



Panduan Pengguna

AWS Health



AWS Health: Panduan Pengguna

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

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

Table of Contents

Apa itu AWS Health?	1
Konsep untuk AWS Health	2
AWS Health acara	2
Acara khusus akun	3
Acara publik	3
AWS Health Dasbor	3
AWS Health Dashboard — Layanan kesehatan	4
Kode jenis acara	4
Kategori jenis acara	4
Status acara	6
Aksionabilitas	6
Persona	7
Entitas terpengaruh	7
AWS Health acara di Amazon EventBridge	7
AWS Health API	8
Tampilan organisasi	8
Notifikasi Pengguna AWS	9
Memulai	10
Menyiapkan	10
Mendaftar untuk Akun AWS	11
Buat pengguna dengan akses administratif	11
Lihat peristiwa akun di AWS Health Dasbor	12
Terbuka dan masalah terbaru	13
Perubahan terjadwal	14
Pemberitahuan lainnya	15
Log peristiwa	15
Detail peristiwa	16
Tipe peristiwa	18
Tampilan kalender	18
Tampilan sumber daya yang terpengaruh	19
Pengaturan zona waktu	20
Kesehatan organisasi Anda	21
Peringatan untuk acara AWS Health	21
Mengkonfigurasi Amazon EventBridge	22

Kelola notifikasi di Notifikasi Pengguna AWS	22
Konfigurasi langganan notifikasi AWS terkelola untuk AWS Health acara	23
AWS pemberitahuan terkelola FAQ	24
AWS Health Dasbor	26
Acara siklus hidup yang direncanakan untuk AWS Health	29
Apa acara siklus hidup yang direncanakan?	29
Apa yang harus saya harapkan ketika saya menerima pemberitahuan peristiwa siklus hidup yang direncanakan?	30
Model tanggung jawab bersama untuk ketahanan	32
Mengakses acara siklus hidup yang direncanakan	33
Integrasi dengan sistem lain menggunakan API AWS Health	34
Menandatangani permintaan AWS Health API	35
Memilih titik akhir untuk permintaan AWS Health API	35
Demo: Mengambil tujuh hari terakhir data acara secara terprogram	37
Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Java	37
Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Python	41
Tutorial: Menggunakan AWS Health API dengan contoh Java	43
Langkah 1: Inisialisasi kredensial	43
Langkah 2: Inisialisasi klien AWS Health API	44
Langkah 3: Gunakan operasi AWS Health API untuk mendapatkan informasi acara	44
Keamanan	48
Perlindungan data	49
Enkripsi data	50
Manajemen identitas dan akses	50
Audiens	51
Mengautentikasi dengan identitas	51
Mengelola akses menggunakan kebijakan	52
Bagaimana AWS Health bekerja dengan IAM	54
Contoh kebijakan berbasis identitas	60
Pemecahan masalah	73
Menggunakan Peran Terkait Layanan	77
AWS kebijakan terkelola untuk AWS Health	78
Penebangan dan pemantauan di AWS Health	84
Validasi kepatuhan	85
Ketahanan	85
Keamanan infrastruktur	86

Konfigurasi dan analisis kerentanan	86
Praktik terbaik keamanan	86
Berikan izin minimum kepada AWS Health pengguna	86
Lihat Dasbor Health	87
Integrasikan AWS Health dengan Amazon Chime atau Slack	87
Monitor untuk AWS Health acara	87
Agregasi acara AWS Health	88
Prasyarat	88
Mengaktifkan tampilan organisasi	89
Melihat tampilan organisasi	93
Menonaktifkan tampilan organisasi	98
Mengelola tampilan administrator yang didelegasikan untuk organisasi	99
Mendaftarkan akun administrator yang didelegasikan	100
Menghapus akun administrator yang didelegasikan	100
Monitoring untuk acara Kesehatan dengan EventBridge	101
Membuat EventBridge aturan untuk Wilayah AWS cakupan	102
Pengaturan ketersediaan tinggi (opsional)	103
Integrasi yang disederhanakan	103
Peristiwa global	103
Memantau acara-acara khusus akun dan publik untuk AWS Health	103
Aturan Backup untuk AWS Health Acara	105
Melihat daftar AWS Health acara berpaginasi di EventBridge	105
Menggabungkan AWS Health peristiwa menggunakan tampilan organisasi dan akses administrator yang didelegasikan	106
Mengintegrasikan pemantauan AWS Health acara dan pemberitahuan dengan JIRA dan ServiceNow	106
Mengonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa	107
Menggunakan API atau AWS Command Line Interface	108
Mengkonfigurasi Pengembang Amazon Q dalam aplikasi obrolan untuk mengirim pemberitahuan tentang acara	110
Prasyarat	110
Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa ..	112
Prasyarat	113
Buat aturan untuk EventBridge	117
Referensi: Amazon EventBridge skema AWS Health acara	120
AWS Health skema acara	120

Acara Kesehatan Masyarakat - Masalah operasional Amazon EC2	134
AWS Health Peristiwa Khusus Akun - Masalah Elastic Load Balancing API	135
AWS Health Acara khusus akun - acara pencadangan untuk Amazon EC2 Instance Store Drive Performance Terdegradasi	136
AWS Health Acara Khusus Akun - Pensiun Instans Amazon EC2	137
AWS Health Acara Khusus Akun - Acara Siklus Hidup yang Direncanakan Lambda	138
Pemantauan AWS Health	140
Pencatatan panggilan AWS Health API dengan AWS CloudTrail	140
AWS Health informasi di CloudTrail	141
Contoh: entri file AWS Health log	142
Riwayat dokumen	144
Pembaruan sebelumnya	156
.....	clvii

Apa itu AWS Health?

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

Semua pelanggan dapat menggunakan [AWS Health Dashboard AWS](#) , yang didukung oleh AWS Health API. Dasbor tidak memerlukan pengaturan, dan siap digunakan untuk [AWS pengguna yang diautentikasi](#). Untuk sorotan layanan lainnya, lihat [halaman detail AWS Health Dashboard halaman](#) .

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

Untuk mempelajari dasar-dasar tentang AWS Health dan istilah yang akan Anda temui saat Anda menggunakan layanan, Untuk memahami dasar-dasar AWS Health lihat [Konsep untuk AWS Health](#).

Catatan

- AWS Health Dasbor 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 AWS Business Support+, Enterprise AWS Support, atau AWS Unified Operations, Anda dapat menggunakan AWS Health API untuk berintegrasi dengan sistem internal dan pihak ketiga. Jika Anda menggunakan paket Wilayah AWS yang tidak menawarkan salah satu AWS Dukungan paket ini, atau jika Anda belum beralih ke salah satu paket ini, Anda dapat menggunakan AWS Health API dengan paket Business, Enterprise On-Ramp, atau Enterprise Support. Untuk informasi lebih lanjut, lihat [Referensi API AWS Health](#).
- Untuk informasi selengkapnya tentang AWS Dukungan paket yang tersedia, lihat [AWS Dukungan](#).

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 di perusahaan Anda Akun AWS.

Topik

- [AWS Health acara](#)
- [AWS Health Dasbor](#)
- [Kode jenis acara](#)
- [Kategori jenis acara](#)
- [Status acara](#)
- [Aksionabilitas](#)
- [Persona](#)
- [Entitas terpengaruh](#)
- [AWS Health acara di Amazon EventBridge](#)
- [AWS Health API](#)
- [Tampilan organisasi](#)
- [Notifikasi Pengguna AWS](#)

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 yang akan datang 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 publik](#)

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 [Amazon EventBridge](#) atau [Pemberitahuan AWS Pengguna 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) 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, lihat [Memulai AWS Health Dashboard Anda](#).

Jika Anda tidak memiliki akun, lihat [AWS Health Dasbor](#).

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 Konsol Manajemen AWS untuk melihat AWS Health Dasbor Anda di <https://health.aws.amazon.com/health/rumah>.

Untuk informasi selengkapnya, lihat [Memulai AWS Health Dashboard 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 Dasbor](#).

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.

Ini adalah praktik terbaik bahwa 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 tagihan yang belum dibayar 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_ISSUE`— Masalah 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 AI membutuhkan acara pemeliharaan, seperti memperbaiki masalah layanan.
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`Amazon 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.

Aksionabilitas

Actionability adalah bidang yang membantu Anda memprioritaskan acara Kesehatan berdasarkan apakah suatu tindakan diperlukan dari Anda. Peristiwa kesehatan mencakup status tindakan yang menunjukkan apakah Anda perlu mengambil tindakan untuk mengurangi risiko terhadap AWS sumber daya Anda atau jika acara tersebut bersifat informasi.

Bidang aksiabilitas dapat berisi salah satu nilai berikut:

- `ACTION_REQUIRED`: Acara dengan status ini memerlukan tindakan dari Anda untuk mengurangi potensi dampak terkait ketersediaan, penagihan, atau keamanan sumber daya Anda. AWS
- `ACTION_MAY_BE_REQUIRED`: Peristiwa dengan status ini mengkomunikasikan perubahan yang memerlukan tindakan, berdasarkan implementasi, dependensi, dan alur kerja spesifik Anda. Peristiwa ini memerlukan peninjauan Anda untuk menentukan apakah tindakan diperlukan.
- `INFORMATIONAL`Acara dengan status ini memberikan visibilitas berkelanjutan ke informasi operasional tentang AWS layanan yang Anda gunakan. Tidak ada tindakan segera yang diharapkan.

