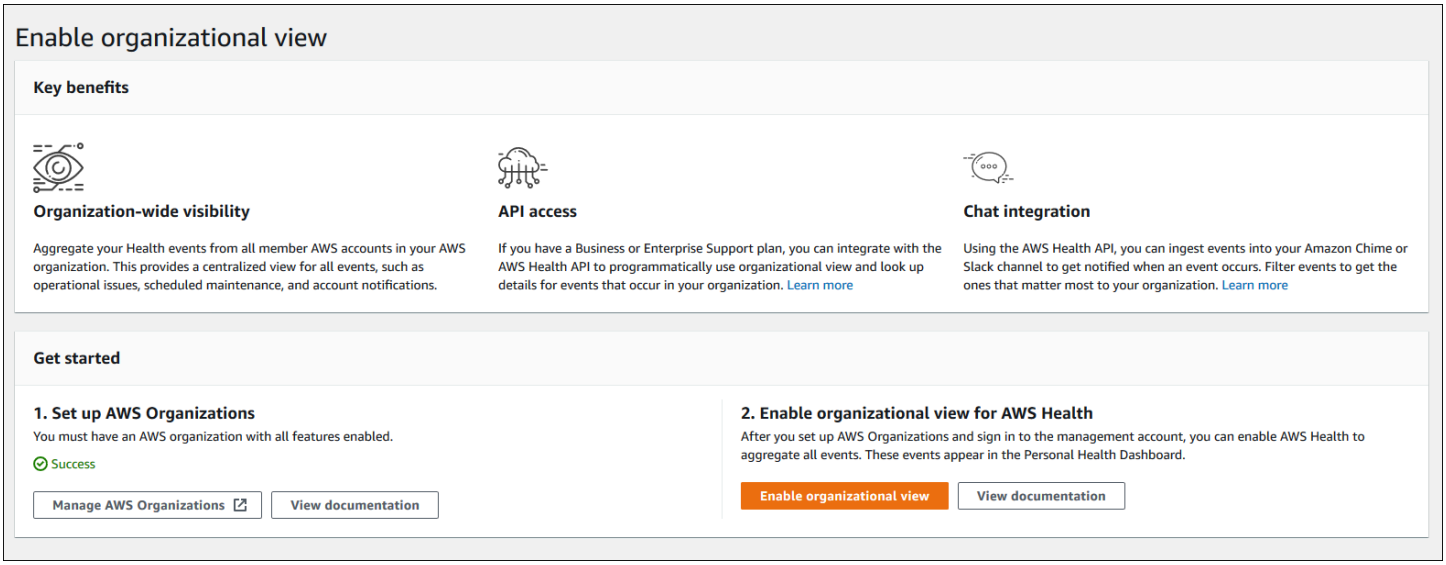
1. Buka AWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di bagian bawah halaman, pilih Preferensi cookie.
3. Pilih Diizinkan untuk cookie Fungsional. Kemudian pilih Simpan preferensi.

4. Di panel navigasi AWS Health Dasbor Anda, pilih Pengaturan zona waktu.
5. Pilih zona waktu untuk sesi AWS Health Dasbor Anda. Lalu pilih Simpan Perubahan.

Kesehatan organisasi Anda

AWS Health berintegrasi dengan AWS Organizations sehingga Anda dapat melihat acara untuk semua akun yang merupakan bagian dari organisasi Anda. Tindakan ini memberi Anda tampilan terpusat untuk peristiwa yang muncul di organisasi Anda. Anda dapat menggunakan peristiwa ini untuk memantau perubahan dalam sumber daya, layanan, dan aplikasi Anda.

Untuk informasi selengkapnya, lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.



Konfigurasikan Amazon EventBridge

Gunakan EventBridge untuk mendeteksi dan bereaksi terhadap perubahan untuk AWS Health peristiwa. Anda dapat memantau AWS Health peristiwa tertentu yang terjadi di akun Anda, dan kemudian mengatur aturan sehingga AWS Health memberi tahu Anda, atau Anda mengambil tindakan, ketika peristiwa berubah.

Gunakan EventBridge dengan AWS Health

1. Buka AWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Untuk menavigasi ke EventBridge konsol untuk membuat aturan, lakukan salah satu hal berikut:
   - Dari panel navigasi, di bawah Integrasi Kesehatan, pilih Amazon. EventBridge

- Di bawah Konfigurasi EventBridge, pilih Buka EventBridge.

3. Ikuti prosedur ini untuk membuat aturan dan memantau acara. Lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.

AWS HealthSadar

Anda dapat memulai dengan AWS Health API dengan menggunakan AWS HealthAware — aplikasi berbiaya rendah yang dapat Anda gunakan untuk mengirim acara kesehatan ke Slack, JIRA, ServiceNow dan banyak lagi. Webinar langsung tanpa biaya tersedia sekarang.

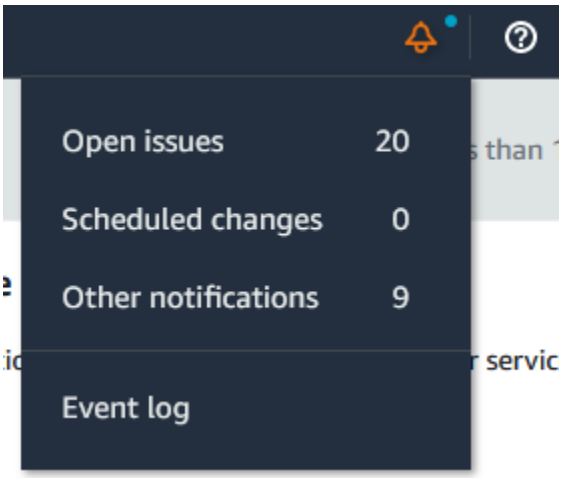
Pemberitahuan untuk peristiwa AWS Health

AWS HealthDasbor Anda memiliki ikon lonceng di bilah navigasi konsol dengan menu peringatan. Fitur ini menampilkan jumlah peristiwa AWS Health terkini yang muncul di dasbor di setiap kategori. Ikon lonceng ini muncul di beberapa AWS konsol, seperti untuk Amazon EC2, Amazon Relational Database Service (Amazon RDSAWS Identity and Access Management), (IAM), dan. AWS Trusted Advisor

Pilih ikon lonceng untuk melihat apakah peristiwa terbaru memengaruhi akun Anda. Anda kemudian dapat memilih acara untuk menavigasi ke AWS Health Dasbor Anda untuk informasi lebih lanjut.

Example : Buka acara

Gambar berikut menunjukkan acara terbuka dan pemberitahuan untuk akun.



KonfigurasikanAWSPemberitahuan Pengguna untukAWS Health

AWS Healthmemberikan informasi tentang operasi layanan, seperti masalah operasional, pemeliharaan terencana, dan peristiwa siklus hidup perangkat lunak yang direncanakan. Untuk visibilitas komprehensif keAWS Healthdetail peristiwa, seperti ID sumber daya yang terpengaruh, status saat ini (terbuka atau tertutup), dan status sumber daya, ini adalah praktik terbaik untuk digunakanAWS Healthtitik akhir, sepertiAWS HealthAPI, sumber aws.health di Amazon EventBridge, danAWS HealthDasbor. Titik akhir ini memberikan informasi paling rinci dan real-time tentang peristiwa yang sedang berlangsung dan perubahan yang mungkin memengaruhi beban kerja Anda.

AWSPemberitahuan Penggunamemberi tahu Anda melalui saluran UX tambahan (email, obrolan, atau pemberitahuan push keAWSAplikasi Seluler Konsol).AWS Healthpemberitahuan acara tidak mengandung data terperinci sebanyak titik akhir yang tercantum di atas; namun, mereka menyediakan cara yang sederhana dan efektif untuk memberi tahu pemangku kepentingan tentang masalah dan perubahan. Berdasarkan aturan yang Anda buat, Pemberitahuan Pengguna membuat dan mengirimkan pemberitahuan saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Anda dapat memilih saluran pengiriman UX mana pemberitahuan dikirim, dan mengatur agregasi untuk mengurangi jumlah notifikasi yang dihasilkan untuk acara tertentu. Pemberitahuan juga terlihat di Pusat Pemberitahuan Konsol. Misalnya, Anda dapat menerima pemberitahuan obrolan jika Anda memiliki sumber daya diAWSakun yang dijadwalkan untuk pembaruan, seperti instans Amazon Elastic Compute Cloud (Amazon EC2).

Untuk mempelajari lebih lanjut tentang pengaturanAWSPemberitahuan Pengguna, lihatMemulai denganAWSPemberitahuan Pengguna.

Mengakses API AWS Health

AWS Health adalah layanan web RESTful yang menggunakan HTTPS sebagai transportasi dan JSON sebagai format serialisasi pesan. Kode aplikasi Anda dapat membuat permintaan langsung ke API AWS Health. Bila Anda langsung menggunakan API REST, Anda harus menulis kode yang diperlukan untuk menandatangani dan autentikasi permintaan Anda. Untuk informasi lebih lanjut tentang operasi dan parameter AWS Health, lihatReferensi API AWS Health.

> **Note**
>
> Anda harus memiliki paket Business, Enterprise On-Ramp, atau Support Perusahaan AWS Supportuntuk menggunakanAWS Health API. Jika Anda memanggilAWS Health API dariAWS akun yang tidak memiliki rencana Support Bisnis, Korporasi, atau Korporasi, atau Korporasi, Anda menerima`SubscriptionRequiredException` galat.

Anda dapat menggunakan SDK AWS untuk merangkum panggilan API REST AWS Health, yang dapat menyederhanakan pengembangan aplikasi Anda. Anda menentukan kredensial AWS Anda, dan pustaka ini mengurus autentikasi dan meminta penandatanganan untuk Anda.

AWS Healthjuga menyediakanAWS Health Dashboard di yang dapat Anda gunakan untuk melihat dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwa dan mencari peristiwaAWS Management Console Lihat Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.

Titik akhir

API AWS Health mengikuti multi-Region application architecture dan memiliki dua titik akhir kewilayahan dalam konfigurasi aktif-pasif. Untuk mendukung failover DNS aktif-pasif, AWS Health menyediakan titik akhir tunggal, global. Anda dapat melakukan pencarian DNS pada titik akhir global untuk menentukan titik akhir aktif dan sesuai penandatanganan Wilayah AWS. Hal ini membantu Anda mengetahui titik akhir mana yang digunakan dalam kode Anda, sehingga Anda bisa mendapatkan informasi terbaru dari AWS Health.

Ketika Anda membuat permintaan ke titik akhir global, Anda harus menentukan akses kredensial AWS Anda ke titik akhir wilayah yang Anda targetkan dan mengkonfigurasi penandatanganan untuk

Wilayah Anda. Jika tidak, autentikasi Anda mungkin gagal. Untuk informasi selengkapnya, lihat Menandatangani permintaan API AWS Health.

Tabel berikut menggambarkan konfigurasi default.

Deskripsi	Penandatanganan Wilayah	Titik akhir	Protokol
Aktif	us-east-1	health.us-east-1.amazonaws.com	HTTPS
Pasif	us-east-2	health.us-east-2.amazonaws.com	HTTPS
Global	us-east-1 **Note** Ini adalah Wilayah penandatanganan titik akhir aktif saat ini.	global.health.amazonaws.com	HTTPS

Untuk menentukan apakah titik akhir adalah Titik akhir aktif, lakukan pencarian DNS pada Titik akhir global CNAME, kemudian ekstrak Wilayah AWS dari nama terselesaikan.

Example : Pencarian DNS pada titik akhir global

Perintah berikut melengkapi pencarian DNS pada titik akhir global.health.amazonaws.com. Perintah kemudian mengembalikan titik akhir Wilayah us-east-1. Output ini memberitahu Anda titik akhir mana yang harus Anda gunakan untuk AWS Health.

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

> **Tip**
>
> Kedua titik akhir aktif dan pasif mengembalikan data AWS Health. Namun, data terbaru AWS Health hanya tersedia dari titik akhir aktif. Data dari titik akhir pasif akhirnya akan konsisten dengan titik akhir aktif. Kami merekomendasikan Anda me-restart setiap alur kerja ketika titik akhir aktif berubah.

Menggunakan demo titik akhir ketersediaan tinggi

Dalam contoh kode berikut, AWS Health menggunakan pencarian DNS terhadap titik akhir global untuk menentukan titik akhir kewilayahan aktif dan penandatanganan Wilayah. Kemudian, kode me-restart alur kerja jika titik akhir aktif berubah.

Topik

Menggunakan demo Java

Prasyarat

Anda harus menginstal Gradle.

Untuk menggunakan contoh Java

1. Unduh demo endpoint ketersediaanAWS Health tinggi dari GitHub.
2. Arahkan ke proyek demo direktori `high-availability-endpoint/java`.
3. Dalam jendela baris perintah, masukkan perintah berikut.

```
gradle build
```

4. Masukkan perintah berikut untuk menentukan kredensial AWS Anda.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Masukkan perintah berikut untuk menjalankan demo.

```
gradle run
```

Example : output peristiwa AWS Health

Contoh kode tersebut mengembalikan peristiwa AWS Health terkini dalam tujuh hari terakhir di akun AWS Anda. Dalam contoh berikut, output mencakup peristiwa AWS Health untuk layanan AWS Config.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.
```

```
Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
```

```
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'

If you have any questions regarding this deprecation plan, please contact AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Sumber daya Java

- Untuk informasi selengkapnya, lihat Antarmuka HealthClient di ReferensiAWS SDK for Java API dan kode sumber.
- Untuk informasi lebih lanjut tentang pustaka yang digunakan dalam demo ini untuk pencarian DNS, lihat dnsjava di GitHub.

Menggunakan demo Python

Prasyarat

Anda harus menginstal Python 3.

Untuk menggunakan contoh Python

1. Unduh demo endpoint ketersediaanAWS Health tinggi dari GitHub.
2. Arahkan ke proyek demo direktori `high-availability-endpoint/python`.
3. Di jendela baris perintah, masukkan perintah berikut.

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Untuk Python 3.3 dan selanjutnya, Anda dapat menggunakan modul `venv` bawaan untuk menciptakan lingkungan virtual, bukan memasang `virtualenv`. Untuk informasi lebih lanjut, lihat venv - Penciptaan lingkungan virtual di situs web Python.
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. Masukkan perintah berikut untuk mengaktifkan lingkungan virtual.

```
source v-aws-health-env/bin/activate
```

5. Masukkan perintah berikut untuk menginstal dependensi.

```
pip install -r requirements.txt
```

6. Masukkan perintah berikut untuk menentukan kredensial AWS Anda.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Masukkan perintah berikut untuk menjalankan demo.

```
python3 main.py
```

Example : output peristiwa AWS Health

Contoh kode mengembalikan peristiwa AWS Health terkini dalam tujuh hari terakhir di akun AWS Anda. Output berikut mengembalikan peristiwa AWS Health untuk notifikasi keamanan AWS.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
```

```
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
```

```
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. Setelah selesai, masukkan perintah berikut untuk nonaktifkan mesin virtual.

```
deactivate
```

Sumber daya Python

- Untuk informasi lebih lanjut tentang `Health. Client`, lihat Referensi API AWS SDK for Python (Boto3).
- Untuk informasi lebih lanjut tentang pustaka yang digunakan dalam demo ini untuk pencarian DNS, lihat toolkit dnspython dan kode sumber daya di GitHub.

Menandatangani permintaan API AWS Health

Ketika Anda menggunakan SDK AWS atau AWS Command Line Interface (AWS CLI) untuk membuat permintaan ke AWS, alat-alat ini secara otomatis memasukkan permintaan untuk Anda dengan access key yang Anda tentukan saat mengonfigurasikan alatnya. Misalnya, jika Anda menggunakan AWS SDK for Java untuk demo titik akhir ketersediaan tinggi sebelumnya, Anda tidak perlu menandatangani permintaan sendiri.

Contoh kode Java

Untuk contoh lebih lanjut tentang cara menggunakan API AWS Health dengan AWS SDK for Java, lihat contoh kode ini.

Ketika Anda membuat permintaan, kami sangat menyarankan agar Anda tidak menggunakan kredensial akun root AWS Anda untuk akses reguler ke AWS Health. Anda dapat menggunakan kredensial untuk membuat pengguna IAM. Untuk informasi lebih lanjut, lihat Mengunci kunci akses pengguna akun root AWS di Panduan Pengguna IAM.

Jika Anda tidak menggunakan SDK AWS atau AWS CLI, maka Anda harus menandatangani permintaan Anda sendiri. Kami merekomendasi Anda menggunakan Tanda tangan AWS Versi 4. Untuk informasi selengkapnya, lihat Menandatangani Permintaan API AWS di Referensi Umum AWS.

Operasi yang didukung di AWS Health

AWS Health mendukung pengoperasian berikut untuk mendapatkan informasi tentang peristiwa yang mempengaruhi akun AWS Anda:

- Jenis peristiwa didukung oleh AWS Health.
- Informasi tentang satu atau lebih peristiwa yang sesuai kriteria filter yang ditentukan.
- Informasi tentang entitas yang dipengaruhi oleh satu atau lebih peristiwa.
- Jumlah peristiwa terkategori atau entitas yang sesuai kriteria filter yang ditentukan.

Semua pengoperasian adalah non-mutating. Artinya, mereka mengambil data namun tidak memodifikasinya. Bagian berikut meringkas pengoperasian AWS Health:

Jenis peristiwa

KlasterDescribeEventTypespengoperasian mengambil jenis peristiwa yang sesuai dengan filter tertentu opsional. Jenis peristiwa adalah definisi templat dari sebuah peristiwa layanan AWS, kode jenis peristiwa, dan kategori. Jenis peristiwa dan peristiwa mirip dengan kelas dan objek dalam pemrograman berorientasi objek. Nomor jenis peristiwa yang didukung oleh pertambahan AWS Health dari waktu ke waktu.

Kejadian

KlasterDescribeEventsmengambil informasi ringkasan tentang peristiwa yang berkaitan denganAWSakun. Peristiwa dapat dikaitkan dengan masalah operasional AWS, perubahan terjadwal untuk infrastruktur AWS, atau pemberitahuan keamanan dan penagihan. KlasterDescribeEventDetailsmengambil informasi rinci tentang satu atau lebih peristiwa, sepertiAWSlayanan, wilayah, Availability Zone, waktu awal dan akhir peristiwa, dan deskripsi teks.

Entitas terpengaruh

KlasterDescribeAffectedEntitiespengoperasian mengambil informasi tentang entitas yang dipengaruhi oleh satu atau lebih peristiwa. Hasil dapat difilter berdasarkan kriteria tambahan, seperti status, yang mungkin ditugaskan ke sumber daya AWS.

Agregasi

KlasterDescribeEventAggregatespengoperasian mengambil hitungan peristiwa di setiap kategori jenis peristiwa, secara opsional difilter berdasarkan kriteria lainnya.

KlasterDescribeEntityAggregatespengoperasian mengambil hitungan entitas (sumber daya) yang dipengaruhi oleh satu atau lebih peristiwa tertentu.

AWS Organizationsdan Tampilan Organisasi

DescribeEventsForOrganization

DescribeEventsForOrganizationmengembalikan informasi ringkasan tentang peristiwa di seluruh akunAWS Organizations, memenuhi kriteria filter yang ditentukan.