Note

Peristiwa kesehatan yang terkait dengan masalah layanan tidak menyertakan label aksionabilitas, karena kebutuhan akan tindakan pemulihan bergantung pada arsitektur aplikasi spesifik Anda.

Persona

Bidang persona menyediakan daftar kontak yang membantu Anda merutekan informasi yang relevan ke tim yang sesuai dalam organisasi Anda. Setiap acara Health dapat mencakup satu atau lebih persona berikut:

- **OPERATIONS:** Untuk acara yang berkaitan dengan kegiatan operasional dan ketersediaan layanan.
- **SECURITY:** Untuk acara yang berkaitan dengan pertimbangan keamanan.
- **BILLING:** Untuk acara dengan implikasi biaya potensial.

Misalnya, ketika AWS mengirim acara tentang akhir dukungan standar yang diubah menjadi dukungan yang diperluas, acara tersebut termasuk **BILLING** dalam daftar persona untuk **OPERATIONS** membantu memastikan informasi mencapai tim yang bertanggung jawab untuk manajemen biaya.

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 peristiwa AWS Health 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 AWS Business Support+, AWS Enterprise Support, atau AWS Unified Operations [AWS Dukungan](#) untuk menggunakan API. AWS Health Jika Anda memanggil AWS Health API dari akun yang tidak memiliki paket AWS Business Support +, Enterprise AWS Support, atau AWS Unified Operations, 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 AWS Health peristiwa di seluruh akun](#).

Notifikasi Pengguna AWS

AWS Health terintegrasi dengan [Notifikasi Pengguna AWS](#) sehingga Anda dapat dengan mudah menerima dan mengontrol pemberitahuan tentang peristiwa yang memengaruhi Anda Akun AWS dan layanan. Notifikasi Pengguna menawarkan pemberitahuan terkelola untuk AWS Health acara secara default. Anda dapat mengonfigurasi langganan ini untuk mengontrol seberapa sering Anda menerima pesan melalui agregasi berbasis waktu, jenis AWS Health acara apa yang Anda beri tahu, dan di mana pemberitahuan dikirimkan. Untuk memulai, buka Notifikasi Pengguna di [Konsol Manajemen AWS](#). Untuk informasi selengkapnya, lihat [Kelola AWS Health notifikasi di Notifikasi Pengguna AWS](#).

Memulai AWS Health Dashboard Anda

Anda dapat menggunakan AWS Health Dasbor Anda untuk mempelajari tentang AWS Health acara. Peristiwa ini dapat memengaruhi Anda Layanan AWS atau Akun 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 Anda AWS 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 memiliki Akun AWS, Anda dapat menggunakan [AWS Health Dasbor](#) 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.

Topik

- [Menyiapkan AWS akun Anda](#)
- [Melihat peristiwa akun Anda di AWS Health Dasbor](#)
- [Mengkonfigurasi Amazon EventBridge](#)
- [Kelola AWS Health notifikasi di Notifikasi Pengguna AWS](#)

Menyiapkan AWS akun Anda

Sebelum Anda dapat mengaktifkan AWS Health, Anda harus memiliki Akun AWS. Jika Anda tidak memiliki AWS akun, selesaikan langkah-langkah berikut untuk membuatnya.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/pendaftaran>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWS dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan [tugas yang memerlukan akses pengguna root](#).

AWS mengirim Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke [Konsol Manajemen AWS](#) sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat [Masuk sebagai pengguna root](#) di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

Untuk petunjuk, lihat [Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root \(konsol\) Anda](#) di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat [Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

Untuk petunjuknya, lihat [Membuat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

Untuk petunjuk, lihat [Menambahkan grup](#) di Panduan AWS IAM Identity Center Pengguna.

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 Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
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 peristiwa](#).

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 terakhir Layanan 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.

Your account health

Stay informed of important events affecting your AWS resources.

Configure EventBridge

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#) ↗

[Open and recent issues \(16\)](#) |
 [Scheduled changes \(0\)](#) |
 [Notifications \(3\)](#) |
 [Event log](#)

Open and recent issues (16)

View events that might affect your AWS infrastructure. **35 issues** were resolved in the past 24 hours.

Service: Elastic Compute Cloud
✕

Clear filter

< 1 >

Event summary

Operational issue - EC2 (Ohio)
 Last update: February 20, 2022 at 11:16:34 PM UTC-8
 us-east-2

Operational issue - EC2 (Ohio)
 Last update: February 17, 2022 at 11:56:09 PM UTC-8
 us-east-2

Operational issue - EC2 (N. Virginia)
 Last update: February 16, 2022 at 1:36:29 AM UTC-8
 us-east-1

Operational issue - EC2 (Ohio) [Back to list view](#) ↗

Details
Affected resources

Event data

<p>Service EC2</p> <p>Status Open</p> <p>Region / Availability Zone us-east-1</p> <p>Account specific No</p>	<p>Start time February 20, 2022 at 11:16:24 PM UTC-8</p> <p>End time -</p> <p>Category Issue</p> <p>Affected resources 1</p>
--	--

Description

[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.

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 peristiwa](#).

Anda dapat memilih opsi filter berikut untuk mempersempit hasil Anda:

- Zona Ketersediaan
- Waktu akhir
- Peristiwa
- Acara ARN
- Kategori acara
- Waktu pembaruan terakhir
- Region
- 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 log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X Clear filter

Last refreshed less than 1 min ago

Event	Status	Event category	Region / Zone	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 peristiwa

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, tetapi mungkin memakan waktu hingga 72 jam untuk mencerminkan status saat ini.

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

Example: AWS Health acara untuk AWS Lambda

Tangkapan layar berikut menunjukkan contoh acara untuk Lambda.

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section shows a search bar with 'Add filter' and a filter dropdown for 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)'. Below the filter is a 'Clear filter' button and a pagination indicator showing '1' item. The 'Event summary' section lists several operational issues, with the top one being 'Lambda operational issue' (last updated October 9, 2020 at 3:11:09 AM UTC-7 us-east-1).

The right side of the screenshot shows the 'Lambda operational issue' details. It has tabs for 'Details' (selected) and 'Affected resources'. The 'Event data' section contains the following information:

Event	Start time
Lambda operational issue	October 9, 2020 at 2:03:48 AM UTC-7
Status	End time
Closed	October 9, 2020 at 3:11:08 AM UTC-7
Region / Availability Zone	Affected resources
us-east-1	-
Category	
Issue	

The 'Description' section contains the following text:

[RESOLVED] Increased Invoke Error Rate

[02:03 AM PDT] We have identified an increase in invoke error rates in the US-EAST-1 Region and are working towards resolution.

[03:11 AM PDT] Between October 8 10:35 PM and October 9 2:25 AM PDT we experienced increased Lambda invoke error rates in the US-EAST-1 Region. The issue has been resolved and the service is operating normally.

Tipe peristiwa

Ada dua jenis AWS Health acara:

- Acara publik adalah acara layanan yang tidak spesifik untuk akun. Misalnya, jika ada masalah dengan Amazon EC2 di sebuah Wilayah 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 instans Wilayah AWS 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](#).
- Gunakan AWS Health API untuk mengembalikan eventScopeCode parameter. Peristiwa dapat memiliki nilai PUBLIC, ACCOUNT_SPECIFIC, atau NONE. Untuk informasi selengkapnya, lihat [DescribeEventDetails](#) operasi 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 Health acara 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.

Scheduled changes Table Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Any event

February 2024

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
28	29	30	31	1	2
	2 Upcoming	2 Upcoming 1 Completed			

30 January 2024 ⚙️ ✕

Scheduled events starting on 30 January 2024 (Showing 3 of 3) [View all on the table view](#)

- [EKS planned lifecycle event \(us-west-2\)](#)
Event status: **Upcoming**
- [EKS planned lifecycle event \(us-east-1\)](#)
Event status: **Upcoming**
- [EKS planned lifecycle event \(eu-west-1\)](#)
Event status: **Completed**

Tampilan sumber daya yang terpengaruh

AWS Health peristiwa mungkin menentukan sumber daya yang tepat yang terpengaruh. Anda dapat melihat sumber daya yang terpengaruh di tab Sumber Daya yang Terkena pada AWS Health acara tersebut. Untuk melihat status, pilih AWS Health acara. Status ditampilkan di tab sumber daya yang terpengaruh di panel samping. Untuk peristiwa siklus hidup yang direncanakan, AWS Health acara menyediakan pembaruan harian tentang status sumber daya yang terpengaruh.

AWS Health Peristiwa tingkat akun menampilkan ringkasan status sumber daya yang terpengaruh di bagian atas tab Sumber Daya yang Terdampak. 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](#)

Saat Anda mengakses tampilan organisasi, AWS Health acara menampilkan ringkasan status semua sumber daya yang terpengaruh untuk semua akun yang disertakan. Setelah 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.

Anda dapat mengunduh daftar sumber daya yang terpengaruh di tab sumber daya yang terpengaruh dalam format CSV atau JSON. Dalam tampilan organisasi, file yang diunduh mencakup semua sumber daya dalam akun yang terdaftar. Arahkan ke tingkat akun dalam tampilan organisasi untuk menyertakan hanya sumber daya untuk akun tersebut dalam file yang diunduh. Setiap sumber daya yang terpengaruh dalam file yang diunduh menyertakan Akun AWS ID, EventArn, nama entitas, entitiYarn, status, dan waktu terakhir sumber daya yang diperbarui. Jika filter diaktifkan, file yang diunduh hanya menyertakan hasil yang difilter.

Anda hanya dapat mengunduh satu file dalam satu waktu. File secara otomatis diunduh ke folder unduhan default browser Anda dan memiliki nama file preset berdasarkan Wilayah AWS, judul acara, tanggal mulai acara, dan tanggal unduhan.

The screenshot displays the AWS Health console interface. At the top, there are tabs for 'Open and recent issues (0)', 'Scheduled changes (1)', 'Other notifications (0)', and 'Event log'. The 'Scheduled changes (1)' tab is active, showing a table of upcoming events. Below this, a section titled 'Lambda planned lifecycle event' is visible, featuring a progress indicator with '4' affected resources. A legend indicates that 4 resources are 'Pending' (100%), 0 are 'Unknown' (0%), and 0 are 'Resolved' (0%). Below the legend, a table lists the affected resources with their ARNs, statuses, and last update times.

Resource ID / ARN	Resource status	Last update time
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUU6P	Pending	3 months ago
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy	Pending	3 months ago

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 Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
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 terintegrasi dengan AWS Organizations sehingga Anda dapat melihat peristiwa 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 AWS Health peristiwa di seluruh akun](#).


Enable organizational view

Key benefits




Organization-wide visibility

Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.



API access

If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. [Learn more](#)



Chat integration

Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. [Learn more](#)

Get started

1. Set up AWS Organizations

You must have an AWS organization with all features enabled.

✔ Success

Manage AWS Organizations [↗](#)
View documentation

2. Enable organizational view for AWS Health

After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard.

Enable organizational view
View documentation

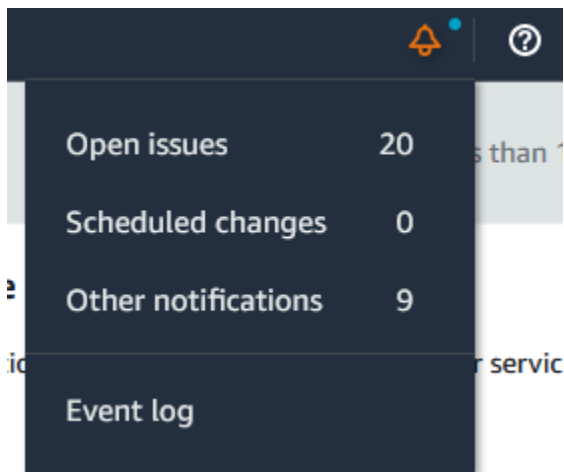
Peringatan untuk acara AWS Health

AWS Health Dasbor Anda memiliki ikon lonceng di bilah navigasi konsol dengan menu peringatan. Fitur ini menampilkan jumlah AWS Health peristiwa terbaru yang muncul di dasbor di setiap kategori. Ikon lonceng ini muncul di beberapa AWS konsol, seperti untuk Amazon EC2, Amazon Relational Database Service (Amazon RDS AWS 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.



Mengkonfigurasi 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 Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
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 peristiwa AWS Health dengan Amazon EventBridge](#).

Kelola AWS Health notifikasi di Notifikasi Pengguna AWS

AWS notifikasi terkelola Notifikasi Pengguna AWS memungkinkan Anda menerima dan mengelola pemberitahuan tentang peristiwa yang memengaruhi Anda Akun AWS dan layanan. Saat Anda menggunakan notifikasi AWS terkelola Notifikasi Pengguna AWS, Anda dapat menentukan kategori AWS Health acara mana yang akan diterima, mengatur tampilan organisasi untuk email, dan mendapatkan notifikasi gabungan alih-alih beberapa email serupa.

Anda dapat memilih saluran tambahan berikut untuk menerima AWS Health acara Anda melalui Notifikasi Pengguna AWS:

- Email
- Obrolan
- Pemberitahuan push ke AWS Console Mobile Application

Meskipun pemberitahuan ini tidak sedetail AWS Health alat langsung, mereka menyediakan cara yang efektif untuk memberi tahu pemangku kepentingan tentang masalah dan perubahan.

Note

Untuk visibilitas komprehensif ke detail AWS Health acara, termasuk sumber daya yang terpengaruh IDs, status saat ini (terbuka atau tertutup), dan status sumber daya, sebaiknya gunakan salah satu AWS Health alat berikut:

- AWS Health API
- Sumber `aws.health` di Amazon EventBridge
- The Dasbor Health

Alat-alat ini memberikan informasi paling rinci dan real-time tentang peristiwa yang sedang berlangsung dan perubahan yang mungkin memengaruhi beban kerja Anda.

Konfigurasi langganan notifikasi AWS terkelola untuk AWS Health acara

Untuk mengonfigurasi langganan notifikasi AWS terkelola, selesaikan langkah-langkah berikut:

1. Buka Notifikasi Pengguna di [Konsol Manajemen AWS](#).
2. Di panel navigasi, pilih langganan notifikasi AWS terkelola.
3. Anda dapat mengelola pemberitahuan AWS Health acara berdasarkan kategori. Untuk informasi selengkapnya, lihat [Menambahkan dan menghapus kontak akun untuk notifikasi AWS terkelola di Notifikasi Pengguna AWS](#).

Note

AWS Health pengiriman email yang dimigrasi ke notifikasi AWS terkelola di Notifikasi Pengguna AWS. Sejak 15 Desember 2025, Anda menerima email dari notifikasi AWS terkelola. Untuk informasi selengkapnya, lihat [Apa yang berubah dalam migrasi ke notifikasi AWS terkelola? di AWS pemberitahuan terkelola di FAQ Pemberitahuan AWS Pengguna](#).

AWS pemberitahuan terkelola di FAQ Pemberitahuan AWS Pengguna

Apa yang berubah dalam migrasi ke notifikasi AWS terkelola?

Secara default, email mengenai notifikasi terkelola dikirim ke kontak akun Anda yang ada (root, operasi, penagihan, dan alamat email keamanan). Email yang Anda terima dari notifikasi AWS terkelola berasal dari `health@aws.com` bukan `no-reply-aws@amazon.com`, dan format email berubah. Jika sebelumnya Anda mengatur aturan email untuk AWS Health notifikasi, seperti merutekan email dengan ID pengirim atau mengikis konten email, maka Anda harus memperbarui pengaturan ini agar sesuai dengan format email baru. Jika Anda memerlukan otomatisasi melalui pemberitahuan push, sebaiknya Anda mengevaluasi AWS Health peristiwa yang dikirim melalui Amazon EventBridge sebagai alternatif dari notifikasi terkelola.

Bagaimana cara kerja agregasi untuk email dan bagaimana cara mengaktifkan fitur ini?

AWS notifikasi terkelola menggabungkan AWS Health peristiwa yang memengaruhi beberapa akun dalam AWS Organizations organisasi yang sama menjadi satu notifikasi gabungan. Anda dapat melihat organisasi gabungan di pusat notifikasi akun manajemen. Notifikasi terkelola mengirimkan notifikasi agregat melalui email ke kontak akun manajemen. Untuk mengurangi duplikat email, notifikasi AWS terkelola mengirimkan satu notifikasi saat kontak akun dibagikan antara akun manajemen dan akun anggota.

Untuk mengaktifkan agregasi, Anda harus telah AWS Organizations mengonfigurasi dan memberikan akses tepercaya antara akun manajemen Anda dan Notifikasi Pengguna AWS layanan.

Untuk informasi selengkapnya, lihat [agregasi notifikasi AWS terkelola di Notifikasi Pengguna AWS](#).

Apakah saya harus mengaktifkan akses AWS Organizations tepercaya Notifikasi Pengguna AWS untuk menerima email gabungan dari notifikasi AWS terkelola?

Ya, akses tepercaya dengan Notifikasi Pengguna AWS from AWS Organizations diperlukan.

Apa perbedaan antara mengaktifkan akses tepercaya melalui AWS Organizations dengan AWS Health dan dengan? Notifikasi Pengguna AWS

Kepercayaan organisasi dan hak istimewa administrator yang didelegasikan terkait ditetapkan oleh layanan dan bertindak sebagai pagar pembatas terhadap izin yang berlebihan. Akses tepercaya untuk AWS Health memungkinkan tampilan organisasi untuk Dasbor Health AWS Health APIs, AWS Health peristiwa yang dikirim melalui Amazon EventBridge, dan konfigurasi notifikasi di Notifikasi Pengguna. Akses tepercaya untuk Notifikasi Pengguna AWS mengaktifkan pemberitahuan agregat dalam notifikasi AWS terkelola. Karena akses tepercaya tidak dibagikan, pengaturan administrator yang didelegasikan perlu ditambahkan secara terpisah untuk setiap layanan.