DescribeAffectedAccountsForOrganization

DescribeAffectedAccountsForOrganizationmengembalikan daftarAWSakun diAWS Organizationsyang dipengaruhi oleh acara yang disediakan.

DescribeEventDetailsForOrganization

DescribeEventDetailsForOrganizationmengembalikan informasi rinci tentang satu atau lebih peristiwa tertentu untuk satu atau lebih akun di akun diAWS Organizations.

DescribeAffectedEntitiesForOrganization

DescribeAffectedEntitiesForOrganizationmenampilkan daftar entitas yang telah dipengaruhi oleh satu atau lebih peristiwa untuk satu atau lebih akun di organisasi Anda, berdasarkan kriteria filter.

EnableHealthServiceAccessForOrganization

EnableHealthServiceAccessForOrganizationoperasi memberikanAWS Healthizin layanan untuk berinteraksiAWS Organizationsatas nama pelanggan dan menerapkan Peran Terkait Layanan ke akun manajemen di organisasi Anda.

DisableHealthServiceAccessForOrganization

DisableHealthServiceAccessForOrganizationoperasi mencabut izin untukAWS Healthlayanan untuk berinteraksiAWS Organizationsatas nama pelanggan.

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganizationpengoperasian menyediakan informasi status dalam mengaktifkan atau menonaktifkanAWS Healthuntuk bekerja dengan organisasi Anda

Untuk informasi selengkapnya tentang pengoperasian ini, lihat Referensi API AWS Health.

Contoh kode Java untuk API AWS Health

Contoh-contoh kode Java berikut ini menunjukkan cara menginisialisasi klien AWS Health dan mengambil informasi tentang peristiwa dan entitas.

Langkah 1: Inisialisasi Kredenisasi

Kredensial yang valid diperlukan untuk berkomunikasi dengan API AWS Health. Anda dapat menggunakan key pair dari setiap pengguna IAM terkait dengan akun AWS.

Buat dan inisialisasi AWSCredentials contoh:

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Langkah 2: InisialisasiAWS HealthKlien API

Menggunakan objek kredensial diinisialisasi dari langkah sebelumnya untuk membuat klien AWS Health:

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Langkah 3: GunakanAWS HealthOperasi API untuk mendapatkan informasi peristiwa

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
```

```
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);
```

```
// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;


DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
```

```
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Keamanan di AWS Health

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 Anda 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 menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Health, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Health. Topik berikut menunjukkan cara mengonfigurasi AWS Health untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Health sumber daya Anda.

Topik

Perlindungan data di AWS Health

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Health. Seperti yang dijelaskan dalam model AWS ini, 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. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). 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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

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 saat Anda bekerja dengan AWS Health 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

Lihat informasi berikut tentang cara AWS Health mengenkripsi data.

Enkripsi data mengacu pada perlindungan data saat dalam perjalanan (saat bepergian dari layanan ke AWS akun Anda), dan saat istirahat (saat disimpan dalam AWS layanan). Anda dapat melindungi data saat transit menggunakan Keamanan Lapisan Pengangkutan (TLS) atau saat istirahat menggunakan enkripsi di sisi klien.

AWS Health tidak mencatat informasi identifikasi pribadi (PII) seperti alamat email atau nama pelanggan dalam acara.

Enkripsi diam

Semua data yang disimpan oleh AWS Health dienkripsi saat istirahat.

Enkripsi bergerak

Semua data yang dikirim ke dan dari AWS Health dienkripsi dalam perjalanan.

Manajemen kunci

AWS Health tidak mendukung kunci enkripsi yang dikelola pelanggan untuk data yang dienkripsi di Cloud. AWS

Identity and access management untuk AWS Health

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Health IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Mengelola akses menggunakan kebijakan
- Bagaimana AWS Health bekerja dengan IAM
- AWS Health contoh kebijakan berbasis identitas
- Memecahkan masalah AWS Health identitas dan akses
- Menggunakan peran terkait layanan untuk AWS Health
- AWS kebijakan terkelola untuk AWS Health

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan. AWS Health

Pengguna layanan — Jika Anda menggunakan AWS Health layanan untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak AWS Health fitur untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS Health, lihat Memecahkan masalah AWS Health identitas dan akses.

Administrator layanan — Jika Anda bertanggung jawab atas AWS Health sumber daya di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Health. Tugas Anda adalah menentukan AWS Health fitur dan sumber daya mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM AWS Health, lihatBagaimana AWS Health bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS Health. Untuk melihat contoh kebijakan AWS Health berbasis identitas yang dapat Anda gunakan di IAM, lihat. AWS Health contoh kebijakan berbasis identitas

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

AWS pengguna root akun

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial

sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.

- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran

dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. 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 Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

AWS Health mendukung kondisi berbasis sumber daya. Anda dapat menentukan peristiwa AWS Health mana yang pengguna dapat lihat. Misalnya, Anda dapat membuat kebijakan yang hanya mengizinkan pengguna IAM mengakses ke peristiwa Amazon EC2 tertentu di AWS Health Dashboard.

Untuk informasi selengkapnya, lihat Sumber daya.

Daftar kontrol akses

Daftar kontrol akses (ACL) mengontrol prinsipal 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.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

AWS Health tidak mendukung ACL.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. 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 cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana AWS Health bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses AWS Health, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan. AWS Health Untuk mendapatkan tampilan tingkat tinggi

tentang cara AWS Health dan AWS layanan lain bekerja dengan IAM, lihat AWS Layanan yang Bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- AWS Health kebijakan berbasis identitas
- AWS Health Kebijakan berbasis sumber daya
- Otorisasi berdasarkan tanda AWS Health
- AWS Health Peran IAM

AWS Health kebijakan berbasis identitas

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi di mana tindakan tersebut diperbolehkan atau ditolak. AWS Health mendukung tindakan tertentu, sumber daya, dan kunci syarat. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan AWS Health menggunakan awalan berikut sebelum tindakan:`health:`. Misalnya, untuk memberikan izin kepada seseorang untuk melihat informasi terperinci tentang peristiwa tertentu dengan operasi API DescribeEventDetail, Anda menyertakan `heath:DescribeEventDetails` tindakan tersebut dalam kebijakan.

Pernyataan kebijakan harus mencakup `NotAction` elemen `Action` atau. AWS Health mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan tindakan dengan koma seperti berikut:

```
"Action": [
      "health:action1",
      "health:action2"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut.

```
"Action": "health:Describe*"
```

Untuk melihat daftar tindakan, lihat AWS Health Tindakan yang Ditentukan oleh AWS Health dalam Panduan Pengguna IAM.

Sumber daya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Sebuah AWS Health acara memiliki format Amazon Resource Name (ARN) berikut.

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Misalnya, untuk menentukan peristiwa `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` dalam pernyataan Anda, gunakan ARN berikut.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Untuk menentukan semua AWS Health peristiwa Amazon EC2 milik akun tertentu, gunakan wildcard (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Untuk informasi selengkapnya tentang format ARN, lihat Nama Sumber Daya Amazon (ARN) dan Ruang Nama AWS Layanan.

Beberapa AWS Health tindakan tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

AWS Health Operasi API dapat melibatkan banyak sumber daya. Misalnya, DescribeEventsoperasi mengembalikan informasi tentang peristiwa yang memenuhi kriteria filter tertentu. Ini berarti bahwa pengguna IAM harus memiliki izin untuk melihat peristiwa ini.

Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health hanya mendukung izin tingkat sumber daya untuk peristiwa kesehatan dan hanya untuk operasi API DescribeAffectedEntitas dan Detail. DescribeEvent Untuk informasi selengkapnya, lihat Sumber daya- dan syarat berbasis aksi.

Untuk melihat daftar jenis AWS Health sumber daya dan ARNnya, lihat Sumber Daya yang Ditentukan oleh AWS Health dalam Panduan Pengguna IAM. Untuk mempelajari tindakan mana yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang Ditentukan oleh AWS Health.

Kunci syarat

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. 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.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

AWS Health mendefinisikan kumpulan kunci kondisinya sendiri dan juga mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Operasi DescribeAffectedEntitas dan DescribeEventDetail API mendukung kunci `health:eventTypeCode` dan `health:service` kondisi.

Untuk melihat daftar kunci AWS Health kondisi, lihat Condition Keys untuk AWS Health di Panduan Pengguna IAM. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh AWS Health.

Contoh

Untuk melihat contoh kebijakan AWS Health berbasis identitas, lihat. AWS Health contoh kebijakan berbasis identitas

AWS Health Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada AWS Health sumber daya dan dalam kondisi apa.

AWS Health mendukung kebijakan izin berbasis sumber daya untuk acara kesehatan. Kebijakan berbasis sumber daya mengizinkan Anda memberikan izin penggunaan ke akun lain berdasarkan penggunaan sumber daya. Anda juga dapat menggunakan kebijakan berbasis sumber daya untuk mengizinkan AWS layanan mengakses acara Anda. AWS Health

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai prinsipal di kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berada di AWS akun yang berbeda, Anda juga harus memberikan izin entitas utama untuk mengakses sumber daya. Berikan izin dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi lebih lanjut, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya di Panduan Pengguna IAM.

AWS Health hanya mendukung kebijakan berbasis sumber daya untuk operasi API DescribeAffectedEntitas dan DescribeEvent Detail. Anda dapat menentukan tindakan ini dalam kebijakan untuk menentukan entitas utama (akun, pengguna, peran, dan pengguna gabungan) yang dapat melakukan tindakan pada AWS Health acara tersebut.

Contoh

Untuk melihat contoh kebijakan AWS Health berbasis sumber daya, lihat. Sumber daya- dan syarat berbasis aksi

Otorisasi berdasarkan tanda AWS Health

AWS Health tidak mendukung penandaan sumber daya atau mengontrol akses berdasarkan tag.

AWS Health Peran IAM

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensyal sementara dengan AWS Health

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau GetFederation Token.

AWS Health mendukung menggunakan kredensyal sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

AWS Health mendukung peran terkait layanan untuk diintegrasikan dengan. AWS Organizations Peran terkait layanan diberi nama. `AWSServiceRoleForHealth_Organizations` Terlampir pada peran tersebut adalah kebijakan yang OrganizationsService RolePolicy AWS dikelola Kesehatan_. Kebijakan AWS terkelola memungkinkan AWS Health untuk mengakses acara kesehatan dari AWS akun lain di organisasi.

Anda dapat menggunakan EnableHealthServiceAccessForOrganizationoperasi untuk membuat peran terkait layanan di akun. Namun, jika Anda ingin menonaktifkan fitur ini, Anda harus terlebih dahulu memanggil DisableHealthServiceAccessForOrganizationoperasi. Anda kemudian dapat menghapus peran melalui konsol IAM, IAM API, atau AWS Command Line Interface ()AWS CLI. Untuk informasi lebih lanjut, lihat Menggunakan peran terkait layanan dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

AWS Health tidak mendukung peran layanan.

AWS Health contoh kebijakan berbasis identitas

Secara default, pengguna dan IAM role tidak memiliki izin untuk membuat atau memodifikasi AWS Health sumber daya. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. Administrator IAM harus membuat kebijakan IAM yang

memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS Health
- Mengizinkan pengguna melihat izin mereka sendiri
- Mengakses AWS Health Dashboard dan API AWS Health
- Sumber daya- dan syarat berbasis aksi

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus AWS Health sumber daya di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS 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 ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS 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 IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

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

Menggunakan konsol AWS Health

Untuk mengakses AWS Health konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang AWS Health sumber daya di AWS akun Anda. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut masih dapat menggunakan AWS Health konsol, Anda dapat melampirkan kebijakan AWS terkelola berikut, AWSHealthFullAccess.

`AWSHealthFullAccess`Kebijakan ini memberikan entitas akses penuh ke hal-hal berikut:

- Mengaktifkan atau menonaktifkan fitur tampilan AWS Health organisasi untuk semua akun di AWS organisasi
- AWS Health Dashboard Di AWS Health konsol

- AWS Health Operasi dan notifikasi API
- Melihat informasi tentang akun yang merupakan bagian dari AWS organisasi Anda
- Lihat unit organisasi (OU) dari akun manajemen

Example : AWSHealthFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
```

```
        }
    ]
}
```

> **Note**
>
> Anda juga dapat menggunakan kebijakan `Health_OrganizationsServiceRolePolicy` AWS terkelola, sehingga AWS Health dapat melihat peristiwa untuk akun lain di organisasi Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Health.

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

Untuk informasi selengkapnya, lihat Menambahkan izin ke 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 menggunakan API atau secara terprogram. AWS CLI AWS

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

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

Mengakses AWS Health Dashboard dan API AWS Health

AWS Health Dashboard Ini tersedia untuk semua AWS akun. AWS Health API hanya tersedia untuk akun dengan paket Business, Enterprise On-Ramp, atau Enterprise Support. Untuk informasi selengkapnya, lihat AWS Support.

Anda dapat menggunakan IAM untuk membuat entitas (pengguna, grup, atau peran), dan kemudian memberikan izin entitas tersebut untuk mengakses AWS Health Dashboard dan API. AWS Health

Secara default, pengguna IAM tidak memiliki akses ke AWS Health Dashboard atau AWS Health API. Anda memberi pengguna akses ke AWS Health informasi akun Anda dengan melampirkan kebijakan IAM ke satu pengguna, sekelompok pengguna, atau peran. Untuk informasi lebih lanjut, lihat Identitas (Pengguna, Grup, dan Peran) dan Gambaran Umum Kebijakan IAM.

Setelah Anda membuat pengguna IAM, Anda dapat memberikan pengguna tersebut kata sandi individu. Kemudian, mereka dapat masuk ke akun Anda dan melihat AWS Health informasi dengan menggunakan halaman login khusus akun. Untuk informasi lebih lanjut, lihat Cara Pengguna Masuk ke Akun Anda.

> **Note**
>
> Pengguna IAM dengan izin untuk melihat AWS Health Dashboard memiliki akses hanya-baca ke informasi kesehatan di semua AWS layanan di akun, yang dapat mencakup, namun tidak

terbatas pada, ID AWS sumber daya seperti ID instans Amazon EC2, alamat IP instans EC2, dan pemberitahuan keamanan umum.
Misalnya, jika kebijakan IAM hanya memberikan akses ke AWS Health Dashboard dan AWS Health API, maka pengguna atau peran yang diterapkan kebijakan tersebut dapat mengakses semua informasi yang diposting tentang AWS layanan dan sumber daya terkait, meskipun kebijakan IAM lainnya tidak mengizinkan akses tersebut.

Anda dapat menggunakan dua grup API untuk AWS Health.

- Akun individual — Anda dapat menggunakan operasi seperti DescribeEventsdan DescribeEventDetail untuk mendapatkan informasi tentang AWS Health peristiwa untuk akun Anda.
- Akun organisasi — Anda dapat menggunakan operasi seperti DescribeEventsForOrganizationdan DescribeEventDetailsForOrganisasi untuk mendapatkan informasi tentang AWS Health peristiwa untuk akun yang merupakan bagian dari organisasi Anda.

Untuk informasi selengkapnya tentang pengoperasian API yang tersedia, lihat Referensi API AWS Health.

Tindakan individu

Anda dapat mengatur elemen `Action` kebijakan IAM untuk `health:Describe*`. Ini memungkinkan akses ke AWS Health Dashboard dan AWS Health. AWS Health mendukung kontrol akses ke acara berdasarkan `eventTypeCode` dan layanan.

Menjelaskan akses

Pernyataan kebijakan ini memberikan akses ke AWS Health Dashboard dan operasi `Describe*` AWS Health API apa pun. Misalnya, pengguna IAM dengan kebijakan ini dapat mengakses AWS Health Dashboard dalam AWS Management Console dan memanggil operasi AWS Health `DescribeEvents` API.