Apakah ada cara untuk menyimpan email teks biasa untuk kasus penggunaan khusus saya?

Tidak. AWS Health Email teks biasa saat ini dinonaktifkan setelah migrasi selesai. Jika Anda menggunakan aturan email untuk mengarahkan alur kerja yang berbeda, sebaiknya Anda mengevaluasi AWS Health peristiwa yang dikirim melalui Amazon EventBridge sebagai alternatif.

Apa yang sesuai dengan kategori notifikasi AWS terkelola dalam AWS Health skema?

Pemberitahuan operasi Kesehatan, Keamanan, dan Penagihan sesuai dengan pemberitahuan AWS Health akun dan perubahan terjadwal yang masing-masing memiliki persona operasi, keamanan, dan penagihan. AWS Health peristiwa dengan lebih dari satu tag persona dikirim melalui kategori Keamanan dan Penagihan. Masalah khusus akun termasuk acara kesehatan kategori masalah yang khusus untuk sebuah. Akun AWS

Acara layanan publik tidak tersedia melalui notifikasi AWS terkelola.

AWS Health Dasbor

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](#).

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 peristiwa, seperti Terdampak atau Terdegradasi
 - 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](#).

- 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.

- Di samping acara layanan yang sedang berlangsung, pilih ikon status



untuk melihat informasi selengkapnya tentang acara tersebut.

- (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.

Service history

List of services List of events


The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Standard Time (PST). To update your time zone, see [Time zone settings](#).

Q Add filter

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.

- (Opsional) Anda dapat melihat acara di zona waktu lokal atau UTC. Untuk informasi selengkapnya, lihat [Pengaturan zona waktu](#).
- (Opsional) Jika Anda memiliki akun, pilih Buka kesehatan akun Anda untuk masuk. Setelah masuk, Anda dapat melihat acara yang spesifik untuk akun Anda. Untuk informasi selengkapnya, lihat [Memulai AWS Health Dashboard Anda](#).

 Note

Meskipun umpan RSS tersedia untuk acara kesehatan, formatnya dapat berubah. Jadi, mengikis umpan RSS mungkin tidak menyediakan semua data yang relevan. Untuk secara terprogram menelan data acara kesehatan, kami sarankan untuk mengintegrasikan dengan Amazon EventBridge. Lihat informasi yang lebih lengkap di [Memantau peristiwa AWS Health dengan Amazon EventBridge](#).

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?](#)
- [Apa yang harus saya harapkan ketika saya menerima pemberitahuan peristiwa siklus hidup yang direncanakan?](#)
- [Model tanggung jawab bersama untuk ketahanan](#)
- [Mengakses acara siklus hidup yang direncanakan](#)

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 dasar 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.](#)

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 Tiongkok.

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 banyak ARNs 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 lead time minimum 180 hari untuk jurusan, jika memungkinkan. versions/changes and 90 days for minor versions/changes

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 Tiongkok.
- Pembaruan status sumber daya dilakukan secara asinkron dan berkala dan dapat mengalami penundaan hingga 72 jam dalam kesempatan langka.

Open and recent issues | **Scheduled changes** | Other notifications | Event log

Scheduled changes

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Table | Calendar

Q Add filter < 1 >

Event	Status	Region / Zone	Start time	End time	Affected resources
EKS planned lifecycle event	Upcoming	us-west-2	January 30, 2024 at 6:00:00 PM UTC-8		9 pending
DMS planned lifecycle event	Upcoming	us-east-1	January 29, 2024 at 6:00:00 PM UTC-8		1 pending
DMS planned lifecycle event	Upcoming	eu-west-1	January 29, 2024 at 6:00:00 PM UTC-8		10 pending
EKS planned lifecycle event	Completed	eu-west-1	January 30, 2024 at 6:00:00 PM UTC-8		-

EKS planned lifecycle event

Resource data is typically refreshed every 24 hours. ■ 0 Resolved No actions required 0%

Affected resources in account 745485236264 (5)

Q Add filter < 1 >

Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⏸ Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	⏸ Pending	15 days ago

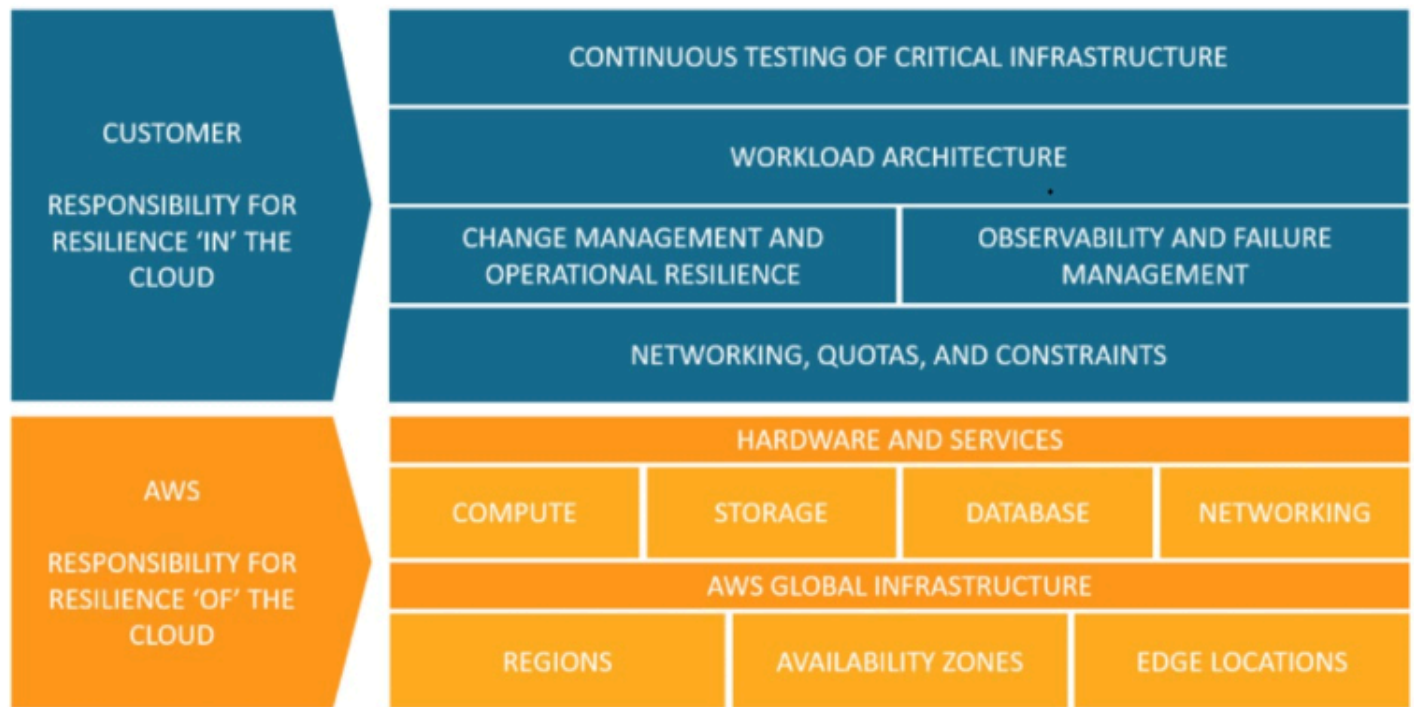
Setelah tanggal acara yang direncanakan berlalu:

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 akan berubah menjadi status `Closed`.
3. Jika Anda memiliki sumber daya yang luar biasa setelah tanggal perubahan yang tidak diselesaikan, maka AWS Health acara tetap terbuka selama 4 tahun setelah tanggal mulai atau berakhir acara (mana yang lebih baru). Setelah waktu ini, AWS Health acara 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 yang disediakan oleh AWS. 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](#)

Integrasi AWS Health dengan sistem lain menggunakan API AWS Health

AWS Health adalah layanan RESTful web 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 selengkapnya tentang AWS Health operasi dan parameter, lihat [Referensi AWS Health API](#).

Note

Anda harus memiliki paket AWS Business Support+, AWS Enterprise Support, atau AWS Unified Operations [AWS Dukungan](#) untuk menggunakan API. AWS Health Jika Anda menggunakan paket Wilayah AWS yang tidak menawarkan salah satu AWS Dukungan paket ini, atau jika Anda belum beralih ke salah satu paket ini, Anda dapat menggunakan AWS Health API dengan paket Business, Enterprise On-Ramp, atau Enterprise Support. Jika Anda memanggil AWS Health API dari Akun AWS yang tidak terdaftar di salah satu paket ini, maka Anda menerima `SubscriptionRequiredException` kesalahan.

Anda dapat menggunakan AWS SDKs untuk membungkus panggilan AWS Health REST API, yang dapat menyederhanakan pengembangan aplikasi Anda. Anda menentukan AWS kredensial Anda, dan pustaka ini menangani otentikasi dan penandatanganan permintaan untuk Anda.

AWS Health juga menyediakan AWS Health Dasbor Konsol Manajemen AWS yang dapat Anda gunakan untuk melihat dan mencari peristiwa dan entitas yang terpengaruh. Lihat [Memulai AWS Health Dashboard Anda](#).