Example : Mendeskripsikan akses

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

```
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

Menolak akses

Pernyataan kebijakan ini menolak akses ke AWS Health Dashboard dan AWS Health API. Pengguna IAM dengan kebijakan ini tidak dapat melihat di AWS Health Dashboard dalam AWS Management Console dan tidak dapat memanggil operasi AWS Health API mana pun.

Example : Tolak akses

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

Tampilan organisasi

Jika Anda ingin mengaktifkan tampilan organisasi AWS Health, Anda harus mengizinkan akses ke AWS Health dan AWS Organizations tindakan.

Unsur `Action` kebijakan IAM harus mencakup izin berikut:

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`

- `organizations:ListParents`

Untuk memahami izin persis yang diperlukan untuk setiap API, lihat Tindakan yang Ditentukan oleh AWS Health API dan Pemberitahuan di Panduan Pengguna IAM.

> **Note**
>
> Anda harus menggunakan kredensi dari akun manajemen agar organisasi dapat mengakses AWS Health API. AWS Organizations Untuk informasi selengkapnya, lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.

Izinkan akses ke tampilan organisasi AWS Health

Pernyataan kebijakan ini memberikan akses ke semua AWS Health dan AWS Organizations tindakan yang Anda perlukan untuk fitur tampilan organisasi.

Example : Izinkan akses tampilan AWS Health organisasi

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

Menolak akses ke tampilan organisasi AWS Health

Pernyataan kebijakan ini menolak akses ke AWS Organizations tindakan tetapi memungkinkan akses ke AWS Health tindakan untuk akun individu.

Example : Tolak akses tampilan AWS Health organisasi

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
```

```
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

> **Note**
>
> Jika pengguna atau grup yang ingin Anda berikan izin sudah memiliki kebijakan IAM, Anda dapat menambahkan pernyataan kebijakan AWS Health-specific ke kebijakan tersebut.

Sumber daya- dan syarat berbasis aksi

AWS Health mendukung kondisi IAM untuk operasi API DescribeAffectedEntitiesdan DescribeEventDetail. Anda dapat menggunakan kondisi berbasis sumber daya dan tindakan untuk membatasi peristiwa yang dikirimkan AWS Health API ke pengguna, grup, atau peran.

Untuk melakukannya, perbarui blok kebijakan IAM `Condition` atau mengatur elemen `Resource`. Anda dapat menggunakan Ketentuan String untuk membatasi akses berdasarkan bidang AWS Health peristiwa tertentu.

Anda dapat menggunakan bidang berikut saat menentukan AWS Health peristiwa dalam kebijakan Anda:

- `eventTypeCode`
- `service`

> **Catatan**
>
> - Operasi API DescribeAffectedEntitiesdan DescribeEventDetails mendukung izin tingkat sumber daya. Misalnya, Anda dapat membuat kebijakan untuk mengizinkan atau tolak spesifik peristiwa AWS Health .
> - Operasi API DescribeAffectedEntitiesForOrganizationdan DescribeEventDetailsForOrganisasi tidak mendukung izin tingkat sumber daya.
> - Untuk informasi selengkapnya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Health API dan Pemberitahuan di Referensi Otorisasi Layanan.

Example : Syarat berbasis tindakan

Pernyataan kebijakan ini memberikan akses ke AWS Health Dashboard dan operasi AWS Health `Describe*` API, tetapi menolak akses ke AWS Health peristiwa apa pun yang terkait dengan Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example : Syarat berbasis sumber daya

Kebijakan berikut memiliki efek yang sama, tetapi menggunakan elemen `Resource` sebagai gantinya.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example : eventTypeCode kondisi

Pernyataan kebijakan ini memberikan akses ke AWS Health Dashboard dan operasi AWS Health `Describe*` API, tetapi menolak akses ke AWS Health peristiwa apa pun dengan `eventTypeCode` yang cocok. `AWS_EC2_*`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
```

```
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

> **Important**
>
> Jika Anda memanggil operasi DescribeAffectedEntitas dan DescribeEventDetail dan tidak memiliki izin untuk mengakses AWS Health acara, `AccessDeniedException` kesalahan akan muncul. Untuk informasi selengkapnya, lihat Memecahkan masalah AWS Health identitas dan akses.

Memecahkan masalah AWS Health identitas dan akses

Gunakan informasi berikut untuk mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Health dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Health
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin melihat access key saya
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses AWS Health
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Health sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AWS Health

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

`AccessDeniedException`Kesalahan muncul ketika pengguna tidak memiliki izin untuk menggunakan AWS Health Dashboard atau operasi AWS Health API.

Dalam kasus ini, administrator pengguna harus memperbarui kebijakan untuk memungkinkan akses pengguna.

AWS Health API memerlukan paket Business, Enterprise On-Ramp, atau Enterprise Support dari. AWS Support Jika Anda memanggil AWS Health API dari akun yang tidak memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support, kode galat berikut akan ditampilkan:. `SubscriptionRequiredException`

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran AWS Health.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut 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 tersebut untuk melakukan tindakan di AWS Health. 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 memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin melihat access key saya

Setelah membuat access key pengguna IAM, Anda dapat melihat access key ID Anda setiap saat. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> **Important**
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Dengan melakukan ini, Anda mungkin memberi seseorang akses permanen ke Anda Akun AWS.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan secret access key Anda, Anda harus menambahkan access key baru ke pengguna IAM Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola access keys di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses AWS Health

Untuk memungkinkan orang lain mengakses AWS Health, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Anda kemudian harus melampirkan kebijakan yang memberi mereka izin yang tepat di AWS Health.

Untuk segera memulai, lihat Membuat pengguna dan grup IAM pertama Anda yang didelegasikan di Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Health sumber daya saya

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 AWS Health mendukung fitur-fitur ini, lihatBagaimana AWS Health bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna 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 yang Akun AWS dimiliki oleh pihak ketiga dalam 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 Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

Menggunakan peran terkait layanan untuk AWS Health

AWS Health menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Health Peran terkait layanan telah ditentukan sebelumnya oleh AWS Health dan menyertakan semua izin yang diperlukan layanan untuk memanggil orang lain untuk Anda. Layanan AWS

Anda dapat menggunakan peran terkait layanan untuk mengatur AWS Health agar tidak menambahkan izin yang diperlukan secara manual. AWS Health mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Health dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Izin peran terkait layanan untuk AWS Health

AWS Health memiliki dua peran terkait layanan:

- AWSServiceRoleForHealth_Organizations— Peran ini mempercayai AWS Health (`health.amazonaws.com`) untuk mengambil peran untuk mengakses Layanan AWS untuk Anda. Terlampir pada peran ini adalah kebijakan yang `Health_OrganizationsServiceRolePolicy` AWS dikelola.

- AWSServiceRoleForHealth_EventProcessor— Peran ini mempercayai kepala AWS Health layanan (`event-processor.health.amazonaws.com`) untuk mengambil peran untuk Anda. Terlampir pada peran ini adalah kebijakan yang `AWSHealth_EventProcessorServiceRolePolicy` AWS dikelola. Prinsipal layanan menggunakan peran tersebut untuk membuat aturan EventBridge terkelola Amazon untuk Deteksi dan Respons AWS Insiden. Aturan ini adalah infrastruktur yang diperlukan dalam Anda Akun AWS untuk mengirimkan informasi perubahan status alarm dari akun Anda ke AWS Health.

Untuk informasi selengkapnya tentang kebijakan AWS terkelola, lihatAWS kebijakan terkelola untuk AWS Health.

Membuat peran terkait layanan untuk AWS Health

Anda tidak perlu membuat peran AWSServiceRoleForHealth_Organizations terkait layanan. Saat Anda memanggil EnableHealthServiceAccessForOrganizationoperasi, AWS Health buat peran terkait layanan ini di akun untuk Anda.

Anda harus secara manual membuat peran AWSServiceRoleForHealth_EventProcessor terkait layanan di akun Anda. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

Mengedit peran terkait layanan untuk AWS Health

AWS Health tidak memungkinkan Anda untuk mengedit peran terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Health

Untuk menghapus AWSServiceRoleForHealth_Organizations peran, Anda harus terlebih dahulu memanggil DisableHealthServiceAccessForOrganizationoperasi. Anda kemudian dapat menghapus peran melalui konsol IAM, IAM API, atau AWS Command Line Interface ()AWS CLI.

Untuk menghapus AWSServiceRoleForHealth_EventProcessor peran, hubungi AWS Support dan minta mereka melepaskan beban kerja Anda dari Deteksi dan Respons AWS Insiden. Setelah proses

ini selesai, Anda kemudian dapat menghapus salah satu peran melalui konsol IAM, IAM API, atau. AWS CLI

Informasi terkait

Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan dalam Panduan Pengguna IAM.

AWS kebijakan terkelola untuk AWS Health

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

AWS Health memiliki kebijakan terkelola berikut.

Daftar Isi

Kebijakan terkelola AWS : AWSHealth_EventProcessorServiceRolePolicy

AWS Health menggunakan kebijakan AWSHealth_EventProcessorServiceRolePolicy AWS terkelola. Kebijakan terkelola ini dilampirkan pada peran terkait layanan `AWSServiceRoleForHealth_EventProcessor`. Kebijakan ini memungkinkan peran terkait layanan untuk menyelesaikan tindakan untuk Anda. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Health.

Kebijakan terkelola memiliki izin berikut untuk mengizinkan mengakses EventBridge aturan Amazon AWS Health untuk Deteksi dan Respons AWS Insiden.

Detail izin

Kebijakan ini mencakup izin berikut.

- `events`— Menjelaskan dan menghapus EventBridge aturan, dan menjelaskan dan memperbarui target untuk aturan tersebut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Untuk daftar perubahan kebijakan, lihatAWS Health pembaruan kebijakan AWS terkelola.

Kebijakan terkelola AWS : Health_OrganizationsServiceRolePolicy

AWS Health menggunakan kebijakan Health_OrganizationsServiceRolePolicy AWS terkelola. Kebijakan terkelola ini dilampirkan pada peran terkait layanan `AWSServiceRoleForHealth_Organizations`. Kebijakan ini memungkinkan peran terkait layanan untuk menyelesaikan tindakan untuk Anda. Anda tidak dapat melampirkan kebijakan ini ke entitas IAM Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Health.

Kebijakan ini memberikan izin yang memungkinkan AWS Health untuk mengakses AWS Organizations detail yang diperlukan untuk tampilan Organisasi Kesehatan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations`— Menjelaskan akun di AWS Organizations dan Layanan AWS yang dapat digunakan dengan Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
```

```
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk daftar perubahan kebijakan, lihatAWS Health pembaruan kebijakan AWS terkelola.

Kebijakan terkelola AWS : AWSHealthFullAccess

AWS Health menggunakan kebijakan AWSHealthFullAccess AWS terkelola. Kebijakan ini memberi entitas (pengguna atau peran IAM) akses ke konsol. AWS Health Untuk informasi selengkapnya, lihat Menggunakan konsol AWS Health.

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations`— Mengaktifkan atau menonaktifkan fitur tampilan AWS Health organisasi untuk semua akun dalam AWS organisasi, dan melihat unit organisasi (OU) dari akun manajemen
- `health`— Akses ke operasi AWS Health API dan pemberitahuan
- `iam`— Membuat peran IAM yang ditautkan layanan AWS Health

```
{
    "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
```

```
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
                "Sid": "ServiceLinkAccess",
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

Untuk daftar perubahan kebijakan, lihatAWS Health pembaruan kebijakan AWS terkelola.

AWS Health pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Health sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman Riwayat dokumen untuk AWS Health.

Tabel berikut menjelaskan pembaruan penting pada kebijakan AWS Health terkelola sejak 13 Januari 2022.

AWS Health

Perubahan	Deskripsi	Tanggal
Kebijakan terkelola AWS : AWSHealthFullAccess - Pembaruan ke kebijakan yang tersedia	AWS Health telah memperluas AWSHealthFullAccess kebijakan ke AWS GovCloud (US) Regions dan Wilayah China.	16 Oktober 2023
Kebijakan terkelola AWS : Health_OrganizationsServiceRolePolicy - Pembaruan ke kebijakan yang tersedia	AWS Health menambahkan AWS Organizations tindakan baru untuk memungkinkan peran terkait layanan untuk menggambarkan akun dan AWS layanan yang dapat digunakan. AWS Organizations	Juli 19, 2023
Ubah log diterbitkan	Ubah log untuk kebijakan AWS Health terkelola.	13 Januari 2023

Penebangan dan pemantauan di AWS Health

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Health dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton AWS Health, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda 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 CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon Elastic Compute Cloud (Amazon EC2) dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

- Amazon EventBridge memberikan near-real-time aliran peristiwa sistem yang menggambarkan perubahan AWS sumber daya. EventBridge memungkinkan komputasi berbasis peristiwa otomatis. Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Untuk informasi selengkapnya, lihat Pemantauan AWS Health.

Validasi kepatuhan untuk AWS Health

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Health

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

AWS Health peristiwa disimpan dan direplikasi di beberapa Availability Zone. Pendekatan ini memastikan bahwa Anda dapat mengaksesnya dari AWS Health Dashboard atau operasi AWS Health API. Anda dapat melihat AWS Health peristiwa hingga 90 hari sejak peristiwa itu terjadi.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur dalam AWS Health

Sebagai layanan terkelola, AWS Health dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper Amazon Web Services: Tinjauan Proses Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Health melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Analisis konfigurasi dan kerentanan di AWS Health

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi selengkapnya, lihat model tanggung jawab AWS bersama.

Praktik terbaik keamanan untuk AWS Health

Lihat praktik terbaik berikut untuk bekerja dengan AWS Health.

Berikan izin minimum kepada AWS Health pengguna

Ikuti prinsip hak istimewa paling sedikit dengan menggunakan seperangkat izin kebijakan akses minimum untuk pengguna dan grup Anda. Misalnya, Anda mungkin mengizinkan akses pengguna AWS Identity and Access Management (IAM) ke file. AWS Health Dashboard Namun, Anda mungkin

tidak mengizinkan pengguna yang sama untuk mengaktifkan atau nonaktifkan akses ke AWS Organizations.

Untuk informasi selengkapnya, lihat AWS Health contoh kebijakan berbasis identitas.

Lihat AWS Health Dashboard

Periksa AWS Health Dashboard sesering mungkin untuk mengidentifikasi peristiwa yang mungkin memengaruhi akun atau aplikasi Anda. Misalnya, Anda mungkin menerima notifikasi peristiwa tentang sumber daya Anda, seperti Instans Amazon Elastic Compute Cloud (Amazon EC2) yang perlu diperbarui.

Untuk informasi selengkapnya, lihat Memulai AWS Health Dashboard Anda — Kesehatan akun Anda.

Integrasikan AWS Health dengan Amazon Chime atau Slack

Anda dapat mengintegrasikan AWS Health dengan alat obrolan Anda. Integrasi ini memungkinkan Anda dan tim Anda mendapatkan pemberitahuan tentang AWS Health peristiwa secara real time. Untuk informasi selengkapnya, lihat AWS Health Alat di GitHub.

Monitor untuk AWS Health acara

Anda dapat berintegrasi AWS Health dengan Amazon CloudWatch Events, sehingga Anda dapat membuat aturan untuk acara tertentu. Saat CloudWatch Acara mendeteksi peristiwa yang cocok dengan aturan Anda, Anda akan diberi tahu dan kemudian dapat mengambil tindakan. CloudWatch Acara acara bersifat khusus Wilayah, jadi Anda harus mengonfigurasi layanan ini di Wilayah tempat aplikasi atau infrastruktur Anda berada.

Dalam beberapa kasus, Wilayah untuk AWS Health acara tidak dapat ditentukan. Jika situasi itu terjadi, secara default kejadian muncul di Wilayah US East (N. Virginia). Anda dapat mengatur CloudWatch Acara di Wilayah ini untuk memastikan bahwa Anda memantau peristiwa ini.

Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.

Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi

Secara default, Anda dapat menggunakan AWS Health untuk melihat peristiwa AWS Health dalam satu akun AWS. Jika Anda menggunakan AWS Organizations, Anda juga dapat melihat peristiwa AWS Health terpusat di seluruh organisasi Anda. Fitur ini menyediakan akses ke informasi yang sama sebagai operasi akun tunggal. Anda dapat menggunakan filter untuk melihat peristiwa di spesifik Wilayah, rekening, dan layanan AWS.

Anda dapat menggabungkan peristiwa untuk mengidentifikasi akun di organisasi Anda yang terpengaruh oleh peristiwa operasional atau mendapatkan pemberitahuan untuk kerentanan keamanan. Kemudian Anda dapat menggunakan informasi ini untuk mengelola dan mengotomatisasi peristiwa pemeliharaan sumber daya secara proaktif di organisasi Anda. Gunakan fitur ini untuk tetap mengetahui perubahan yang akan datang ke layanan AWS yang mungkin memerlukan pembaruan atau perubahan kode.

Ini adalah praktik terbaik untuk menggunakanAdministrator yang Didelegasikanfitur untuk mendelegasikan akses keAWS HealthPandangan organisasi ke akun anggota. Hal ini memudahkan tim operasional untuk mengaksesAWS Healthperistiwa di organisasi Anda. Fitur Delegasi Administrator memungkinkan Anda untuk menjaga akun manajemen Anda dibatasi, sambil memberikan tim dengan visibilitas yang mereka butuhkan untuk bertindakAWS Healthperistiwa.

Important

- AWS Health tidak merekam peristiwa yang terjadi di organisasi Anda sebelum Anda mengaktifkan tampilan organisasi. Misalnya, jika akun anggota (111122223333) di organisasi Anda menerima peristiwa untuk Amazon Elastic Compute Cloud (Amazon EC2) sebelum Anda mengaktifkan fitur ini, peristiwa tidak akan muncul dalam tampilan organisasi Anda.
- AWS Health peristiwa yang dikirim untuk akun di organisasi Anda akan muncul dalam tampilan organisasi selama peristiwa tersedia, hingga 90 hari, meskipun satu atau beberapa akun tersebut keluar dari organisasi Anda.
- Peristiwa organisasi tersedia selama 90 hari sebelum dihapus. Kuota ini tidak dapat ditingkatkan.

Prasyarat

Sebelum Anda menggunakan tampilan organisasi, Anda harus:

- Jadilah bagian dari organisasi dengan semua fitur diaktifkan.
- Masuk ke akun manajemen sebagai pengguna AWS Identity and Access Management (IAM) atau ambil IAM role.

  Anda juga dapat masuk sebagai root user (tidak disarankan) di akun manajemen organisasi Anda. Untuk informasi lebih lanjut, lihat Kunci akses akun AWS root user Anda dalam Panduan Pengguna IAM.
- Jika Anda masuk sebagai pengguna IAM, gunakan kebijakan IAM yang memberikan akses keAWS Healthdan tindakan Organisasi, sepertiAWSHealthFullAccesskebijakan. Untuk informasi selengkapnya, lihat AWS Health contoh kebijakan berbasis identitas.

Topik

Tampilan organisasi (konsol)

Anda dapat menggunakan konsol AWS Health tersebut untuk mendapatkan tampilan terpusat untuk kondisi kesehatan di organisasi AWS Anda.

Tampilan organisasi tersedia di konsol AWS Health tersebut untuk semua rencana AWS Support tanpa biaya tambahan.

> **Note**
>
> Jika Anda ingin mengizinkan pengguna mengakses fitur ini di akun manajemen, mereka harus memiliki izin seperti AWSHealthFullAccesskebijakan tersebut. Untuk informasi selengkapnya, lihat AWS Health contoh kebijakan berbasis identitas.

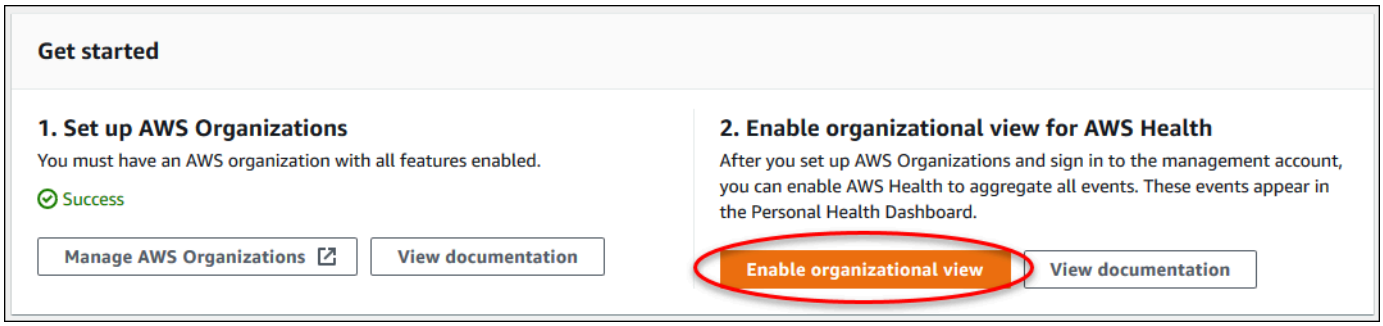
Daftar Isi

Mengaktifkan tampilan organisasi (konsol)

Anda dapat mengaktifkan tampilan organisasi dari konsol AWS Health. Anda harus masuk ke akun manajemen organisasi AWS Anda.

Untuk melihatAWS Health Dasbor organisasi Anda

1. BukaAWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Konfigurasi.
3. Pada halaman Aktifkan tampilan organisasi, pilih Aktifkan tampilan organisasi.



4. (Opsional) Jika Anda ingin membuat perubahan pada organisasi AWS Anda, seperti membuat unit organisasi (UO), pilih Kelola AWS Organizations.

   Untuk informasi lebih lanjut, lihat Memulai dengan AWS Organizations dalam Panduan Pengguna AWS Organizations.

Catatan

- Mengaktifkan fitur ini adalah proses asinkron dan membutuhkan waktu untuk menyelesaikannya. Tergantung pada jumlah akun di organisasi Anda, perlu beberapa menit untuk memuat akun. Anda dapat pergi dan memeriksa konsol AWS Health tersebut kemudian.
- Jika Anda memiliki rencana Support Bisnis, Korporasi Korporasi, atau Korporasi Korporasi Korporasi DescribeHealthServiceStatusForOrganizationAPI untuk memeriksa status proses tersebut.
- Ketika Anda mengaktifkan fitur ini, peran yang`AWSServiceRoleForHealth_Organizations` terkait layanan dengan kebijakan`Health_OrganizationsServiceRolePolicy`AWS terkelola diterapkan ke akun manajemen di organisasi. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk AWS Health.

Melihat peristiwa tampilan organisasi (konsol)

Setelah Anda mengaktifkan tampilan organisasi, AWS Health menampilkan kondisi kesehatan untuk semua akun di organisasi Anda.

Saat akun bergabung dengan organisasi Anda, AWS Health secara otomatis menambahkan akun ke tampilan organisasi. Bila akun meninggalkan organisasi Anda, peristiwa baru dari akun tersebut tidak lagi masuk ke tampilan organisasi. Namun, peristiwa yang ada tetap dan Anda masih bisa kueri hingga batas 90 hari.