Topik

- [Menandatangani permintaan AWS Health API](#)
- [Memilih titik akhir untuk permintaan AWS Health API](#)
- [Demo: Mengambil tujuh hari terakhir data AWS Health acara secara terprogram](#)
- [Tutorial: Menggunakan AWS Health API dengan contoh Java](#)

Menandatangani permintaan AWS Health API

Saat Anda menggunakan AWS SDKs atau AWS Command Line Interface (AWS CLI) untuk membuat permintaan AWS, alat ini secara otomatis menandatangani permintaan untuk Anda dengan kunci akses yang Anda tentukan saat Anda mengonfigurasi alat. Misalnya, jika Anda menggunakan demo titik akhir ketersediaan tinggi sebelumnya, Anda tidak perlu menandatangani permintaan sendiri. AWS SDK untuk Java

Contoh kode Java

Untuk contoh selengkapnya tentang cara menggunakan AWS Health API dengan AWS SDK untuk Java, lihat [contoh kode](#) ini.

Saat Anda mengajukan permintaan, kami sangat menyarankan agar Anda tidak menggunakan kredensial akun AWS root Anda untuk akses reguler. AWS Health Anda dapat menggunakan kredensial untuk membuat pengguna IAM. Untuk informasi selengkapnya, lihat [Mengunci Kunci Akses Pengguna Root AWS Akun Anda](#) di Panduan Pengguna IAM.

Jika Anda tidak menggunakan AWS SDKs atau AWS CLI, maka Anda harus menandatangani permintaan Anda sendiri. Kami menyarankan Anda menggunakan AWS Signature Version 4. Untuk informasi selengkapnya, lihat [Menandatangani Permintaan AWS API](#) di bagian Referensi Umum AWS.

Memilih titik akhir untuk permintaan AWS Health API


AWS Health API mengikuti arsitektur aplikasi Multi-region Arsitektur aplikasi dan memiliki dua titik akhir regional dalam konfigurasi aktif-pasif. Untuk mendukung failover DNS aktif-pasif, AWS Health menyediakan titik akhir tunggal, global. Anda dapat melakukan pencarian DNS di titik akhir global untuk menentukan titik akhir aktif dan Wilayah penandatanganan yang sesuai. AWS Ini membantu Anda mengetahui titik akhir mana yang akan digunakan dalam kode Anda, sehingga Anda bisa mendapatkan informasi terbaru dari AWS Health.

Saat Anda membuat permintaan ke titik akhir global, Anda harus menentukan kredensial AWS akses Anda ke titik akhir regional yang Anda targetkan dan mengonfigurasi penandatanganan untuk Wilayah Anda. Jika tidak, autentikasi Anda mungkin gagal. Untuk informasi selengkapnya, lihat [Menandatangani permintaan AWS Health API](#).

Untuk permintaan IPv6 -only, sebaiknya lakukan pencarian DNS di titik akhir global untuk menentukan aktif Wilayah AWS dan kemudian memanggil titik akhir dual-stack yang IPv6 didukung untuk Wilayah tersebut.

Tabel berikut menggambarkan konfigurasi default.

Deskripsi	Penandatanganan Wilayah	Titik akhir	Protokol
Aktif	us-east-1	health.us-east-1.a mazonaws.com (IPv4- hanya) health.us-east-1.a pi.aws (dan didukung) IPv4 IPv6	HTTPS
Pasif	us-east-2	health.us-east-2.a mazonaws.com (IPv4- hanya) health.us-east-2.a pi.aws (dan didukung) IPv4 IPv6	HTTPS
Global	us-east-1	global.health.amaz onaws.com	HTTPS

 **Note**
Ini adalah Wilayah penandatanganan titik akhir aktif saat ini.

Untuk menentukan apakah titik akhir adalah titik akhir aktif, lakukan pencarian DNS pada CNAME titik akhir global, lalu ekstrak Wilayah dari nama yang AWS diselesaikan.

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 memberi tahu Anda titik akhir mana yang harus Anda gunakan. AWS Health

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

Tip

Endpoint aktif dan pasif mengembalikan AWS Health data. 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.

Demo: Mengambil tujuh hari terakhir data AWS Health acara secara terprogram

Dalam contoh kode berikut, AWS Health gunakan pencarian DNS terhadap titik akhir global untuk menentukan titik akhir regional aktif dan Region penandatanganan. AWS Health menggunakan informasi ini untuk mengambil laporan dari tujuh hari terakhir data peristiwa. Kode memulai ulang alur kerja jika titik akhir aktif berubah.

Topik

- [Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Java](#)
- [Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Python](#)

Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Java

Prasyarat

Anda harus menginstal [Gradle](#).

Untuk menggunakan contoh Java

1. Unduh [demo titik akhir ketersediaan AWS 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 AWS kredensial 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: keluaran AWS Health acara

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

```
> 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 Dukungan [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 Referensi AWS SDK untuk Java API dan [kode sumber](#).
- [Untuk informasi selengkapnya tentang pustaka yang digunakan dalam demo ini untuk pencarian DNS, lihat dnsjava di GitHub](#)

Demo: Mengambil tujuh hari terakhir data AWS Health acara menggunakan Python

Prasyarat

Anda harus menginstal [Python 3](#).

Untuk menggunakan contoh Python

1. Unduh [demo titik akhir ketersediaan AWS 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 AWS kredensial 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: keluaran AWS Health acara

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

```
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 Dukungan [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?\n\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].

What is Transport Layer Security (TLS)?

Transport Layer Security (TLS Protocols) are cryptographic protocols designed to provide secure communication across a computer network [6].

What are AWS FIPS endpoints? All 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.

[1] <https://aws.amazon.com/blogs/security/tag/tls/>

[2] <https://aws.amazon.com/support/>

[3] <https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html>

[4] <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html>

[5] <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html>

[6] <https://aws.amazon.com/tools/>

[7] <https://aws.amazon.com/blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints/>

[8] https://en.wikipedia.org/wiki/Transport_Layer_Security

[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 selengkapnya tentang pustaka yang digunakan dalam demo ini untuk pencarian DNS, lihat toolkit dnspython dan kode sumber aktif.](#) GitHub

Tutorial: Menggunakan AWS Health API dengan contoh Java

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

Langkah 1: Inisialisasi kredensial

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

Membuat dan menginisialisasi sebuah [AWSCredentials](#) instance:

```
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: Inisialisasi klien AWS Health 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: Gunakan operasi AWS Health API untuk mendapatkan informasi acara

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 dari 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](#) . 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-faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, dan 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](#)
- [Identitas dan manajemen akses untuk AWS Health](#)
- [Penebangan dan pemantauan di AWS Health](#)
- [Validasi kepatuhan untuk AWS Health](#)
- [Ketahanan di AWS Health](#)
- [Keamanan infrastruktur di AWS Health](#)
- [Analisis konfigurasi dan kerentanan di AWS Health](#)
- [Praktik terbaik keamanan untuk AWS Health](#)

Perlindungan data di AWS Health

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di. 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 kredensi 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 AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. 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 saat diam

Semua data yang disimpan oleh AWS Health dienkripsi saat istirahat.

Enkripsi saat 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

Identitas dan manajemen akses 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

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [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 berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah AWS Health identitas dan akses](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana AWS Health bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [AWS Health contoh kebijakan berbasis identitas](#))

Mengautentikasi dengan identitas

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

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

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

AWS pengguna root akun

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

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

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

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

Peran IAM

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

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

Mengelola akses menggunakan kebijakan

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

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

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

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola 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. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

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 akses pengguna IAM ke peristiwa Amazon EC2 tertentu di AWS Health Dasbor.

Untuk informasi selengkapnya, lihat [Sumber daya](#).

Daftar kontrol akses

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ringkasan daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

AWS Health tidak mendukung ACLs.

Jenis-jenis kebijakan lain

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

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

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari 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 tag 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. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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 [DescribeEventDetails](#) API, Anda menyertakan `health: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. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

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

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

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 ARNs, lihat [Amazon Resource Names \(ARNs\) 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, [DescribeEvents](#) operasi 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 ARNs dengan koma.

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

AWS Health hanya mendukung izin tingkat sumber daya untuk acara kesehatan dan hanya untuk operasi dan API. [DescribeAffectedEntitiesDescribeEventDetails](#) Untuk informasi selengkapnya, lihat [Sumber daya- dan syarat berbasis aksi](#).

Untuk melihat daftar jenis sumber daya dan jenis AWS Health sumber daya ARNs, 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. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua 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 [DescribeAffectedEntities](#) dan [DescribeEventDetails](#) 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 memungkinkan Anda memberikan izin penggunaan ke akun lain berdasarkan penggunaan sumber daya. Anda juga dapat menggunakan kebijakan berbasis sumber daya untuk memungkinkan 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 principal 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 dan API. [DescribeAffectedEntitiesDescribeEventDetails](#) 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 tag 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 kredensi sementara dengan AWS Health

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensi keamanan sementara dengan memanggil operasi AWS STS API seperti [AssumeRole](#) atau [GetFederationToken](#)

AWS Health mendukung menggunakan kredensial 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 `OrganizationsServiceRolePolicy` AWS dikelola [Kesehatan](#). Kebijakan AWS terkelola memungkinkan AWS Health untuk mengakses acara kesehatan dari AWS akun lain di organisasi.

Anda dapat menggunakan [EnableHealthServiceAccessForOrganization](#) operasi untuk membuat peran terkait layanan di akun. Namun, jika Anda ingin menonaktifkan fitur ini, Anda harus terlebih dahulu memanggil [DisableHealthServiceAccessForOrganization](#) operasi. 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 AWS Health peristiwa di seluruh akun](#).

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 Konsol Manajemen AWS, 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 AWS Health konsol](#)
- [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 CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang 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 [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan AWS Health konsol

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](#).

AWSHealthFullAccessKebijakan 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 Dasbor 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

JSON

```
{
  "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:ListGroupsWithUser",
        "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 Dasbor tersedia untuk semua AWS akun. AWS Health API hanya tersedia untuk akun dengan paket AWS Business Support+, Enterprise AWS Support, atau AWS Unified Operations. Untuk informasi selengkapnya, lihat [Dukungan](#).