AWS mempertahankan data kebijakan untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Di akhir periode 90 hari, AWS menghapus semua data kebijakan untuk akun secara permanen.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan di bucket S3.
- Selama AWS mempertahankan data kebijakan, saat Anda membuka kembali akun yang tertutup, AWS menetapkan ulang akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun.
- Untuk informasi selengkapnya, lihat Menutup akun.

> **Important**
>
> Untuk pelanggan di Wilayah AWS GovCloud (US):
>
> - Sebelum menutup akun Anda, cadangkan, lalu hapus sumber daya akun Anda sebelum menutup akun Anda, cadangkan, lalu hapus sumber daya akun Anda. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

> **Note**
>
> Ketika Anda mengaktifkan fitur ini,AWS Health konsol tersebut dapat menampilkan peristiwa publik dari AWS HealthDasbor — Kesehatan layanan selama 7 hari terakhir. Peristiwa publik ini tidak spesifik untuk akun di organisasi Anda. Peristiwa dariAWS Health Dasbor — Layanan kesehatan memberikan informasi publik tentang ketersediaan kewilayahan dariAWS layanan.

Anda dapat melihat organisasi tampilan organisasi di halaman berikut:.

Topik

Terbuka dan masalah terbaru

Anda dapat menggunakan tab Buka dan masalah terbaru untuk melihat peristiwa yang mungkin memengaruhiAWS infrastruktur, seperti perubahanLayanan AWS dan sumber daya yang memengaruhi organisasi Anda.

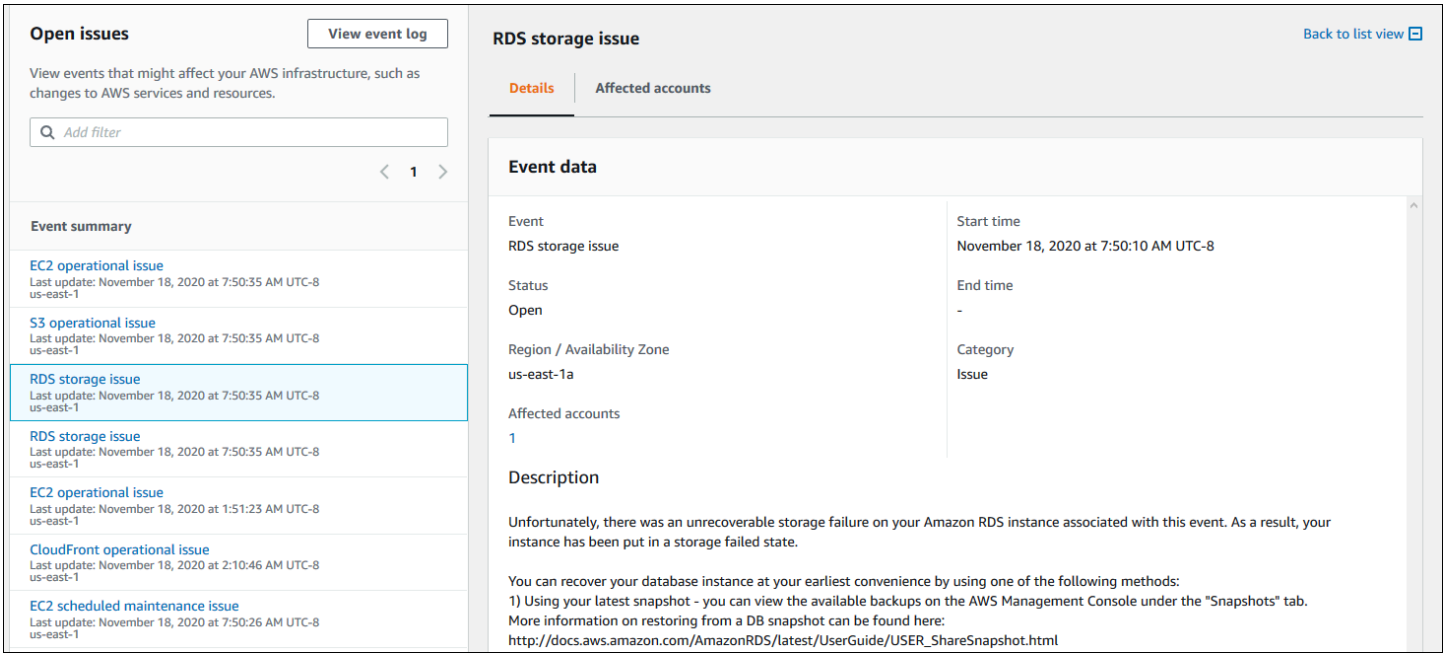
Untuk melihat organisasi tampilan organisasi organisasi tampilan organisasi di organisasi tampilan organisasi di organisasi.

1. BukaAWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.

2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Buka dan masalah terbaru untuk melihat peristiwa yang baru dilaporkan.
3. Pilih acara. Pada tab Rincian, Anda dapat meninjau informasi berikut tentang peristiwa:
    - Nama peristiwa
    - Status
    - Wilayah atau Availability Zone
    - Akun yang terpengaruh
    - Waktu mulai
    - Waktu akhir
    - Kategori
    - Deskripsi

Example : Membuka masalah untuk tampilan organisasi terbuka untuk tampilan organisasi: Membuka masalah organisasi terbuka

Peristiwa Amazon Relational Database Service (Amazon RDS) berikut muncul di tab Buka dan masalah organisasi untuk tampilan organisasi dan memengaruhi satu akun di organisasi.



Perubahan terjadwal

Gunakan tab Perubahan terjadwal untuk melihat peristiwa mendatang yang mungkin memengaruhi organisasi Anda. Acara ini dapat mencakup kegiatan pemeliharaan terjadwal untuk layanan.

notifikasi lainnya

Gunakan tab Notifikasi untuk melihat semua notifikasi lain dan peristiwa yang sedang berlangsung dari tujuh hari terakhir yang mungkin memengaruhi organisasi Anda. Ini dapat mencakup peristiwa, seperti rotasi sertifikat, pemberitahuan penagihan, dan kerentanan keamanan.

Log peristiwa

Anda juga dapat menggunakan tab Log peristiwa log peristiwa untuk melihatAWS Health peristiwa untuk tampilan organisasi. Tata letak dan perilaku kolom mirip dengan tab Buka dan masalah terbaru, kecuali bahwa tab Log peristiwa menyertakan kolom tambahan dan opsi filter, seperti kategori Acara, Status, dan Waktu mulai.

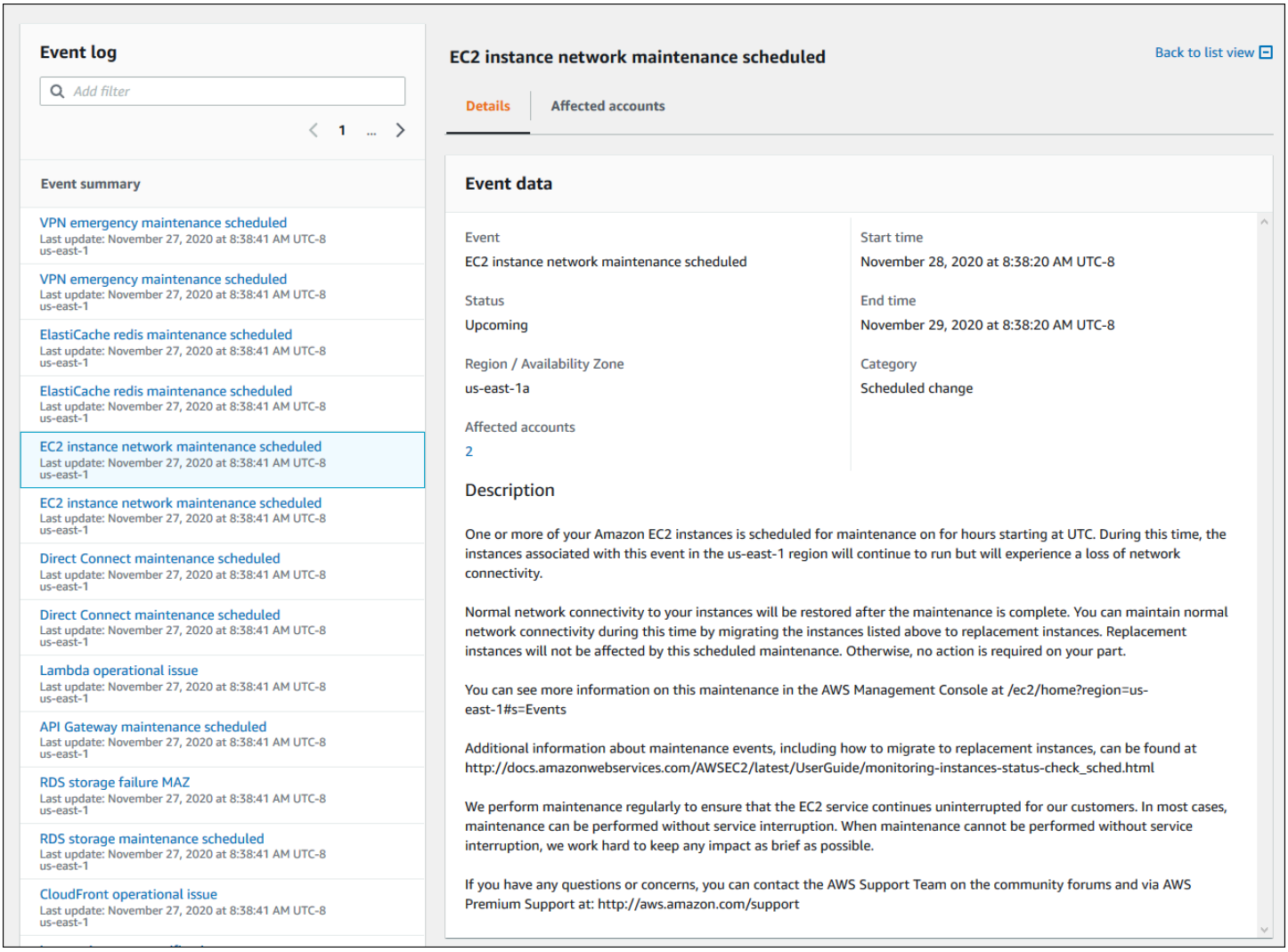
Untuk melihat organisasi di tab Log peristiwa tampilan organisasi di tab Log peristiwa tampilan organisasi di tab Log peristiwa tampilan organisasi di tab Log peristiwa

1. BukaAWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Log peristiwa.
3. Di bawah Log peristiwa, pilih nama peristiwa. Anda dapat meninjau informasi berikut tentang peristiwa:

   - Nama peristiwa
   - Status
   - Wilayah atau Availability Zone
   - Akun yang terpengaruh
   - Waktu mulai
   - Waktu akhir
   - Kategori
   - Deskripsi

Example : Tab log peristiwa untuk tampilan organisasi: tab log peristiwa untuk tampilan organisasi: Tab log peristiwa untuk

Contoh berikut peristiwa Amazon DynamoDB (DynamoDB) berikut muncul di tab Log peristiwa dan memengaruhi dua akun di organisasi.

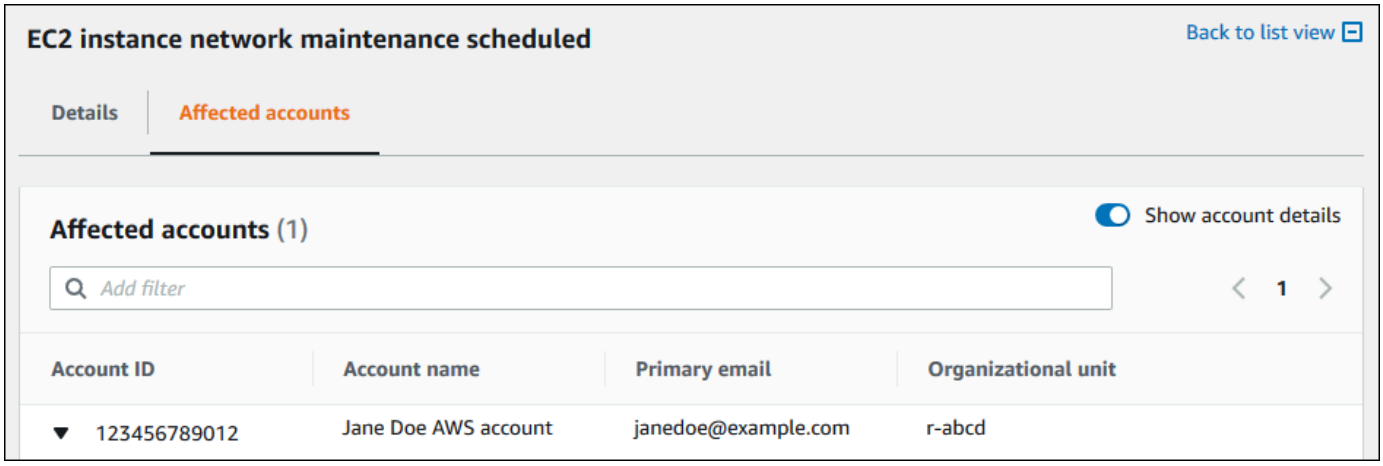


Melihat akun dan sumber daya yang terpengaruh (konsol)

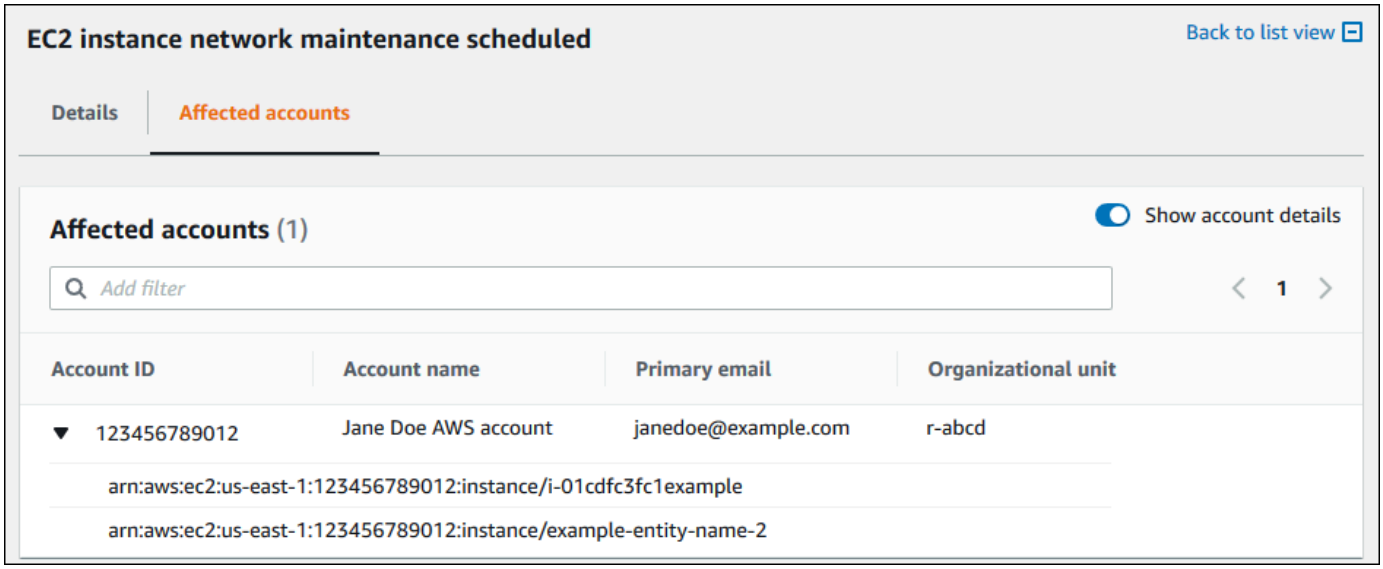
Di bawah kesehatan organisasi Anda, Anda dapat melihat akun di organisasi Anda yang terpengaruh oleh peristiwa dan sumber daya terkait. Sebagai contoh, jika ada acara mendatang untuk pemeliharaan instans Amazon Elastic Compute Cloud (Amazon EC2), akun di organisasi Anda yang memiliki instans Amazon EC2 dapat muncul di tab Detail. Anda dapat mengidentifikasi sumber daya tertentu dan kemudian kontak pemilik akun.

Untuk melihat akun dan sumber daya yang terpengaruh

1. BukaAWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih salah satu tab tersebut.
3. Pilih peristiwa yang memiliki nilai untuk akun yang terkena dampak.
4. Pilih tab Akun yang terpengaruh.
5. Pilih Tampilkan detail akun untuk melihat informasi berikut untuk akun:
   - ID Akun
   - Nama akun
   - Email utama
   - Unit organisasi (OU)



6. Perluas akun untuk melihat sumber daya yang terpengaruh.



7. Jika ada lebih dari 10 sumber daya, pilih Lihat semua sumber daya untuk melihat mereka.
8. Untuk memfilter menurut ID akun untuk peristiwa tertentu ini, lakukan hal berikut:
   a. Pada tab Akun yang terpengaruh, pilih Tambahkan filter, pilih ID Akun, lalu masukkan ID akun. Anda hanya dapat memasukkan satu ID akun pada satu waktu.
   b. Pilih Terapkan. Akun yang Anda masukkan akan muncul dalam daftar.

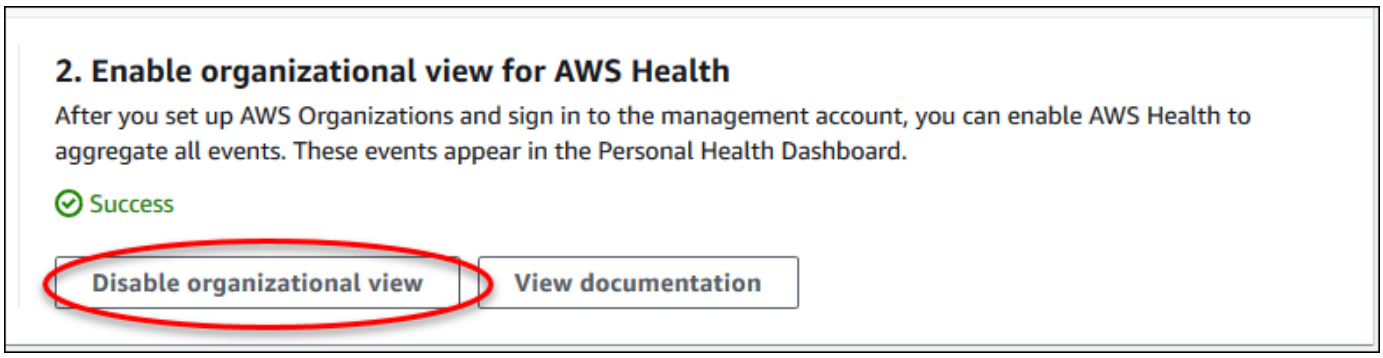
Nonaktifkan tampilan organisasi (konsol)

Jika tidak ingin menggabungkan peristiwa untuk organisasi, Anda dapat nonaktifkan fitur ini dari akun manajemen.

AWS Health berhenti menggabungkan peristiwa untuk semua akun lain di organisasi Anda. Anda dapat terus melihat peristiwa sebelumnya dari organisasi Anda hingga peristiwa dihapus.