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

Secara default, pengguna IAM tidak memiliki akses ke AWS Health Dasbor 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 Dasbor 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 Dasbor dan AWS Health API, 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 kelompok APIs untuk AWS Health.

- Akun individual — Anda dapat menggunakan operasi seperti [DescribeEvents](#) dan [DescribeEventDetails](#) untuk mendapatkan informasi tentang AWS Health peristiwa untuk akun Anda.
- Akun organisasi — Anda dapat menggunakan operasi seperti [DescribeEventsForOrganization](#) dan [DescribeEventDetailsForOrganization](#) 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 Dasbor dan AWS Health. AWS Health mendukung kontrol akses ke acara berdasarkan `eventTypeCode` dan layanan.

Menjelaskan akses

Pernyataan kebijakan ini memberikan akses ke AWS Health Dasbor dan operasi `Describe*` AWS Health API apa pun. Misalnya, pengguna IAM dengan kebijakan ini dapat mengakses AWS Health Dasbor di Konsol Manajemen AWS dan memanggil operasi AWS Health `DescribeEvents` API.

Example: Mendeskripsikan akses

JSON

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

Menolak akses

Pernyataan kebijakan ini menolak akses ke AWS Health Dasbor dan AWS Health API. Pengguna IAM dengan kebijakan ini tidak dapat melihat AWS Health Dasbor di Konsol Manajemen AWS dan tidak dapat memanggil operasi AWS Health API mana pun.

Example: Tolak akses

JSON

```
{
  "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 masing-masing APIs, lihat [Tindakan yang Ditetapkan oleh AWS Health APIs dan Pemberitahuan](#) di Panduan Pengguna IAM.

Note

Anda harus menggunakan kredensi dari akun manajemen untuk organisasi untuk mengakses untuk. AWS Health APIs AWS Organizations Untuk informasi selengkapnya, lihat [Menggabungkan AWS Health peristiwa di seluruh akun](#).

Izinkan akses ke tampilan AWS Health organisasi

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

JSON

```
{
  "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*"
    }
  ]
}

```

Tolak akses ke tampilan AWS Health organisasi

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

JSON

```

{
  "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 [DescribeAffectedEntities](#) dan [DescribeEventDetails](#) API. 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 [DescribeAffectedEntities](#) dan [DescribeEventDetails](#) API mendukung izin tingkat sumber daya. Misalnya, Anda dapat membuat kebijakan untuk mengizinkan atau tolak spesifik peristiwa AWS Health .
- Operasi [DescribeEventDetailsForOrganization](#) API [DescribeAffectedEntitiesForOrganization](#) dan tidak mendukung izin tingkat sumber daya.
- Untuk informasi selengkapnya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk AWS Health APIs dan Pemberitahuan](#) di Referensi Otorisasi Layanan.

Example: Syarat berbasis tindakan

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

JSON

```
{
  "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.

JSON

```

{
  "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 Dasbor dan operasi AWS Health Describe* API, tetapi menolak akses ke AWS Health peristiwa apa pun dengan eventTypeCode yang cocok. AWS_EC2_*

JSON

```
{
  "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 [DescribeAffectedEntities](#) dan [DescribeEventDetails](#) operasi 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 Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan suatu 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 Dasbor atau operasi AWS Health API.

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

AWS Health API memerlukan paket AWS Business Support+, Enterprise AWS Support, atau AWS Unified Operations dari [AWS Dukungan](#) Jika Anda memanggil AWS Health API dari akun yang tidak memiliki paket AWS Business Support+, Enterprise AWS Support, atau AWS Unified Operations, 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 memberikan izin kepada orang atau aplikasi yang membutuhkan akses. Jika Anda menggunakan AWS IAM Identity Center

untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan kebijakan IAM ke peran IAM yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat [Set izin](#) di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan IAM Identity Center, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan yang memberi mereka izin yang tepat di AWS Health. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensial tersebut untuk mengakses. Untuk mempelajari selengkapnya tentang membuat pengguna, grup, kebijakan, dan izin IAM, lihat [Identitas dan Kebijakan IAM dan izin di IAM 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 (ACLs), 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, lihat [Bagaimana 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 [Akses sumber daya lintas akun di IAM di 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, lihat [AWS kebijakan terkelola untuk AWS Health](#).

Membuat peran terkait layanan untuk AWS Health

Anda tidak perlu membuat peran `AWSServiceRoleForHealth_Organizations` terkait layanan. Saat Anda memanggil [EnableHealthServiceAccessForOrganization](#) operasi, 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, silakan lihat [Membuat peran terkait 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 selengkapnya, 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 [DisableHealthServiceAccessForOrganization](#) operasi. Anda kemudian dapat menghapus peran melalui konsol IAM, IAM API, atau AWS Command Line Interface (AWS CLI).

Untuk menghapus `AWSServiceRoleForHealth_EventProcessor` peran, hubungi AWS Dukungan 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 [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS Health memiliki kebijakan terkelola berikut.

Daftar Isi

- [AWS kebijakan terkelola: AWSHealth_EventProcessorServiceRolePolicy](#)
- [AWS kebijakan terkelola: Health_OrganizationsServiceRolePolicy](#)
- [AWS kebijakan terkelola: AWSHealthFullAccess](#)
- [AWS Health pembaruan kebijakan AWS terkelola](#)

AWS kebijakan terkelola: 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.

JSON

```
{
  "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, lihat [AWS Health pembaruan kebijakan AWS terkelola](#).

AWS kebijakan terkelola: `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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk daftar perubahan kebijakan, lihat [AWS Health pembaruan kebijakan AWS terkelola](#).

AWS kebijakan terkelola: 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 AWS Health konsol](#).