Untuk nonaktifkan tampilan organisasi

1. BukaAWS Health Dasbor Anda di https://health.aws.amazon.com/health/home.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Konfigurasi.
3. Pada halaman Aktifkan tampilan organisasi, pilih Nonaktifkan tampilan organisasi.



Setelah Anda mematikan fitur ini, AWS Health tidak lagi menggabungkan peristiwa dari organisasi Anda. Namun, peran terkait layanan tetap ada di akun manajemen hingga Anda menghapusnya melalui AWS Identity and Access Management (IAM) konsol, API IAM, atau AWS Command Line Interface (AWS CLI). Untuk informasi lebih lanjut, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Tampilan organisasi (CLI)

Anda juga dapat mengaktifkan fitur tampilan organisasi melalui AWS Command Line Interface (AWS CLI) dari pada konsol AWS Health tersebut. Untuk menggunakan konsol tersebut, lihat Mengaktifkan tampilan organisasi (konsol).

> **Note**
>
> Jika Anda ingin mengizinkan pengguna mengakses akun manajemen untuk fitur tampilan organisasi, mereka harus memiliki izin sepertiAWSHealthFullAccesskebijakan. Untuk informasi selengkapnya, lihat AWS Health contoh kebijakan berbasis identitas.

Daftar Isi

Mengaktifkan tampilan organisasi (CLI)

Anda dapat mengaktifkan tampilan organisasi dengan menggunakanEnableHealthServiceAccessForOrganizationOperasi API.

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) atau kode Anda sendiri untuk memanggil operasi ini.

> **Note**
>
> - Anda harus memilikiBisnis,Perusahaan On-Ramp, atauEnterpriseRencana dukungan untuk memanggilAWS HealthAPI.
> - Anda harus menggunakan titik akhir Wilayah US East (N. Virginia).

Example

Perintah AWS CLI berikut memungkinkan fitur ini dari akun AWS Anda. Anda dapat menggunakan perintah ini dari akun manajemen atau dari akun yang dapat mengambil peran dengan izin yang dibutuhkan.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

Contoh kode berikut memanggilEnableHealthServiceAccessForOrganizationOperasi API.

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Anda dapat menggunakan SDK AWS untuk versi Java 2.0 untuk contoh berikut.

```
import software.amazon.awssdk.services.health.HealthClient;
```

```
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );
```

```
            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
        }
    }
}
```

Untuk informasi selengkapnya, lihat Panduan Developer AWS SDK for Java 2.0.

Ketika Anda mengaktifkan fitur ini,`AWSServiceRoleForHealth_Organizations` peran terkait layanandengan`Health_OrganizationsServiceRolePolicy` AWSkebijakan yang dikelola diterapkan ke akun manajemen dalam organisasi.

> **Note**
>
> Mengaktifkan fitur ini adalah proses asinkron dan membutuhkan waktu untuk menyelesaikannya. Anda dapat menghubungiDescribeHealthServiceStatusForOrganizationoperasi untuk memeriksa status proses.

Melihat peristiwa tampilan organisasi (CLI)

Setelah Anda mengaktifkan fitur ini, AWS Health mulai mencatat peristiwa yang memengaruhi akun dalam organisasi. Saat akun bergabung dengan organisasi Anda, AWS Health secara otomatis menambahkan akun ke tampilan organisasi.

> **Note**
>
> AWS Health tidak merekam peristiwa yang terjadi di organisasi Anda sebelum Anda mengaktifkan tampilan organisasi.

Bila akun meninggalkan organisasi Anda, peristiwa baru dari akun tersebut tidak lagi masuk ke tampilan organisasi. Namun, peristiwa yang ada tetap dan Anda masih bisa kueri hingga batas 90 hari.

AWS mempertahankan data kebijakan untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Di akhir periode 90 hari, AWS menghapus semua data kebijakan untuk akun secara permanen.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom denganEventBridgeaturan untuk menyimpan temuan dalam ember S3.
- Selama AWS mempertahankan data kebijakan, saat Anda membuka kembali akun yang tertutup, AWS menetapkan ulang akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun.
- Untuk informasi lebih lanjut, lihatMenutup akun.

> **Important**
>
> Untuk pelanggan di Wilayah AWS GovCloud (US):
>
> - Sebelum menutup akun, cadangkan dan kemudian hapus sumber daya akun. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

Anda dapat menggunakan operasi API AWS Health untuk mengembalikan peristiwa dari tampilan organisasi.

Example : Menjelaskan peristiwa tampilan organisasi

Perintah AWS CLI berikut mengembalikan peristiwa kesehatan untuk akun AWS di organisasi Anda.

```
aws health describe-events-for-organization --region us-east-1
```

Lihat bagian berikut untuk operasi API AWS Health lain.

Nonaktifkan tampilan organisasi (CLI)

Anda dapat menonaktifkan tampilan organisasi dengan menggunakanDisableHealthServiceAccessForOrganizationOperasi API.

Example

Perintah AWS CLI berikut menonaktifkan fitur ini dari akun Anda.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> Anda juga dapat menonaktifkan fitur organisasi dengan menggunakan OrganisasiNonaktifkanAWSServiceAccessOperasi API. Setelah Anda memanggil operasi ini, AWS Health berhenti menggabungkan peristiwa untuk semua akun lain di organisasi Anda. Jika Anda memanggil operasi API AWS Health untuk tampilan organisasi, AWS Health mengembalikan kesalahan. AWS Health berlanjut mengumpulkan peristiwa kesehatan untuk akun AWS Anda.

Setelah Anda menonaktifkan fitur ini, AWS Health tidak lagi mengumpulkan acara dari organisasi Anda. Namun, peran yang berkaitan dengan layanan tetap ada di akun manajemen hingga Anda menghapusnya melalui konsol AWS Identity and Access Management (IAM), API IAM, atau AWS CLI. Untuk informasi lebih lanjut, lihat Menghapus Peran terkait layanan dalam Panduan Pengguna IAM.

Tampilan organisasi AWS Health operasi API

Anda dapat menggunakan berikut operasi API AWS Health untuk tampilan organisasi:

- DescribeEventsForOrganization- Mengembalikan informasi ringkasan tentang peristiwa di seluruh organisasi.
- DescribeAffectedAccountsForOrganization- Mengembalikan daftarAWSakun dalam organisasi yang dipengaruhi oleh peristiwa yang ditentukan.
- DescribeEventDetailsForOrganization- Mengembalikan informasi rinci tentang peristiwa yang ditentukan untuk satu atau lebih akun dalam organisasi.
- DescribeAffectedEntitiesForOrganization- Mengembalikan daftar entitas yang telah dipengaruhi oleh satu atau lebih peristiwa untuk satu atau lebih akun dalam suatu organisasi.

Anda dapat menggunakan operasi berikut untuk mengaktifkan atau nonaktifkan AWS Health dari bekerja dengan Organisasi:

- EnableHealthServiceAccessForOrganization— HibahAWS Healthizin untuk berinteraksi dengan Organisasi dan menerapkan SLR ke akun manajemen di organisasi.
- DisableHealthServiceAccessForOrganization- Mencabut izin untukAWS Healthuntuk berinteraksi dengan Organisasi.
- DescribeHealthServiceStatusForOrganization- Mengembalikan informasi status tentang apakahAWS Healthdiaktifkan untuk organisasi Anda.

Anda harus memiliki paket Business, Enterprise On-Ramp, atau Enterprise Support untuk memanggil operasi API ini. Jika Anda memanggil operasi `DescribeEventForOrganization` dan `DescribeAffectedAccountsForOrganization` dari akun yang memiliki setidaknya rencana dukungan Bisnis, Anda dapat mengembalikan informasi tentang akun apa pun di organisasi, terlepas dari tingkat dukungan akun individual. Lihat contoh-contoh berikut.

Example Contoh: Organisasi dengan akun yang memiliki rencana dukungan Bisnis dan Developer

- Anda memiliki tiga akun di organisasi Anda. Akun manajemen memiliki rencana dukungan Bisnis dan dua akun lainnya memiliki rencana dukungan Developer.
- Anda memanggil operasi API `DescribeEventForOrganization` dari akun manajemen atau dari akun yang dapat mengambil peran dengan izin yang diperlukan.
- AWS Health mengembalikan informasi untuk ketiga akun.

Jika Anda meneleponDescribeEventDetailsForOrganizationdanDescribeAffectedEntitiesForOrganiz API dari akun yang memiliki setidaknya paket dukungan Bisnis, Anda hanya dapat mengembalikan informasi tentang akun di organisasi yang memiliki paket Dukungan Bisnis, Perusahaan On-Ramp, atau Perusahaan.

Example Contoh: Organisasi dengan akun yang memiliki paket Dukungan Perusahaan, Bisnis, dan Pengembang

- Anda memiliki lima akun di organisasi Anda. Akun manajemen memiliki rencana dukungan Korporasi, dua akun memiliki rencana dukungan Bisnis, dan dua akun memiliki rencana dukungan Developer.
- Anda memanggil operasi API `DescribeEventDetailsForOrganization` dari akun manajemen.

- AWS Health mengembalikan informasi hanya untuk akun yang memiliki rencana dukungan Korporasi atau Bisnis. Akun yang memiliki rencana dukungan Developer muncul di tanggapan `failedSet`.

Tampilan organisasi administrator yang didelegasikan

DenganAWS Health, Anda dapat memanfaatkan fitur administrator yang didelegasikan dariAWS Organizationsyang memungkinkan akun selain akun manajemen untuk melihat agregatAWS Healthperistiwa diAWS HealthDasboratau pemrograman melaluiAWS HealthAPI. Fitur administrator yang didelegasikan memberikan fleksibilitas bagi tim yang berbeda untuk melihat dan mengelola acara kesehatan di seluruh organisasi Anda. Ini adalahAWSpraktik terbaik keamanan untuk mendelegasikan tanggung jawab di luar akun manajemen jika memungkinkan.

Daftar Isi

Daftarkan administrator yang didelegasikan untuk tampilan organisasi Anda

Setelah mengaktifkan tampilan organisasi untuk organisasi, Anda dapat mendaftarkan hingga lima akun anggota di organisasi sebagai administrator yang didelegasikan. Untuk melakukan ini, hubungiRegisterDelegatedAdministratorOperasi API. Setelah Anda mendaftarkan akun anggota, mereka didelegasikan mengelola akun dan dapat mengaksesAWS Healthpandangan organisasi dariAWS HealthDasbor. Jika akun memilikiBisnis,Perusahaan On-Ramp, atauEnterpriseRencana dukungan, maka administrator yang didelegasikan dapat menggunakanAWS HealthAPI untuk mengaksesAWS Healthpandangan organisasi.

Untuk membuat administrator yang didelegasikan, dari akun manajemen di organisasi Anda, hubungi yang berikutAWS Command Line Interface(AWS CLI) perintah. Anda dapat menggunakan perintah ini dari akun manajemen atau dari akun yang dapat mengambil peran dengan yang diperlukanAWS Identity and Access Managementizin. Dalam contoh perintah berikut, gantiACCOUNT_IDdengan ID akun anggota yang ingin Anda daftarkan bersama denganAWS Healthlayanan utama “health.amazonaws.com”.

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Setelah administrator yang didelegasikan terdaftar, Anda memiliki visibilitas ke semuaAWS Healthperistiwa yang memengaruhi akun di seluruh organisasi Anda. Anda dapat melihat peristiwa historis selama 90 hari terakhir atau sejak fitur tampilan organisasi pertama kali diaktifkan, mana saja yang lebih baru. Perhatikan bahwa mengaktifkan fitur administrator yang didelegasikan adalah proses asinkron dan membutuhkan waktu hingga satu menit untuk menyelesaikannya.

Menghapus administrator yang didelegasikan dari tampilan organisasi

Untuk menghapus akses administrator yang didelegasikan, hubungiDeregisterDelegatedAdministratorOperasi API.

Dari akun manajemen organisasi Anda, hubungi yang berikutAWS CLIperintah untuk menghapus akun anggota sebagai administrator didelegasikan. Dalam contoh perintah berikut, gantiACCOUNT_IDdengan ID akun anggota yang ingin Anda hapus.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Memantau AWS Health peristiwa dengan Amazon EventBridge

Anda dapat menggunakan Amazon EventBridge untuk mendeteksi dan bereaksi terhadap AWS Health peristiwa. Kemudian, berdasarkan aturan yang Anda buat, EventBridge memanggil satu atau beberapa tindakan target saat peristiwa cocok dengan nilai yang Anda tentukan dalam aturan. Bergantung pada jenis acara, Anda dapat menangkap informasi acara, memulai acara tambahan, mengirim pemberitahuan, mengambil tindakan korektif, atau melakukan tindakan lain. Misalnya, Anda dapat menggunakan AWS Health untuk menerima pemberitahuan email jika Anda memiliki AWS sumber daya Akun AWS yang dijadwalkan untuk pembaruan, seperti instans Amazon Elastic Compute Cloud (Amazon EC2).

> **Catatan**
>
> - AWS Health memberikan acara atas dasar upaya terbaik. Acara tidak selalu dijamin akan dikirimkan ke EventBridge.
> - EventBridge Aturan apa pun yang Anda buat hanya dapat menerima pemberitahuan untuk Anda Akun AWS. Untuk menerima acara organisasi untuk akun lain di dalam akun Anda AWS Organizations, silakan lihat Mengagregasi AWS Health acara menggunakan tampilan organisasi dan akses administrator yang didelegasikan.

Anda dapat memilih di antara beberapa jenis target EventBridge sebagai bagian dari AWS Health alur kerja Anda, termasuk:

- AWS Lambda fungsi
- Amazon Kinesis Data Streams
- Antrean Amazon Simple Queue Service (Amazon SQS)
- Target bawaan (seperti tindakan CloudWatch alarm)
- Topik Amazon Simple Notification Service (Amazon SNS)

Sebagai contoh, Anda dapat menggunakan fungsi Lambda untuk menyampaikan notifikasi ke saluran Slack ketika peristiwa AWS Health terjadi. Atau, Anda dapat menggunakan Lambda dan EventBridge

mengirim pemberitahuan teks atau SMS khusus dengan Amazon SNS ketika AWS Health suatu peristiwa terjadi.

Untuk contoh otomatisasi dan peringatan khusus yang dapat Anda buat sebagai respons terhadap AWS Health peristiwa, lihat AWS Health Alat di GitHub.

Topik

Tentang Wilayah AWS untuk AWS Health

Anda harus membuat EventBridge aturan untuk setiap Wilayah tempat Anda ingin menerima AWS Health acara. Jika Anda tidak membuat aturan, Anda tidak akan menerima peristiwa. Sebagai contoh, untuk menerima peristiwa dari Wilayah US West (Oregon), Anda harus membuat aturan untuk Wilayah ini.

Menyiapkan aturan tambahan di Wilayah cadangan menambahkan lapisan ketahanan ekstra ke alur kerja Anda, jika aturan utama Anda dipengaruhi oleh peristiwa yang sedang berlangsung. Acara publik untuk AWS Health dikirim secara bersamaan ke Wilayah yang terkena dampak dan ke Wilayah cadangan. Lihat Tentang acara publik untuk AWS Health untuk informasi selengkapnya. Untuk semua Wilayah di partisi AWS standar, Anda dapat mengatur aturan di US West (Oregon) sebagai cadangan untuk terus menerima acara meskipun Wilayah utama Anda dipengaruhi oleh masalah yang sedang berlangsung. Wilayah cadangan untuk Wilayah Barat AS (Oregon) adalah Wilayah AS Timur (Virginia N.).

Misalnya, jika Anda memantau peristiwa di Wilayah Eropa (Frankfurt) dan Wilayah tersebut untuk sementara tidak tersedia, maka juga AWS Health akan mengirimkan acara tersebut ke Wilayah Barat AS (Oregon). Selanjutnya, EventBridge aturan cadangan Anda mengirimkan acara ke target yang Anda tentukan. Untuk membuat aturan cadangan, ikuti prosedur di bawah ini untuk Membuat EventBridge aturan untuk AWS Health dan gunakan Wilayah AS Barat (Oregon).

Beberapa AWS Health acara tidak spesifik Wilayah. Peristiwa yang tidak spesifik untuk suatu Wilayah disebut peristiwa global. Ini termasuk acara yang dikirim untuk AWS Identity and Access Management (IAM). Untuk menerima acara global, Anda harus membuat aturan untuk Wilayah AS Timur (Virginia N.) untuk Wilayah utama dan Wilayah Barat AS (Oregon) sebagai Wilayah cadangan.

Untuk menerima acara global di AWS GovCloud (US), Anda harus membuat aturan di Wilayah AWS GovCloud (AS-Barat).

Tentang acara publik untuk AWS Health

Saat Anda membuat EventBridge aturan untuk memantau peristiwa AWS Health, aturan akan memberikan acara khusus akun dan acara publik:

- Peristiwa khusus akun memengaruhi akun dan sumber daya Anda, seperti peristiwa yang memberi tahu Anda tentang pembaruan yang diperlukan untuk instans Amazon EC2 atau peristiwa perubahan terjadwal lainnya.
- Acara publik muncul di AWS Health Dasbor — Kesehatan layanan. Acara publik tidak spesifik untuk Akun AWS dan memberikan informasi publik tentang ketersediaan layanan Regional.

> **Important**
>
> Untuk menerima kedua jenis acara, aturan Anda harus menggunakan `"source": [ "aws.health"]` nilainya. Wildcard, seperti `"source": [ "aws.health*"]` tidak akan cocok dengan pola untuk memantau peristiwa apa pun.

Jika Anda memantau acara publik dari sebuah Wilayah AWS, kami sarankan Anda membuat aturan cadangan. Acara publik untuk AWS Health dikirim secara bersamaan ke Wilayah yang terkena dampak dan ke Wilayah cadangan. Disarankan agar Anda menghapus duplikat AWS Health peristiwa menggunakan EventArn dan CommunicationId karena ini tetap konsisten untuk AWS Health pesan yang dikirim ke Wilayah cadangan.

Anda dapat mengidentifikasi apakah suatu peristiwa bersifat publik atau khusus akun EventBridge, dengan menggunakan parameter. eventScopeCode Acara dapat memiliki `PUBLIC` atau`ACCOUNT_SPECIFIC`. Anda juga dapat memfilter aturan Anda pada parameter ini.

Contoh: Acara publik untuk Amazon Elastic Compute Cloud

Acara berikut menunjukkan masalah operasional untuk Amazon EC2 di Wilayah AS Timur (Virginia N.).


```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [
            {
                "latestDescription": "We are investigating increased API Error rates
 and Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
                "language": "en_US"
            }
        ],
        "page": "1",
        "totalPages": "1",
        "affectedAccount":"123456789012",

    }
}
```

Prosesor acara untuk AWS Health

Jika Anda menggunakan Deteksi dan Respons AWS Insiden untuk akun Anda, maka Anda harus menginstal peran `AWSServiceRoleForHealth_EventProcessor` terkait layanan di akun Anda.

Peran ini mempercayai kepala `event-processor.health.amazonaws.com` layanan untuk mengambil peran tersebut. Terlampir pada peran ini adalah kebijakan yang `AWSHealth_EventProcessorServiceRolePolicy` AWS dikelola. Kebijakan ini mencantumkan izin yang dapat dilakukan peran, seperti memanggil orang lain Layanan AWS untuk Anda.

Peran ini kemudian membuat aturan EventBridge terkelola Amazon di akun Anda. Aturannya dinamai`AWSHealthEventProcessor-DO-NOT-DELETE`. Aturan ini adalah infrastruktur yang diperlukan untuk akun Anda sehingga EventBridge dapat mengirimkan informasi perubahan status alarm dari akun Anda ke akun Anda AWS Health.

Informasi terkait

Untuk mempelajari lebih lanjut, lihat topik berikut:

- Menggunakan peran terkait layanan untuk AWS Health
- Kebijakan terkelola AWS : AWSHealth_EventProcessorServiceRolePolicy

Membuat EventBridge aturan untuk AWS Health

Anda dapat membuat EventBridge aturan untuk mendapatkan pemberitahuan untuk AWS Health acara di akun Anda. Sebelum Anda membuat aturan acara untuk AWS Health, lakukan hal berikut:

- Biasakan diri Anda dengan acara, aturan, dan target di EventBridge. Untuk informasi selengkapnya, lihat Apa itu Amazon EventBridge? di Panduan EventBridge Pengguna Amazon dan Baru EventBridge — Lacak dan Tanggapi Perubahan AWS Sumber Daya Anda.
- Buat target tersebut atau target untuk digunakan dalam aturan peristiwa Anda.

Untuk membuat EventBridge aturan untuk AWS Health

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Untuk mengubah Wilayah AWS, gunakan pemilih Wilayah di sudut kanan atas halaman. Pilih Wilayah tempat Anda ingin melacak AWS Health acara.

3. Di panel navigasi, pilih Aturan.
4. Pilih Buat aturan.
5. Pada halaman Tentukan detail aturan, masukkan nama dan deskripsi untuk aturan Anda.
6. Simpan nilai default untuk bus Acara dan tipe Aturan, lalu pilih Berikutnya.
7. Pada halaman pola acara Build, untuk sumber Event, pilih AWS event dan event EventBridge partner.
8. Di bawah Pola acara, untuk sumber Acara, pilih Layanan AWS.
9. Di bawah pola acara, untuk Layanan AWS, pilih Health.
10. Untuk jenis Acara, pilih salah satu opsi berikut.
    - Acara Penyalahgunaan Kesehatan Khusus - Buat aturan untuk AWS Health acara yang memiliki kata `Abuse` dalam nama jenis acara.
    - Acara Kesehatan Khusus - Buat aturan untuk acara tertentu Layanan AWS, seperti Amazon EC2.
11. Anda dapat memilih Layanan apa pun atau Layanan khusus. Jika Anda memilih layanan tertentu, pilih salah satu opsi berikut:
    - Pilih Kategori jenis peristiwa apa pun untuk membuat aturan yang berlaku untuk semua kategori jenis peristiwa.
    - Pilih kategori jenis peristiwa tertentu dan kemudian pilih nilai dari daftar, seperti masalah, AccountNotification, atau ScheduledChange.

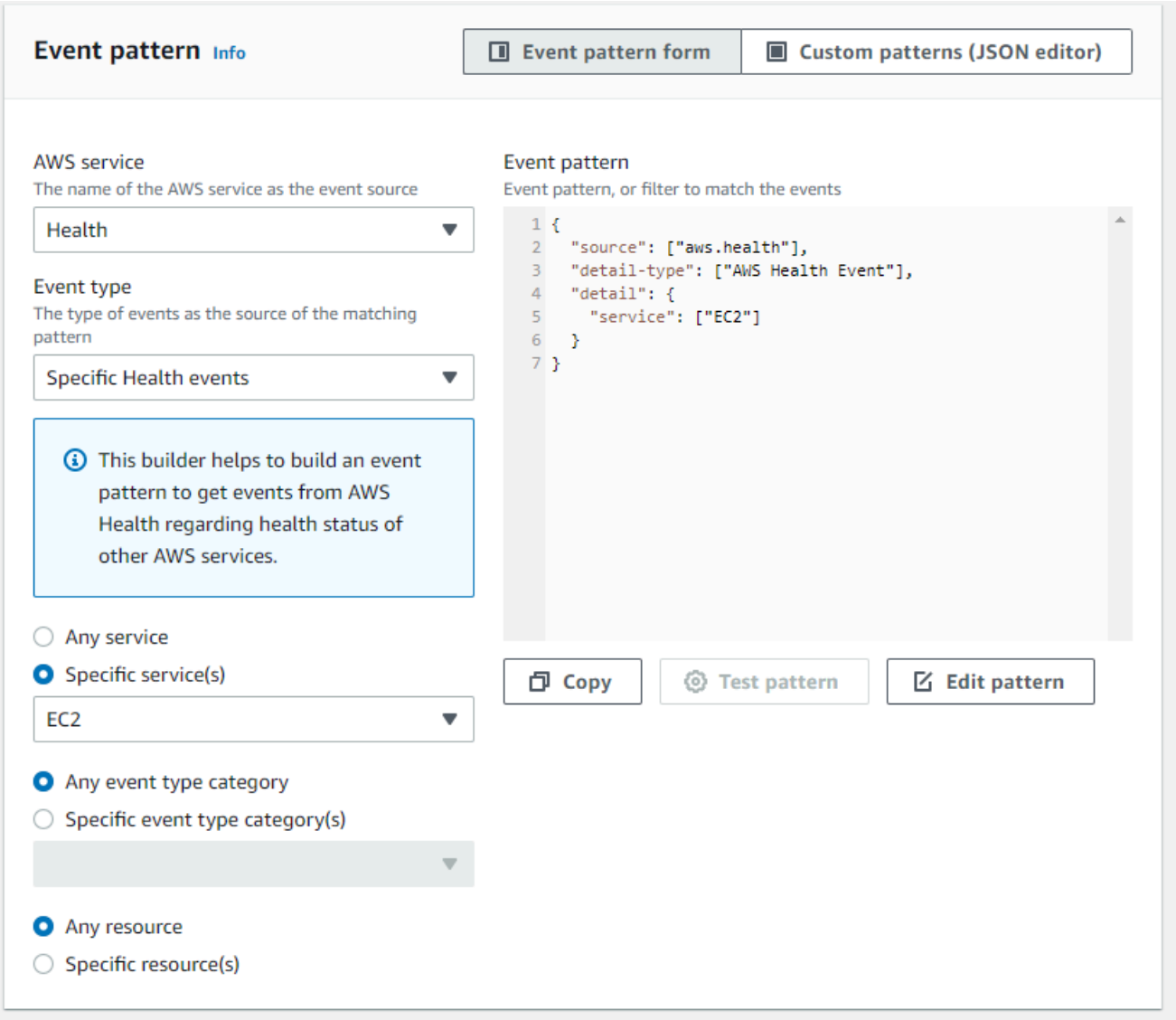
    > **Tip**
    >
    > - Untuk memantau semua AWS Health acara untuk layanan tertentu, kami sarankan Anda memilih Kategori jenis acara apa pun dan sumber daya apa pun. Hal ini memastikan bahwa aturan Anda memantau untuk setiap peristiwa AWS Health , termasuk kode jenis peristiwa baru apa pun, untuk layanan yang Anda tentukan. Sebagai aturan contoh, lihat semua peristiwa Amazon EC2.
    > - Anda dapat membuat aturan untuk memantau untuk lebih dari satu layanan atau peristiwa jenis kategori. Untuk melakukannya, Anda harus secara manual memperbarui pola peristiwa untuk aturan. Untuk informasi selengkapnya, lihat Membuat aturan untuk beberapa layanan dan kategori.
12. Jika Anda memilih kategori layanan dan jenis acara tertentu, pilih salah satu opsi berikut untuk kode jenis peristiwa.

- Pilih Kode jenis peristiwa apa pun untuk membuat aturan yang berlaku untuk semua kode jenis peristiwa.
- Pilih Kode jenis peristiwa tertentu dan kemudian pilih satu atau lebih nilai dari daftar. Hal ini menciptakan aturan yang hanya berlaku untuk kode jenis peristiwa tertentu. Sebagai contoh, jika Anda memilih **`AWS_EC2_INSTANCE_STOP_SCHEDULED`** dan **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**, aturan Anda hanya berlaku untuk peristiwa ini bila terjadi di akun Anda.

13. Pilih salah satu opsi berikut untuk sumber daya terpengaruh.
    - Pilih Semua sumber daya untuk membuat aturan yang berlaku ke semua sumber daya.
    - Pilih Sumber daya spesifik dan masukkan ID dari satu atau lebih sumber daya. Misalnya, Anda dapat menentukan ID instans Amazon EC2, seperti *`i-ExampleA1B2C3DE4`*, untuk memantau peristiwa yang hanya memengaruhi sumber daya ini.
14. Tinjau pengaturan aturan Anda sehingga memenuhi persyaratan pemantauan acara Anda.
15. Pilih Selanjutnya.
16. Pada halaman Pilih target, pilih jenis target yang Anda buat untuk aturan ini, lalu konfigurasikan opsi tambahan apa pun yang diperlukan untuk jenis tersebut. Misalnya, Anda dapat mengirim acara ke antrean Amazon SQS atau topik Amazon SNS.
17. Pilih Selanjutnya.
18. (Opsional) Pada halaman Konfigurasi tag, tambahkan tag apa pun lalu pilih Berikutnya.
    - Catatan: Tag saat ini tidak dikirim oleh sumber aws.health di. EventBridge
19. Pada halaman Tinjau dan buat, tinjau pengaturan aturan Anda dan pastikan aturan tersebut memenuhi persyaratan pemantauan acara Anda.
20. Pilih Buat aturan.

Example : Aturan untuk semua peristiwa Amazon EC2

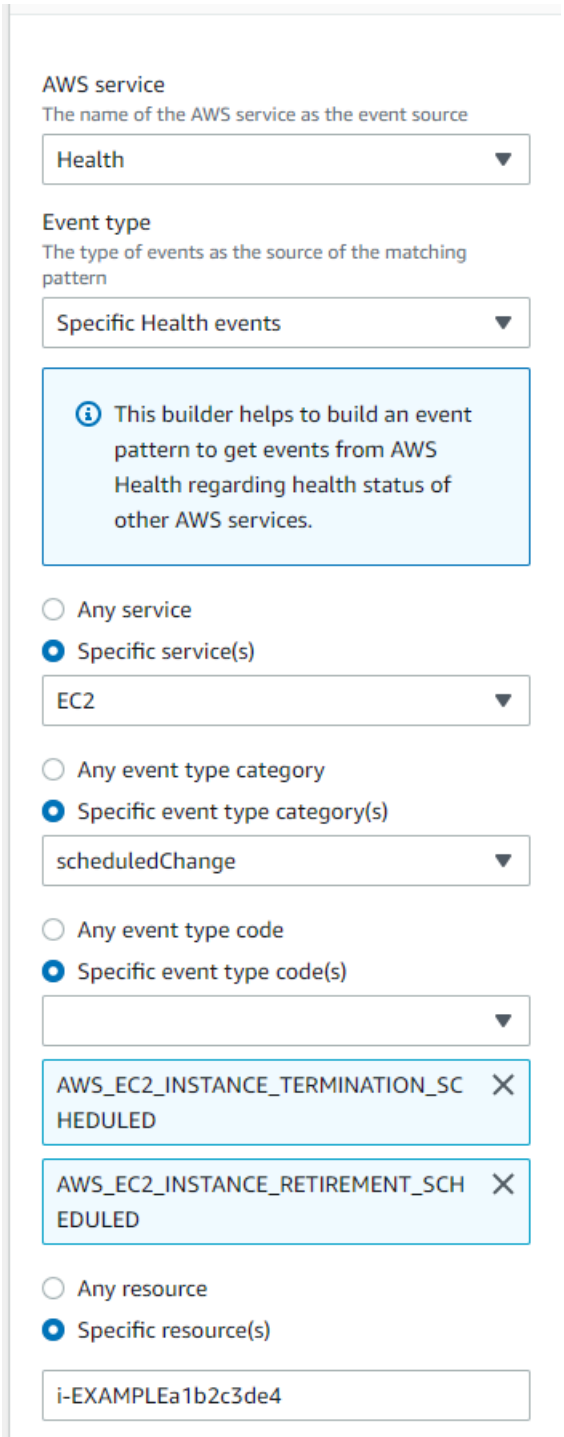
Contoh berikut membuat aturan sehingga EventBridge memantau semua peristiwa Amazon EC2, termasuk kategori jenis acara, kode peristiwa, dan sumber daya.



Example : Aturan untuk peristiwa Amazon EC2 tertentu

Contoh berikut membuat aturan sehingga EventBridge memantau hal-hal berikut:

- Layanan Amazon EC2
- Kategori jenis peristiwa scheduledChange
- Kode jenis peristiwa untuk `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` dan `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- Contoh dengan ID `i-EXAMPLEa1b2c3de4`



Membuat aturan untuk beberapa layanan dan kategori

Contoh dalam prosedur sebelumnya menunjukkan Anda cara membuat aturan untuk layanan tunggal dan kategori jenis peristiwa. Anda juga dapat membuat aturan untuk beberapa layanan dan kategori jenis peristiwa. Ini berarti Anda tidak perlu membuat aturan terpisah untuk setiap layanan dan

kategori yang ingin Anda pantau. Untuk melakukannya, Anda harus mengedit pola peristiwa dan kemudian memasukkan perubahan Anda secara manual.

Anda dapat menggunakan salah satu opsi berikut.

Untuk menambahkan layanan dan kategori untuk aturan yang ada

1. Di EventBridge konsol, pada halaman Aturan, pilih nama aturan.
2. Di sudut kanan atas, pilih Edit.
3. Pilih Selanjutnya.
4. Untuk pola Acara, pilih Edit pola, lalu masukkan perubahan Anda ke dalam bidang teks.
5. Pilih Berikutnya hingga Anda mencapai halaman Review dan update.
6. Pilih Aturan pembaruan untuk menyimpan perubahan Anda.

Untuk menambahkan layanan dan kategori untuk aturan baru

1. Ikuti prosedur Membuat EventBridge aturan untuk AWS Health ke langkah 9.
2. Alih-alih memilih satu layanan atau kategori dari daftar, untuk pola Acara, pilih Edit pola.
3. Masukkan perubahan Anda ke dalam bidang teks. Lihat contoh pola berikut sebagai model untuk membuat pola acara Anda sendiri.
4. Tinjau pola acara Anda, lalu ikuti prosedur lainnya Membuat EventBridge aturan untuk AWS Health untuk membuat aturan Anda.

Gunakan API atau AWS Command Line Interface (AWS CLI)

Untuk aturan baru atau yang sudah ada, gunakan operasi PutRuleAPI atau `aws events put-rule` perintah untuk memperbarui pola peristiwa. Untuk contoh AWS CLI perintah, lihat put-rule di AWS CLI Command Reference.

Example Contoh: Beberapa layanan dan kategori jenis peristiwa

Pola peristiwa berikut membuat aturan untuk memantau peristiwa untuk`issue`,`accountNotification`, dan kategori jenis `scheduledChange` acara untuk tiga AWS layanan: Amazon EC2, Amazon EC2 Auto Scaling, dan Amazon VPC.

```
{
  "detail": {
    "eventTypeCategory": [
```

```
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

AWS HealthAmazon EventBridge Skema Acara

Berikut ini adalah skema untuk AWS Health acara. Perubahan atau penambahan skema versi sebelumnya disorot sebagai “Baru”. Muatan sampel disediakan setelah skema.

AWS Health Skema Acara

AWS Health Skema Acara

Parameter	Deskripsi	Diperlukan
versi	EventBridge Versi, saat ini “0"	Ya
id	uniqueEventBridge Pengenal untuk acara tersebut	Ya
detail-tipe	Menjelaskan jenis	Ya

Parameter	Deskripsi	Diperlukan
	detailnya. Untuk AWS Health acara ini akan menjadi &AWS Health Event atau AWS Health Abuse Event	
sumber	Sumber bus acara. Untuk AWS Health acara ini akan aws.health	Ya

Parameter	Deskripsi	Diperlukan
akun	AccountId untuk acara AWS Health tersebut dikirim ke. **Note** Untuk tampilan organisasi, ini akan berbeda dari AffectedAccount jika diterima di akun administrator manajeme atau didelegasikan.	Ya

Parameter	Deskripsi	Diperlukan
waktu	Waktu di mana pemberitahuan dikirim ke EventBridge. Format: `yyyy-mm-ddThh:mm:ssZ` .	Ya

Parameter	Deskripsi	Diperlukan
region	Mengidentifikasi tempat Wilayah AWS notifikasi dikirimkan. **Note** Bidang ini tidak menunjukan Wilayah yang terkena dampak untuk AWS Health acara ini. Ini disediakan oleh “detail.eventRegion”.	Ya

Parameter	Deskripsi	Diperlukan
sumber daya	Menjelaskan daftar sumber daya yang terpengaruh dalam akun, jika ada sumber daya yang terpengaruh. **Note** Bidang ini bisa kosong jika tidak ada sumber daya yang direferensikan.	Tidak
detail	Bagian ini berisi semua detail AWS Health acara, seperti yang tercantum di bawah ini.	Ya

Parameter		Deskripsi	Diperlukan
	EventARN	Pengenal unik untuk AWS Health acara untuk Wilayah tertentu, termasuk Wilayah dan id acara. **Note** EventARN tidak unik untuk akun pelanggan tertentu atau ke Wilayah.	Ya

Parameter		Deskripsi	Diperlukan
	layanan	yang Layanan AWS terpengaruh oleh AWS Health peristiwa tersebut. Misalnya, Amazon EC2, Layanan Penyimpanan Sederhana Amazon, Amazon Redshift, atau Amazon Relational Database Service.	Ya

Parameter		Deskripsi	Diperlukan
	acara TypeCode	Pengidentifikasi unik untuk jenis peristiwa tersebut. Misalnya: `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` dan `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED`. Acara yang mencakup `MAINTENANCE_SCHEDULED` umumnya didorong keluar sekitar dua minggu sebelum StartTime. **Note** Semua peristiwa siklus	Ya

Parameter		Deskripsi	Diperlukan
		hidup baru yang direncanakan memiliki jenis acara. `AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT`	
	acara TypeCategory	Kode kategori peristiwa. Nilai yang mungkin adalah `issue`, `notification`, `investigation`, dan `scheduledChange`.	Ya

Parameter		Deskripsi	Diperlukan
	acara ScopeCode	Menunjukkan apakah AWS Health acara tersebut spesifik akun atau publik. Nilai yang mungkin adalah `ACCOUNT_SPECIFIC` atau`PUBLIC`.	Ya

Parameter		Deskripsi	Diperlukan
	CommunicationId (Baru)	Pengidentifikasi unik untuk komunikasi ini untuk AWS Health acara tersebut. Pesan dengan CommunicationID yang sama adalah kemungkinan pesan cadangan atau halaman dari satu AWS Health peristiwa. Pengenal ini dapat digunakan dengan accountID untuk membantu menghilangkan duplikat pesan.	Ya

Parameter	Deskripsi	Diperlukan
	Note Dengan rilis fitur paginatio n, Communi tionId menyertal an nomor halaman untuk menjaga Communi tionId unik di seluruh halaman, misalnya, 12345678 10-1. Untuk informasi selengkap nya, lihat Paginasi AWS Health acara di	

Parameter		Deskripsi	Diperlukan
		EventBridge.	
	startTime	Waktu mulai AWS Health acara dalam format:`DoW, DD, MMM, YYYY, HH:MM:SS TZ`. **Note** Waktu mulai bisa di masa depan untuk acara yang dijadwalkan.	Ya

Parameter		Deskripsi	Diperlukan
	endTime	Waktu akhir AWS Health acara dalam format:`DoW, DD MMM YYYY HH:MM:SS TZ`. **Note** EndTime mungkin tidak disediakan untuk acara yang ditetapkan di masa depan.	Tidak
	terakhir UpdatedTime	Waktu pembaruan terakhir untuk AWS Health acara dalam format:`DoW, DD MMM YYYY HH:MM:SS TZ`.	Ya

Parameter		Deskripsi	Diperlukan
	statusCode	Status AWS Health acara. Kategori tipe memiliki status yang berbeda. Nilai yang mungkin untuk kategori `Issue` acara adalah`open`, `closed` atau`upcoming`. `scheduled Changes` kateg acara memiliki status yang berbeda:`Upcom` atau`Complete` . `AccountNo tificatio ns` kategori acara tidak memiliki status dan disetel ke`"-"`.	Ya

Parameter		Deskripsi	Diperlukan
	EventRegion	Wilayah yang terkena dampak dijelaskan oleh AWS Health peristiwa ini.	Ya
	Deskripsi Acara	Bagian yang menjelaskan AWS Health peristiwa tersebut. Ini termasuk bidang untuk bahasa dan teks untuk menggambarkan acara.	Ya

Parameter			Deskripsi	Diperlukan
		language	Bahasa yang digunakan dalam AWS Health acara tersebut. Ini biasanya ditentukan oleh Wilayah tempat acara tersebut dipublika sikan. Untuk Wilayah us-east-1, ini biasanya “en_US”.	Ya

Parameter			Deskripsi	Diperlukan
		Keterangan Terkini	Menjelaskan AWS Health peristiwa saat dirender dari AWS Health API dan biasanya muncul di AWS Health dasbor. **Note** Untuk acara publik, ini hanya berisi pembarua terbaru dan bukan seluruh riwayat acara.	Ya

Parameter			Deskripsi	Diperlukan
	EventMetadata		Metadata acara tambahan yang dapat disediakan untuk acara tersebut. AWS Health	Tidak
		<metadata key 1>	kunci metadata, string nilai “keystring1": “keyvalue1" **Note** Pasangan kunci-nilai untuk metadata peristiwa ditentukan oleh layanan yang mengirim acara. AWS Health	Tidak

Parameter			Deskripsi	Diperlukan
	TerpengaruhDentitas		Array yang menjelaskan nilai sumber daya dan status sumber daya yang terpengaruh dalam AWS Health acara ini.	Tidak
		EntityValue	ID sumber daya/entitas	Tidak
		LastUpdatedTime (Baru)	Waktu ketika status sumber daya/entitas ini terakhir diperbarui dalam format: `DoW, DD MMM YYYY HH:MM:SS TZ`	Tidak
		status (baru)	Status sumber daya/entitas yang terpengaruh. Nilai yang mungkin termasuk`IMPAI D ,PENDING,RE`	Tidak : WN.

Parameter		Deskripsi	Diperlukan
	halaman (Baru)	Halaman yang diwakili pesan ini. Untuk informasi selengkapnya, lihat Paginasi AWS Health acara di EventBridge. Note Pagination hanya terjadi pada sumber daya. Penyebab lain untuk pelanggaran batas ukuran 256KB akan menyebabkan komunika	Ya

Parameter		Deskripsi	Diperlukan
		i gagal.	

Parameter		Deskripsi	Diperlukan
	TotalPages (Baru)	Jumlah total halaman untuk acara kesehatan ini. Untuk informasi selengkapnya, lihat Paginasi AWS Health acara di EventBridge. **Note** Anda dapat menggunakan ini untuk menentukan apakah Anda menerima semua halaman komunikasi multi-halaman untuk	Ya

Parameter	Deskripsi	Diperlukan
	sebuah akun.	

Parameter		Deskripsi	Diperlukan
	AffectedAccount (Baru)	Ini adalah accountID dari akun yang terkena dampak. **Note** Ini mungkin berbeda dari bidang “akun” jika acara kesehatar ini dikirim ke akun yang merupaka bagian dari AWS Organizat ions dan ini diterima di akun manajeme atau	Ya

Parameter		Deskripsi	Diperlukan
		administrator yang didelegasikan.	

Acara Kesehatan Masyarakat - Masalah operasional Amazon EC2