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

JSON

```
{
  "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, lihat [AWS 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

Ubah	Deskripsi	Date
AWS kebijakan terkelola : AWSHealthFullAccess -	AWS Health telah memperluas AWSHealth FullAccess	16 Oktober 2023

Ubah	Deskripsi	Date
Pembaruan ke kebijakan yang tersedia	kebijakan ke AWS GovCloud (US) Regions dan Wilayah Tiongkok.	
AWS kebijakan terkelola: Health_OrganizationsService RolePolicy - 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 kejadian tertentu dan memicu tindakan otomatis dalam layanan AWS lainnya saat kejadian ini terjadi. Untuk informasi selengkapnya, lihat [Memantau peristiwa AWS Health 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 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 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. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi AWS Keamanan](#).

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 Dasbor Health 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 di 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 principal 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. Dasbor Health 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 Dasbor Health

Periksa Dasbor Health 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](#).

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 peristiwa AWS Health dengan Amazon EventBridge](#).

Menggabungkan AWS Health peristiwa di seluruh akun

Secara default, Anda dapat menggunakan AWS Health untuk melihat AWS Health peristiwa dari satu AWS akun. Jika Anda menggunakan AWS Organizations, Anda juga dapat melihat AWS Health acara secara 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 AWS Wilayah, akun, dan layanan tertentu.

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 pada AWS layanan yang mungkin memerlukan pembaruan atau perubahan kode.

Merupakan praktik terbaik untuk menggunakan fitur [Administrator Delegasi](#) untuk mendelegasikan akses ke tampilan AWS Health Organisasi ke akun anggota. Ini memudahkan tim operasional untuk mengakses AWS Health acara di organisasi Anda. Fitur Administrator Delegasi memungkinkan Anda untuk menjaga akun manajemen Anda dibatasi, sambil memberikan tim dengan visibilitas yang mereka butuhkan untuk bertindak atas AWS Health peristiwa.

Important

- AWS Health peristiwa yang dikirim untuk akun di organisasi Anda akan muncul dalam tampilan organisasi selama acara tersedia, hingga 90 hari, bahkan jika satu atau beberapa akun tersebut meninggalkan 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 peran IAM.

Anda juga dapat masuk sebagai root user (tidak disarankan) di akun manajemen organisasi Anda. Untuk informasi selengkapnya, lihat [Mengunci kunci akses pengguna root AWS akun Anda](#) di Panduan Pengguna IAM.

- Jika Anda masuk sebagai pengguna IAM, gunakan kebijakan IAM yang memberikan akses ke tindakan dan AWS Health Organizations, seperti kebijakan tersebut. [AWSHealthFullAccess](#) Untuk informasi selengkapnya, lihat [AWS Health contoh kebijakan berbasis identitas](#).

Topik

- [Mengaktifkan tampilan organisasi](#)
- [Melihat tampilan organisasi](#)
- [Menonaktifkan tampilan organisasi](#)
- [Mengelola tampilan administrator yang didelegasikan untuk organisasi](#)

Mengaktifkan tampilan organisasi

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

Tampilan organisasi tersedia di AWS Health konsol untuk semua AWS Dukungan paket tanpa biaya tambahan.

Note

Jika Anda ingin mengizinkan pengguna mengakses fitur ini di akun manajemen, mereka harus memiliki izin seperti [AWSHealthFullAccess](#) kebijakan. Untuk informasi selengkapnya, lihat [AWS Health contoh kebijakan berbasis identitas](#).

Enabling organizational view (Console)

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

Untuk melihat AWS Health Dasbor untuk organisasi Anda

1. Buka AWS Health Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.

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 AWS organisasi Anda, seperti membuat unit organisasi (OUs), pilih Kelola AWS Organizations.

Untuk informasi selengkapnya, lihat [Memulai dengan AWS Organizations](#) dalam Panduan Pengguna AWS Organizations .

Catatan

- Saat Anda mengaktifkan tampilan AWS Health organisasi, proses pemuatan akun awal berjalan di latar belakang dan mungkin memerlukan beberapa menit untuk menyelesaikannya. Anda dapat menutup AWS Health konsol dan kembali nanti, karena Anda tidak perlu menunggu proses selesai. Peristiwa kesehatan historis (yang dibuat sebelum Anda mengaktifkan fitur) mungkin membutuhkan waktu hingga 24 jam untuk muncul di tampilan organisasi Anda.
- Jika Anda memiliki paket AWS Business Support+, AWS Enterprise Support, atau AWS Unified Operations, Anda dapat memanggil operasi [DescribeHealthServiceStatusForOrganization](#) API untuk memeriksa status proses.
- Saat Anda mengaktifkan fitur ini, peran `AWSServiceRoleForHealth_Organizations` terkait layanan dengan kebijakan `Health_OrganizationsServiceRolePolicy` AWS terkelola akan diterapkan ke akun manajemen di organisasi. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk AWS Health](#).

Enabling organizational view (CLI)

Anda dapat mengaktifkan tampilan organisasi dengan menggunakan operasi [EnableHealthServiceAccessForOrganization](#) API.

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

Note

- Anda harus memiliki paket [Business](#), [Enterprise On-Ramp](#), atau Enterprise [Support](#) untuk memanggil API. AWS Health
- Anda harus menggunakan titik akhir Wilayah US East (N. Virginia).

Example

AWS CLI Perintah berikut mengaktifkan fitur ini dari AWS akun 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 memanggil operasi [EnableHealthServiceAccessForOrganizationAPI](#).

Python

```
import boto3

client = boto3.client('health', region_name='us-east-1')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Anda dapat menggunakan AWS SDK 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.EnableHealthServiceAccessForOrganizationRequest;
import
    software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
import
    software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
```

```
import
software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

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](#).

Saat Anda mengaktifkan fitur ini, [peran `AWSServiceRoleForHealth_Organizations` terkait layanan](#) dengan kebijakan `Health_OrganizationsServiceRolePolicy` AWS terkelola akan diterapkan ke akun manajemen di organisasi.

Note

Mengaktifkan fitur ini adalah proses asinkron dan membutuhkan waktu untuk menyelesaikannya. Anda dapat memanggil [DescribeHealthServiceStatusForOrganization](#) operasi untuk memeriksa status proses.

Melihat tampilan organisasi

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

Tampilan organisasi tersedia di AWS Health konsol untuk semua AWS Dukungan paket tanpa biaya tambahan.

Note

Jika Anda ingin mengizinkan pengguna mengakses fitur ini di akun manajemen, mereka harus memiliki izin seperti [AWSHealthFullAccess](#) kebijakan. Untuk informasi selengkapnya, lihat [AWS Health contoh kebijakan berbasis identitas](#).


Viewing organizational view events (Console)

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

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

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan dalam bucket S3.
- Selama AWS mempertahankan data kebijakan, ketika Anda membuka kembali akun yang ditutup, AWS menetapkan kembali akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun tersebut.
- Untuk informasi selengkapnya, lihat [Menutup akun](#).

 Important

Untuk pelanggan di AWS GovCloud (US) Wilayah:

- Sebelum menutup akun Anda, buat cadangan lalu hapus sumber daya akun. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

 Note

Saat Anda mengaktifkan fitur ini, AWS Health konsol dapat menampilkan acara publik dari [AWS Health Dasbor — Kesehatan layanan](#) selama 7 hari terakhir. Peristiwa publik ini tidak spesifik untuk akun di organisasi Anda. Acara dari AWS Health Dasbor — Layanan kesehatan memberikan informasi publik tentang ketersediaan AWS layanan regional.

Anda dapat melihat peristiwa tampilan organisasi di halaman berikut:

Masalah Terbuka dan Terbaru

Anda dapat menggunakan tab Terbuka dan masalah terbaru untuk melihat peristiwa yang mungkin memengaruhi AWS infrastruktur Anda, seperti perubahan Layanan AWS dan sumber daya yang memengaruhi organisasi Anda.

Untuk melihat acara tampilan organisasi

1. Buka AWS Health Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Buka dan masalah terbaru untuk melihat peristiwa yang dilaporkan baru-baru ini.
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

Perubahan Terjadwal

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

Pemberitahuan Lainnya

Gunakan tab Notifikasi untuk melihat semua pemberitahuan lain dan acara 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 untuk melihat AWS Health peristiwa untuk tampilan organisasi. Tata letak dan perilaku kolom mirip dengan tab Terbuka dan masalah terbaru, kecuali bahwa tab log Peristiwa menyertakan kolom tambahan dan opsi filter, seperti kategori Acara, Status, dan Waktu mulai.

Untuk melihat peristiwa tampilan organisasi di tab Log peristiwa

1. Buka AWS Health Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.

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

Viewing affected accounts and resources (Console)

Di bawah kesehatan organisasi Anda, Anda dapat melihat akun di organisasi Anda yang terpengaruh oleh acara dan sumber daya terkait. Misalnya, jika ada acara mendatang untuk pemeliharaan instans Amazon Elastic Compute Cloud (Amazon EC2), akun di organisasi Anda yang memiliki EC2 instans Amazon 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. Buka AWS Health Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih salah satu tab.
3. Pilih acara yang memiliki nilai untuk akun yang terpengaruh.
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.

Viewing organizational view events (CLI)

Setelah mengaktifkan fitur ini, AWS Health mulai merekam peristiwa yang memengaruhi akun di 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 menyimpan data kebijakan untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Pada akhir periode 90 hari, AWS secara permanen menghapus semua data kebijakan untuk akun.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan dalam bucket S3.
- Selama AWS mempertahankan data kebijakan, ketika Anda membuka kembali akun yang ditutup, AWS menetapkan kembali akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun tersebut.
- Untuk informasi selengkapnya, lihat [Menutup akun](#).

Important

Untuk pelanggan di AWS GovCloud (US) Wilayah:

- Sebelum menutup akun Anda, buat cadangan lalu hapus sumber daya akun. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

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

Example: Menjelaskan peristiwa tampilan organisasi

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

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

Menonaktifkan tampilan organisasi

Jika Anda tidak ingin menggabungkan peristiwa untuk organisasi Anda, Anda dapat menonaktifkan fitur ini dari akun manajemen atau Anda dapat menonaktifkan tampilan organisasi menggunakan operasi [DisableHealthServiceAccessForOrganization](#) API.

Disabling organizational view events (Console)

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. Buka AWS Health Dashboard Anda di <https://health.aws.amazon.com/health/rumah>.
2. Di panel navigasi, di bawah Kesehatan organisasi Anda, pilih Konfigurasi.
3. Pada halaman Aktifkan tampilan organisasi, pilih Nonaktifkan tampilan organisasi.

Setelah menonaktifkan fitur ini, AWS Health jangan lagi mengumpulkan peristiwa dari organisasi Anda. Namun, peran terkait layanan tetap ada di akun manajemen hingga Anda menghapusnya melalui konsol AWS Identity and Access Management (IAM), IAM API, atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan](#) dalam Panduan Pengguna IAM.

Disabling organizational view events (CLI)

Example

AWS CLI Perintah 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 operasi Organizations [Disable AWSService Access](#) API. Setelah Anda memanggil operasi ini, AWS Health berhenti menggabungkan peristiwa untuk semua akun lain di organisasi Anda. Jika Anda memanggil operasi AWS Health API untuk tampilan organisasi, AWS Health menampilkan kesalahan. AWS Health terus mengumpulkan acara kesehatan untuk AWS akun Anda.