```
        {
          "version": "0",
          "id": "7bf73129-1428-4cd3-a780-95db273d1602",
          "detail-type": "AWS Health Event",
          "source": "aws.health",
          "account": "123456789012",
          "time": "2023-01-27T09:01:22Z",
          "region": "af-south-1",
          "resources": [],
          "detail": {
            "eventArn": "arn:aws:health:af-south-1::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-
d0179ed6d68f",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "eventScopeCode": "PUBLIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
            "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
            "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
            "statusCode": "open",
            "eventRegion": "af-south-1",
            "eventDescription":
            [{
              "language": "en_US",
              "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
```

```
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
            }],
            "affectedEntities":[],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
        }
```

AWS Health Peristiwa Khusus Akun - Masalah Elastic Load Balancing API

```
        {
          "version": "0",
          "id": "121345678-1234-1234-1234-123456789012",
          "detail-type": "AWS Health Event",
          "source": "aws.health",
          "account": "123456789012",
          "time": "2022-06-10T06:27:57Z",
          "region": "ap-southeast-2",
          "resources": [],
          "detail": {
            "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
            "service": "ELASTICLOADBALANCING",
            "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
            "eventTypeCategory": "issue",
            "eventScopeCode": "ACCOUNT_SPECIFIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
            "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
            "statusCode": "open",
            "eventRegion": "ap-southeast-2",
            "eventDescription": [{
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
```

```
        }
```

AWS Health Peristiwa Khusus Akun - Kinerja Drive Toko Instans Amazon EC2 Menurun

```
        {
          "version": "0",
          "id": "121345678-1234-1234-1234-123456789012",
          "detail-type": "AWS Health Event",
          "source": "aws.health",
          "account": "123456789012",
          "time": "2022-06-03T06:27:57Z",
          "region": "us-west-2",
          "resources": [
            "i-abcd1111"
          ],
          "detail": {
            "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
            "eventTypeCategory": "issue",
            "eventScopeCode": "ACCOUNT_SPECIFIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
            "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
            "statusCode": "open",
            "eventRegion": "us-west-2",
            "eventDescription": [{
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }],
            "affectedEntities": [{
              "entityValue": "i-abcd1111",
            }],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
        }
```

Paginasi AWS Health acara di EventBridge

AWS Health mendukung pagination AWS Health peristiwa ketika daftar “resource” atau “affectEdentities” menyebabkan ukuran pesan melebihi batas ukuran pesan 256KB EventBridge. Sebelumnya, AWS Health tidak mengomunikasikan daftar lengkap sumber daya dengan peristiwa ketika melebihi batas ini.

AWS Health sekarang mencakup semua “sumber daya” dan “detail.AffectEdentities” dalam pesan. Jika daftar “sumber daya” dan “detail.AffecteDentities” ini melebihi 256KB, kemudian AWS Health membagi acara kesehatan menjadi beberapa halaman dan mempublikasikan halaman ini sebagai pesan individual. EventBridge Setiap halaman mempertahankan EventArn dan CommunicationId yang sama untuk membantu menggabungkan kembali daftar “resource” atau “detail.affectEdentities” setelah semua halaman diterima.

Pesan tambahan ini dapat menyebabkan pesan yang tidak perlu, misalnya ketika EventBridge aturan diarahkan ke antarmuka yang dapat dibaca manusia seperti email atau obrolan. Pelanggan dengan notifikasi yang dapat dibaca manusia dapat menambahkan filter untuk bidang “detail.page” untuk memproses hanya halaman pertama, yang menghilangkan pesan yang tidak perlu yang dibuat dari halaman berikutnya.

Beberapa perubahan skema disertakan untuk mendukung peluncuran pagination. Setiap communicationId sekarang menyertakan nomor halaman tanda hubung setelah communicationId, bahkan ketika hanya ada 1 halaman. Ada juga dua bidang baru, detail.page dan detail.totalPages, yang menggambarkan nomor halaman saat ini dan jumlah total halaman untuk acara tersebut. AWS Health Informasi yang terkandung dalam setiap pesan paginasi adalah sama kecuali untuk daftar “detail.affecteDentities” atau “resources”. Daftar ini dapat direkonstruksi setelah semua halaman diterima. Halaman-halaman sumber daya dan entitas yang terpengaruh adalah urutan-agnostik.

Menggabungkan AWS Health peristiwa menggunakan tampilan organisasi dan akses administrator yang didelegasikan

AWS Health mendukung tampilan organisasi dan akses administrator yang didelegasikan untuk AWS Health acara yang dipublikasikan di Amazon EventBridge. Ketika tampilan organisasi diaktifkan AWS Health, maka akun manajemen atau akun administrator yang didelegasikan akan menerima satu umpan AWS Health peristiwa dari semua akun dalam AWS Organizations organisasi Anda.

Fitur ini dirancang untuk memberikan tampilan terpusat untuk membantu mengelola AWS Health acara di seluruh organisasi Anda. Menyiapkan tampilan organisasi dan EventBridge aturan di akun manajemen tidak menonaktifkan EventBridge aturan untuk akun lain di organisasi Anda.

Untuk informasi selengkapnya tentang mengaktifkan tampilan organisasi dan akses administrator yang didelegasikan AWS Health, lihat Menggabungkan AWS Health Acara.

Menerima AWS Health acara dengan AWS Chatbot

Anda dapat menerima AWS Health acara langsung di klien obrolan Anda, seperti Slack dan Amazon Chime. Anda dapat menggunakan acara ini untuk mengidentifikasi masalah AWS layanan terbaru yang mungkin memengaruhi AWS aplikasi dan infrastruktur Anda. Kemudian, Anda dapat masuk ke AWS Health Dasbor untuk mempelajari lebih lanjut tentang pembaruan. Misalnya, jika Anda memantau jenis `AWS_EC2_INSTANCE_STOP_SCHEDULED` acara di AWS akun Anda, AWS Health acara dapat muncul langsung ke saluran Slack Anda.

Prasyarat

Sebelum memulai, Anda harus memiliki hal berikut:

- Klien obrolan yang dikonfigurasi dengan AWS Chatbot. Anda dapat mengkonfigurasi Amazon Chime dan Slack. Untuk informasi selengkapnya, lihat Memulai dengan AWS Chatbot di Panduan Administrator AWS Chatbot .
- Topik Amazon SNS yang Anda buat dan langganan Anda. Jika Anda sudah memiliki topik SNS, Anda dapat menggunakan topik yang sudah ada. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

Untuk menerima AWS Health acara dengan AWS Chatbot

1. Ikuti prosedur Membuat EventBridge aturan untuk AWS Health melalui langkah 13.

   a. Ketika Anda selesai menyiapkan pola acara di langkah 13, tambahkan koma ke baris terakhir pola, dan tambahkan baris berikut untuk menghapus pesan obrolan yang tidak perlu dari acara paginasi AWS Health . Lihat Paginasi AWS Health acara di EventBridge.

   ```
   "detail.page": ["1"]
   ```

   b. Saat Anda memilih target di langkah 14, pilih topik SNS. Anda akan menggunakan topik SNS yang sama ini di AWS Chatbot konsol.

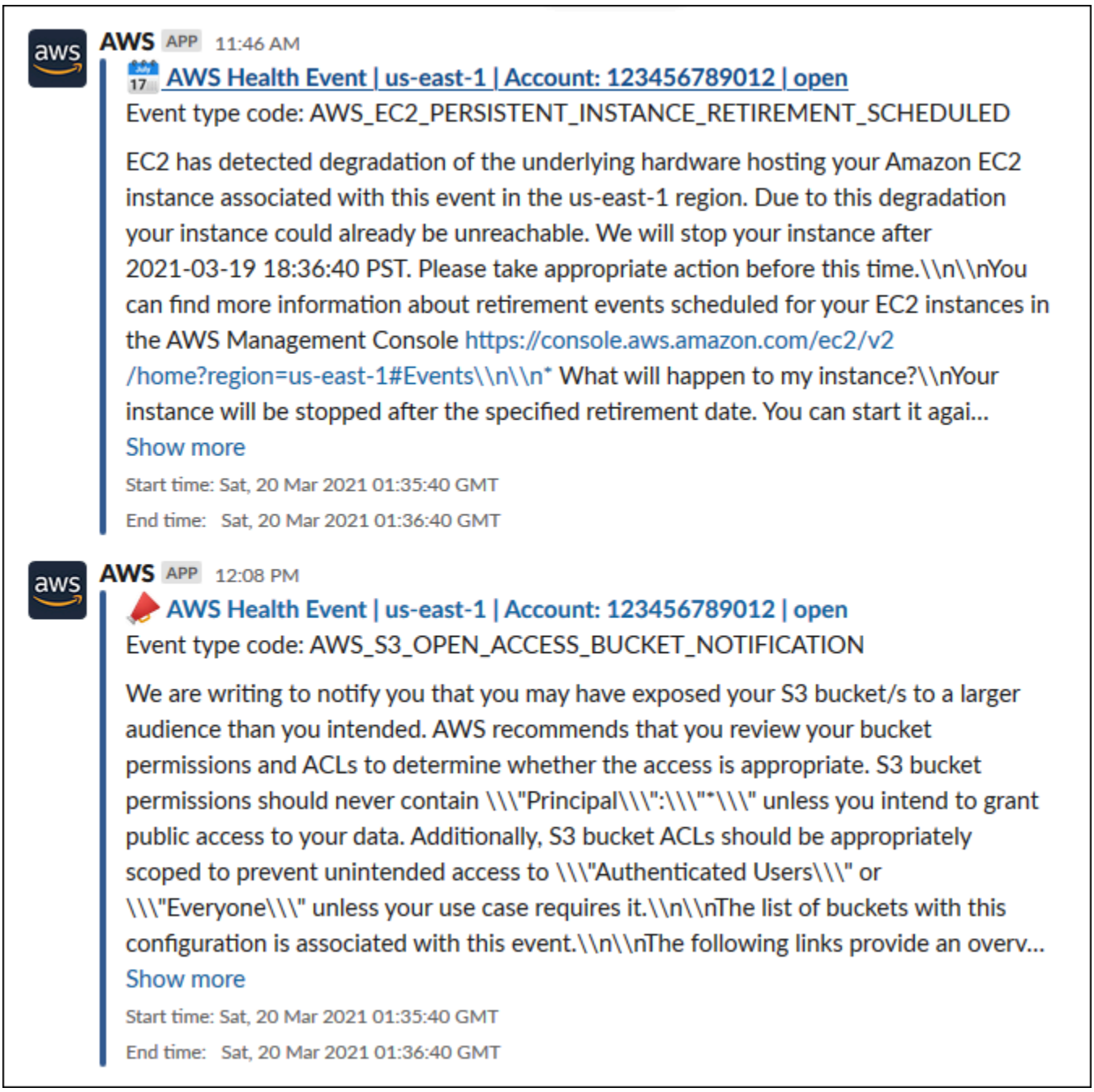
c. Selesaikan prosedur lainnya untuk membuat aturan.

2. Navigasikan ke konsol AWS Chatbot.
3. Pilih obrolan klien Anda, seperti nama saluran Slack, lalu pilih Sunting.
4. Di bagian Pemberitahuan - opsional, untuk Topik, pilih topik SNS yang sama yang Anda tentukan di langkah 1.
5. Pilih Simpan.

   Saat AWS Health mengirim acara EventBridge yang sesuai dengan aturan Anda, AWS Health acara tersebut akan muncul di klien obrolan Anda.
6. Pilih nama acara untuk melihat informasi lebih lanjut di AWS Health Dasbor Anda.

Example : AWS Health acara dikirim ke Slack

Berikut ini adalah contoh dua AWS Health peristiwa untuk Amazon EC2 dan Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) di Wilayah AS Timur (Virginia N.) yang muncul di saluran Slack.



Otomatisasi tindakan untuk Instans Amazon EC2

Anda dapat mengotomatiskan tindakan yang merespons peristiwa terjadwal untuk instans Amazon EC2 Anda. Saat AWS Health mengirim acara ke AWS akun Anda, EventBridge aturan Anda kemudian dapat memanggil target, seperti dokumen AWS Systems Manager Otomasi, untuk mengotomatiskan tindakan atas nama Anda.

Misalnya, ketika acara pensiun instans Amazon EC2 dijadwalkan untuk instans EC2 yang didukung Amazon Elastic Block Store (Amazon EBS) AWS Health , akan mengirimkan jenis acara ke Dasbor Anda. `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` AWS Health Ketika aturan Anda mendeteksi jenis peristiwa ini, Anda dapat otomatisasi berhenti dan mulai instans. Dengan cara ini, Anda tidak perlu melakukan tindakan ini secara manual.

> **Note**
>
> Untuk mengotomatiskan tindakan untuk instans Amazon EC2 Anda, instans harus dikelola oleh Systems Manager.

Untuk informasi selengkapnya, lihat Mengotomatiskan Amazon EC2 EventBridge dengan di Panduan Pengguna Amazon EC2.

Prasyarat

Anda harus membuat kebijakan AWS Identity and Access Management (IAM), membuat peran IAM, dan memperbarui kebijakan kepercayaan peran sebelum Anda dapat membuat aturan.

Buat kebijakan IAM

Ikuti prosedur ini untuk membuat kebijakan dikelola pelanggan untuk peran Anda. Kebijakan ini mengizinkan peran untuk melakukan tindakan atas nama Anda. Prosedur ini menggunakan editor kebijakan JSON di konsol IAM.

Untuk membuat kebijakan IAM

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Pilih Buat kebijakan.
4. Pilih tab JSON.
5. Salin JSON berikut dan kemudian ganti JSON default di editor.

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
}
```

a. Dalam `Resource` parameter, untuk Nama Sumber Daya Amazon (ARN), masukkan ID AWS akun Anda.

b. Anda juga dapat mengganti nama peran atau menggunakan default. Contoh ini menggunakan *`AutomationEvRole`*.

6. Pilih Berikutnya: Tag.
7. (Opsional) Anda dapat menggunakan tag sebagai pasangan nilai kunci untuk menambahkan metadata ke kebijakan.
8. Pilih Selanjutnya: Tinjau.
9. Pada halaman Kebijakan tinjau, masukkan Nama, seperti ***AutomatioNev RolePolicy*** dan Deskripsi opsional.
10. Tinjau halaman Ringkasan untuk melihat izin yang diizinkan kebijakan. Jika Anda puas dengan kebijakan Anda, pilih Buat kebijakan.

Kebijakan ini menentukan tindakan yang dapat dilakukan peran tersebut. Untuk informasi selengkapnya, lihat Membuat kebijakan IAM (konsol) dalam Panduan Pengguna IAM.

Buat IAM role

Setelah Anda membuat kebijakan, Anda harus membuat IAM role, dan kemudian melampirkan kebijakan untuk peran tersebut.

Untuk membuat peran untuk AWS layanan

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Untuk Pilih jenis entitas tepercaya, pilih Layanan AWS .
4. Pilih EC2 untuk layanan yang ingin Anda perbolehkan untuk mengasumsikan peran ini.
5. Pilih Berikutnya: Izin.
6. Masukkan nama kebijakan yang Anda buat, seperti *`AutomatioNev RolePolicy`*, lalu pilih kotak centang di sebelah kebijakan.
7. Pilih Berikutnya: Tag.
8. (Opsional) Anda dapat menggunakan tag sebagai pasangan nilai kunci untuk menambahkan metadata ke peran.
9. Pilih Selanjutnya: Tinjau.
10. Untuk nama Peran, masukkan *`AutomationEvRole`*. Nama ini harus nama yang sama yang muncul di ARN kebijakan IAM yang Anda buat.
11. (Opsional) Untuk Deskripsi peran, masukkan deskripsi untuk peran tersebut.
12. Tinjau peran dan kemudian pilih Buat peran.

Untuk informasi selengkapnya, lihat Membuat peran untuk AWS layanan di Panduan Pengguna IAM.

Memperbarui kebijakan kepercayaan

Terakhir, Anda dapat memperbarui kebijakan kepercayaan untuk peran yang Anda buat. Anda harus menyelesaikan prosedur ini sehingga Anda dapat memilih peran ini di EventBridge konsol.

Untuk memperbarui kebijakan kepercayaan untuk peran tersebut

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Peran.
3. Dalam daftar peran di AWS akun Anda, pilih nama peran yang Anda buat, seperti *AutomationEvRole*.
4. Pilih tab Hubungan kepercayaan, dan kemudian pilihUbah hubungan kepercayaan.
5. Untuk Dokumen Kebijakan, salin JSON berikut, hapus kebijakan default, dan tempel JSON yang disalin di tempatnya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. Pilih Perbarui Kebijakan Kepercayaan.

Untuk informasi selengkapnya, lihat Mengubah kebijakan kepercayaan peran (konsol) di Panduan Pengguna IAM.

Buat aturan untuk EventBridge

Ikuti prosedur ini untuk membuat aturan di EventBridge konsol sehingga Anda dapat mengotomatiskan penghentian dan awal instans EC2 yang dijadwalkan untuk pensiun.

Untuk membuat aturan EventBridge untuk tindakan otomatis Systems Manager

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, di dalam Peristiwa, pilih Aturan.
3. Pada halaman Buat aturan, masukkan Nama dan Deskripsi untuk aturan Anda.
4. Di bawah Tentukan pola, pilih Pola acara, lalu pilih Pola yang telah ditentukan sebelumnya berdasarkan layanan.
5. Untuk Penyedia layanan, pilih AWS.
6. Untuk nama Layanan, pilih Health.
7. Untuk jenis Acara, pilih acara Kesehatan Spesifik.
8. Pilih Layanan khusus lalu pilih EC2.
9. Pilih Kategori jenis peristiwa tertentu lalu pilih scheduledChange.
10. Pilih Kode jenis peristiwa tertentu dan kemudian pilih kode jenis peristiwa.

    Sebagai contoh, untuk Instans Amazon EC2 EBS yang didukung, pilih **`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`**. Untuk Penyimpanan instans Amazon EC2 instans yang didukung, pilih **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**.
11. Pilih Sumber daya apa pun.

    Pola acara Anda akan terlihat mirip dengan contoh berikut.

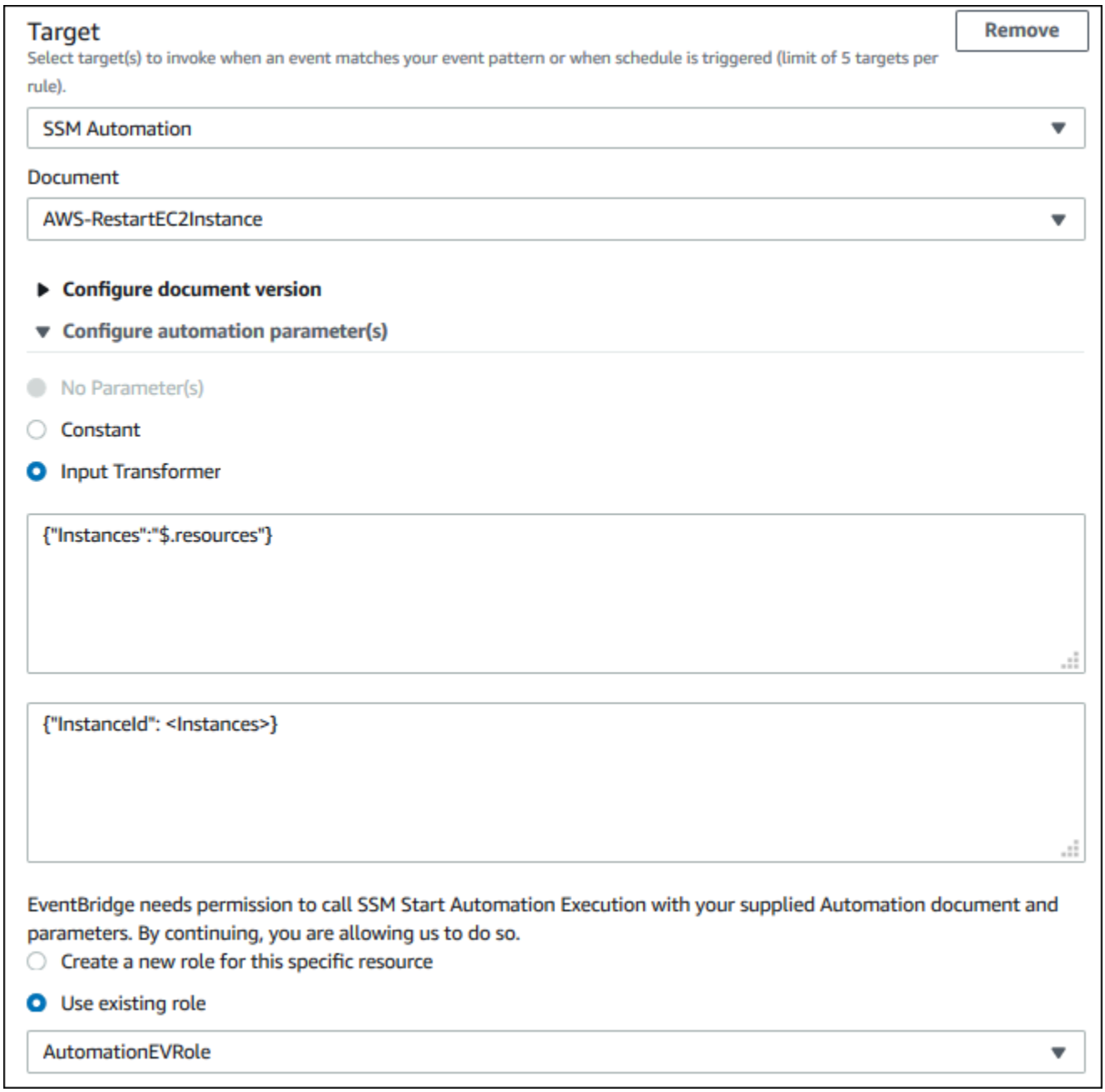
    Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
```

```
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Menambahkan target dokumen otomatisasi Systems Manager. Di bawah Pilih target, untuk Target, pilih SSM Automation.
13. Untuk Dokumen, pilih `AWS-RestartEC2Instance`.
14. Perluas Konfigurasi parameter otomasi lalu pilih Transformer input.
15. Untuk bidang Jalur Input, masukkan **`{"Instances":"$.resources"}`**.
16. Untuk bidang kedua, masukkan **`{"InstanceId": <Instances>}`**.
17. Pilih Gunakan peran yang ada, lalu pilih peran IAM yang Anda buat, seperti *`AutomationEvRole`*.

    Nama server Anda akan terlihat seperti contoh berikut.



> **Note**
>
> Jika Anda tidak memiliki IAM role yang ada dengan EC2 dan izin Systems Manager serta hubungan tepercaya yang diperlukan, peran Anda tidak akan muncul dalam daftar. Untuk informasi selengkapnya, lihat Prasyarat.

18. Pilih Buat.

Jika peristiwa terjadi di akun Anda yang cocok dengan aturan Anda, EventBridge akan mengirim acara ke target yang Anda tentukan.

Konfigurasikan konektor SMC untuk AWS Health

Anda dapat mengintegrasikan AWS Health acara dengan JIRA dan ServiceNow untuk menerima informasi operasional dan akun, mempersiapkan perubahan terjadwal, dan mengelola acara Kesehatan menggunakan Konektor Manajemen Layanan (SMC). Integrasi SMC dengan AWS Health dapat menggunakan acara Kesehatan yang dikirim EventBridge untuk membuat, memetakan, dan memperbarui tiket dan ServiceNow insiden JIRA secara otomatis.

Anda dapat menggunakan tampilan organisasi dan akses administrator yang didelegasikan untuk mengelola acara Kesehatan dengan mudah di seluruh organisasi dalam JIRA dan ServiceNow, serta memasukkan AWS Health informasi langsung ke dalam alur kerja tim Anda.

Untuk informasi selengkapnya tentang ServiceNow integrasi menggunakan SMC, lihat Mengintegrasikan. AWS Health ServiceNow

Untuk informasi selengkapnya tentang integrasi JIRA Management Cloud menggunakan SMC, lihat AWS Health di JIRA.

Pemantauan AWS Health

Pemantauan adalah bagian penting dari menjaga keandalan, ketersediaan, dan kinerja AWS Health dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton AWS Health, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda 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. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.

  Anda dapat menggunakan Amazon EventBridge sehingga Anda diberi tahu tentang AWS Health peristiwa yang mungkin memengaruhi layanan dan sumber daya Anda. Misalnya, jika AWS Health memublikasikan peristiwa tentang instans Amazon EC2 Anda, Anda dapat menggunakan pemberitahuan ini untuk mengambil tindakan dan memperbarui atau mengganti sumber daya sesuai kebutuhan. Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.
- AWS CloudTrail menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS CloudTrail.

Topik

Pencatatan panggilan AWS Health API dengan AWS CloudTrail

AWS Health terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Health. CloudTrail menangkap panggilan API untuk AWS Health sebagai acara. Panggilan yang diambil termasuk panggilan dari AWS Health konsol dan panggilan kode ke operasi AWS Health API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Health Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat

peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Health, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

AWS Health informasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di AWS Health, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Health, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam 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 File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua operasi AWS Health API dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS Health API. Misalnya, panggilan ke`DescribeEvents`,`DescribeEventDetails`, dan `DescribeAffectedEntities` operasi menghasilkan entri dalam file CloudTrail log.

AWS Health mendukung pencatatan tindakan berikut sebagai peristiwa dalam file CloudTrail log:

- Jika permintaan tersebut dibuat dengan kredensial root atau IAM
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan

- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.

Anda dapat menyimpan berkas log dalam bucket Amazon S3 selama yang diinginkan. Anda juga dapat mendefinisikan aturan siklus hidup Amazon S3 untuk mengarsipkan atau menghapus berkas log secara otomatis. Secara default, berkas log Anda dienkripsi dengan menggunakan enkripsi sisi server (SSE) Amazon S3.

Untuk diberi tahu saat pengiriman file log, Anda dapat mengonfigurasi CloudTrail untuk mempublikasikan notifikasi Amazon SNS saat file log baru dikirimkan. Untuk informasi selengkapnya, lihat Mengonfigurasi Notifikasi Amazon SNS untuk. CloudTrail

Anda juga dapat menggabungkan file AWS Health log dari beberapa AWS wilayah dan beberapa AWS akun ke dalam satu bucket Amazon S3.

Untuk informasi selengkapnya, lihat Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun.

Contoh: entri file AWS Health log

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 mana 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 entri CloudTrail log yang menunjukkan operasi DescribeEntityAgregat.


```
{
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Riwayat dokumen untuk AWS Health

Tabel berikut menjelaskan dokumentasi untuk rilis ini AWS Health.

- Versi API: 2016-08-04

Tabel berikut menjelaskan pembaruan penting pada AWS Health dokumentasi, dimulai pada 28 Agustus 2020. Anda dapat berlangganan ke umpan RSS untuk menerima pemberitahuan tentang pembaruan.

Perubahan	Deskripsi	Tanggal
Menghapus privasi lalu lintas Internetwork dari dokumentasi bagian Keamanan AWS Health	Untuk informasi selengkapnya, lihat Keamanan di AWS Health	Maret 27, 2024
Memperbarui AWS Health Dasbor — Kesehatan layanan dan peristiwa siklus hidup yang direncanakan untuk AWS Health dokumentasi.	Untuk informasi selengkapnya, lihat AWS Health Dasbor — Kesehatan layanan dan Acara siklus hidup yang direncanakan untuk. AWS Health	Februari 15, 2024
Menghapus titik bullet duplikat di Membuat aturan untuk EventBridge AWS Health	Menghapus titik bullet duplikat di Membuat aturan untuk EventBridge . AWS Health	Desember 4, 2023
Menambahkan dokumentasi untuk Acara Siklus Hidup yang Direncanakan	Untuk informasi selengkapnya, lihat Acara Siklus Hidup yang Direncanakan untuk. AWS Health	31 Oktober 2023
Dokumentasi diperbarui untuk `AWSHealthFullAccess`	Anda sekarang dapat menggunakan kebijakan `AWSHealthFullAccess` terkelola di AWS GovCloud (US) Regions. Lihat kebijakan	16 Oktober 2023

	AWS terkelola untuk AWS Health.	
Menambahkan dokumentasi untuk mengonfigurasi Pemberitahuan AWS Pengguna di AWS Health.	Anda sekarang dapat mengkonfigurasi Pemberitahuan AWS Pengguna di AWS Health. Untuk informasi selengkapnya, lihat Mengonfigurasi Pemberitahuan AWS Pengguna untuk AWS Health.	Agustus 30, 2023
Menambahkan dokumentasi untuk fitur administrator yang didelegasikan ke bagian Agregasi peristiwa. AWS Health	Untuk informasi selengkapnya, lihat Tampilan organisasi administrator yang didelegasikan.	Juli 27, 2023
Pembaruan kebijakan SLR	Perbarui ke kebijakan AWS terkelola: Kesehatan_OrganizationsServiceRolePolicy. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk AWS Health.	Juli 19, 2023
AWS Health skema sekarang mendukung metadata acara	Anda sekarang dapat menerima metadata acara dari AWS Health acara. Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.	20 Juni 2023

Dokumentasi diperbarui untuk Amazon EventBridge	Anda sekarang dapat menggunakan EventBridge aturan Amazon untuk memantau acara khusus akun dan acara publik. Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.	2 Mei 2023
Ditambahkan dokumentasi untuk kebijakan AWS terkelola	Menambahkan dokumentasi untuk kebijakan AWS terkelola AWS Health dan Menggunakan peran terkait layanan untuk. AWS Health	18 Januari 2023
Ditambahkan zona waktu pengaturan dokumentasi	Gunakan fitur zona waktu baru untuk melihat AWS Health Dasbor di zona waktu lokal Anda atau di UTC. Untuk informasi selengkapnya, lihat Memulai AWS Health Dasbor — Kesehatan akun Anda dan AWS Health Dasbor — Kesehatan layanan.	21 September 2022
Dokumentasi diperbarui	Ditambahkan dokumentasi untuk AWS Health Aware. Untuk informasi lebih lanjut, lihat AWS Health Sadar.	25 Mei 2022

Dokumentasi diperbarui	The Service Health Dashboard and the AWS Personal Health Dashboard telah diganti namanya menjadi Dashboard. AWS Health Untuk informasi selengkapnya, lihat Memulai AWS Health Dasbor — Kesehatan akun Anda dan AWS Health Dasbor — Kesehatan layanan.	28 Februari 2022
Dokumentasi diperbarui untuk Amazon EventBridge	Topik baru AWS Health untuk menggunakan Amazon EventBridge untuk memantau acara Kesehatan. Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge.	3 Februari, 2022
Dokumentasi diperbarui	Jika Anda memiliki paket Enterprise On-Ramp Support, Anda dapat menggunakan API. AWS Health	24 November 2021
Dokumentasi ditambahkan	Topik baru untuk AWS Health konsep. Untuk informasi selengkapnya, lihat Konsep untuk AWS Health.	29 Juli 2021

Dokumentasi diperbarui untuk CloudWatch Acara	Menambahkan bagian tentang cara membuat aturan untuk beberapa layanan dan kategori jenis peristiwa . Untuk informasi selengkap nya, lihat Membuat aturan untuk beberapa layanan dan kategori.	7 Mei 2021
Dokumentasi diperbarui untuk CloudWatch Acara	Memperbarui bagian untuk mengotomatiskan AWS Systems Manager tindakan untuk aturan Amazon CloudWatch Events. Untuk informasi selengkapnya, lihat Otomatisasi tindakan untuk Instans Amazon EC2.	28 April 2021
Dokumentasi diperbarui untuk CloudWatch Acara	Menambahkan bagian untuk menerima AWS Health acara di klien obrolan Anda. Untuk informasi selengkapnya, lihat Menerima AWS Health acara dengan AWS Chatbot.	16 Maret 2021

Dokumentasi diperbarui	Topik berikut diperbarui: • Memperbarui topik Menggabungkan peristiwa AWS Health • Menata ulang dan memperbarui Monitor untuk AWS Health acara dengan topik Amazon CloudWatch Events • Memperbarui bagian Sumber daya- dan kondisi berbasis aksi	29 Januari 2021
Menambahkan AWS Health Dasbor untuk tampilan organisasi di AWS Health konsol	Anda dapat menggunakan AWS Health konsol untuk mengaktifkan fitur tampilan organisasi. Kemudian, Anda dapat melihat kondisi kesehatan untuk akun anggota di organisasi AWS Anda.	14 Desember 2020
Demo titik akhir ketersediaan tinggi	Anda dapat menggunakan kode contoh untuk menentukan titik akhir regional aktif dan menandatangani AWS Region untuk AWS Health.	22 Oktober 2020
Pembaruan untuk Panduan AWS Health Pengguna	Pembaruan organisasi dan menambahkan umpan RSS sehingga Anda dapat berlangganan pembaruan terbaru ke AWS Health dokumentasi.	28 Agustus 2020

Pembaruan sebelumnya

Perubahan	Deskripsi	Tanggal
Memperbarui topik tampilan organisasi untuk menyertakan contoh.	Lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.	3 Juni 2020
Keamanan dan AWS Health	Menambahkan informasi tentang pertimbangan keamanan saat menggunakan AWS Health. Lihat Keamanan di AWS Health.	Mei 5, 2020
Menambahkan bagian baru untuk menjelaskan cara menggunakan tampilan organisasi untuk peristiwa yang dikumpulkan di semua akun di AWS Organizations.	Lihat Menggabungkan peristiwa AWS Health di seluruh akun dengan tampilan organisasi.	18 Desember 2019
Menambahkan bagian baru “Kondisi Berbasis Sumber Daya dan Tindakan” untuk menjelaskan pembatasan Acara yang dijual oleh API. AWS Health	Lihat Identity and access management untuk AWS Health.	2 Agustus 2018
Menambahkan catatan tentang visibilitas AWS Health informasi.	Lihat Identity and access management untuk AWS Health.	16 Agustus 2017
Rilis pelayanan.	AWS Health dirilis.	1 Desember 2016

Daftar istilah AWS

Untuk terminologi AWS terbaru, lihat Daftar istilah AWS di Referensi Glosarium AWS.

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