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

Mengelola tampilan administrator yang didelegasikan untuk organisasi

[Dengan AWS Health, Anda dapat memanfaatkan fitur administrator yang didelegasikan dari AWS Organizations yang memungkinkan akun selain akun manajemen untuk melihat AWS Health peristiwa agregat di AWS Health Dasbor atau secara terprogram melalui API.](#) AWS Health Fitur administrator yang didelegasikan memberikan fleksibilitas bagi tim yang berbeda untuk melihat dan mengelola acara kesehatan di seluruh organisasi Anda. Ini adalah praktik terbaik AWS keamanan untuk mendelegasikan tanggung jawab di luar akun manajemen jika memungkinkan.

Daftar Isi

- [Mendaftarkan administrator yang didelegasikan untuk tampilan organisasi Anda](#)
- [Menghapus administrator yang didelegasikan dari tampilan organisasi](#)

Mendaftarkan administrator yang didelegasikan untuk tampilan organisasi Anda

Setelah mengaktifkan tampilan organisasi untuk organisasi, Anda dapat mendaftarkan hingga lima akun anggota di organisasi Anda sebagai administrator yang didelegasikan. Untuk melakukan ini, panggil operasi [RegisterDelegatedAdministrator](#) API. Setelah Anda mendaftarkan akun anggota, akun tersebut didelegasikan mengelola akun dan dapat mengakses tampilan AWS Health organisasi dari Dasbor. AWS Health Jika akun memiliki paket [Business](#), [Enterprise On-Ramp](#), atau [Enterprise Support](#), administrator yang didelegasikan dapat menggunakan AWS Health API untuk mengakses tampilan organisasi. AWS Health

Untuk membuat administrator yang didelegasikan, dari akun manajemen di organisasi Anda, panggil perintah AWS Command Line Interface (AWS CLI) berikut. Anda dapat menggunakan perintah ini dari akun manajemen atau dari akun yang dapat mengambil peran dengan AWS Identity and Access Management izin yang diperlukan. Dalam contoh perintah berikut, ganti ACCOUNT_ID dengan ID akun anggota yang ingin Anda daftarkan bersama dengan kepala AWS Health layanan "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 semua AWS Health peristiwa 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 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 bagi administrator yang didelegasikan, panggil operasi [DeregisterDelegatedAdministrator](#) API.

Dari akun manajemen organisasi Anda, hubungi AWS CLI perintah berikut untuk menghapus akun anggota sebagai administrator yang didelegasikan. Dalam contoh perintah berikut, ganti ACCOUNT_ID dengan ID akun anggota yang ingin Anda hapus.

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

Memantau peristiwa AWS Health 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 secara tahan lama dan upaya untuk berhasil menyampaikan acara EventBridge setidaknya sekali.
- EventBridge Aturan apa pun yang Anda buat hanya dapat menerima pemberitahuan untuk Anda Akun AWS. Untuk menerima acara organisasi untuk akun lain di dalam Anda AWS Organizations, lihat [Menggabungkan AWS Health peristiwa menggunakan tampilan organisasi dan akses administrator yang didelegasikan](#).
- Acara kesehatan masyarakat mungkin memakan waktu hingga satu jam untuk mulai mengirim setelah Anda membuat EventBridge aturan.

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

- [Membuat EventBridge aturan untuk Wilayah AWS cakupan](#)
- [Memantau acara-acara khusus akun dan publik untuk AWS Health](#)
- [Melihat daftar AWS Health acara berpaginasi di EventBridge](#)
- [Menggabungkan AWS Health peristiwa menggunakan tampilan organisasi dan akses administrator yang didelegasikan](#)
- [Mengintegrasikan pemantauan AWS Health acara dan pemberitahuan dengan JIRA dan ServiceNow](#)
- [Mengkonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di AWS Health](#)
- [Mengkonfigurasi Pengembang Amazon Q dalam aplikasi obrolan untuk mengirim pemberitahuan tentang peristiwa di AWS Health](#)
- [Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa di AWS Health](#)
- [Referensi: Amazon EventBridge skema AWS Health acara](#)

Membuat EventBridge aturan untuk Wilayah AWS cakupan

Anda dapat membuat EventBridge aturan untuk setiap Wilayah tempat Anda ingin menerima AWS Health acara. Misalnya, untuk menerima acara dari Wilayah Eropa (Frankfurt), Anda dapat membuat aturan untuk Wilayah ini.

Untuk meningkatkan keandalan AWS Health notifikasi, Anda dapat mengatur aturan di Wilayah cadangan khusus. Dalam AWS partisi standar, Wilayah Barat AS (Oregon) bertindak sebagai wilayah cadangan untuk semua Wilayah lainnya, sementara Wilayah AS Timur (Virginia N.) berfungsi sebagai cadangan untuk Wilayah Barat AS (Oregon). Ketika peristiwa kesehatan terjadi, mereka secara otomatis dikirim ke Wilayah utama dan Wilayah cadangan yang ditunjuk. Misalnya, jika

Anda memantau peristiwa di Wilayah Eropa (Frankfurt), maka setiap acara kesehatan dikirimkan ke Wilayah Eropa (Frankfurt) dan Wilayah AS Barat (Oregon). Sistem ini memastikan Anda terus menerima pemberitahuan kesehatan bahkan jika Wilayah utama Anda mengalami masalah. Untuk membuat aturan cadangan, ikuti prosedur untuk [Mengkonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di AWS Health](#).

Jika Anda memilih untuk tidak menggunakan fungsionalitas cadangan, maka Anda harus menambahkan filter ke aturan wilayah cadangan Anda. Misalnya, menerapkan filter untuk `detail.backupEvent = False`. Ini mencegah Anda menerima acara cadangan dari wilayah lain.

Pengaturan ketersediaan tinggi (opsional)

Jika Anda ingin membuat EventBridge integrasi dengan ketersediaan tinggi, pastikan Anda telah menerapkan aturan di Wilayah yang relevan dan cadangan, lalu terapkan de-duplikasi menggunakan `detail.communicationId`. Ini memastikan Anda menerima semua acara sambil menghindari duplikat. Untuk informasi selengkapnya, lihat [Referensi: Amazon EventBridge skema AWS Health acara](#).

Integrasi yang disederhanakan

Jika Anda ingin menangkap peristiwa dari beberapa Wilayah AWS, tetapi lebih suka mengkonfigurasi hanya satu aturan, maka integrasi yang disederhanakan adalah opsi yang sesuai. Untuk menerima AWS Health acara dari semua Wilayah di AWS partisi standar, Anda dapat mengatur aturan pusat di Wilayah Barat AS (Oregon). Aturan tunggal ini secara otomatis menggabungkan peristiwa dari semua wilayah partisi standar tempat Anda menerima acara Kesehatan. Namun, Anda tidak akan memiliki konfigurasi ketersediaan tinggi.

Peristiwa global

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 peristiwa global, Anda harus membuat aturan untuk Wilayah US East (N. Virginia).

Memantau acara-acara khusus akun dan 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.

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"
}
}
```

Aturan Backup untuk AWS Health Acara

Jika Anda memantau acara publik dari sebuah Wilayah AWS, kami sarankan Anda membuat aturan cadangan. Acara publik untuk dikirim AWS Health secara bersamaan ke Wilayah yang terkena dampak dan ke Wilayah cadangan ketika aturan yang valid ditetapkan di Wilayah yang terkena dampak.

AWS Health mengirimkan peristiwa khusus akun ke Wilayah yang terkena dampak dan ke Wilayah cadangan, terlepas dari aturan apa pun yang dikonfigurasi di Wilayah yang terkena dampak.

Kami menyarankan Anda menghapus duplikat AWS Health peristiwa menggunakan `eventARN` dan `communicationId` karena nilai-nilai ini tetap konsisten untuk AWS Health pesan yang dikirim ke Wilayah cadangan.

Melihat daftar AWS Health acara berpaginasi di EventBridge

AWS Health mendukung pagination AWS Health peristiwa ketika daftar `resources` atau `affectedEntities` menyebabkan ukuran pesan melebihi batas EventBridge ukuran pesan 256KB.

AWS Health termasuk semua `resources` dan `detail.affectedEntities` bidang dalam pesan. Jika daftar `resources` dan `detail.affectedEntities` nilai ini melebihi 256KB, kemudian AWS Health membagi acara kesehatan menjadi beberapa halaman dan mempublikasikan halaman ini sebagai pesan individual. EventBridge Setiap halaman mempertahankan nilai `eventARN` dan `communicationId` nilai yang sama untuk membantu menggabungkan kembali daftar `resources` 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 `detail.page` bidang untuk memproses hanya halaman pertama, yang menghilangkan pesan yang tidak perlu yang dibuat dari halaman berikutnya.

Dalam skema, setiap `communicationId` menyertakan nomor halaman tanda hubung setelah `communicationId`, bahkan ketika hanya ada 1 halaman. Bidang `detail.page` dan `detail.totalPages` jelaskan nomor halaman saat ini dan jumlah total halaman untuk AWS Health acara tersebut. 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 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](#).

Mengintegrasikan pemantauan AWS Health acara dan pemberitahuan dengan JIRA dan ServiceNow

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](#).

Mengkonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di AWS Health

Anda dapat membuat EventBridge aturan Amazon untuk mengintegrasikan AWS Health peristiwa secara terprogram dengan layanan, aplikasi, dan beban kerja lainnya. EventBridge menyediakan antarmuka konsol seret dan lepas serta API untuk menyiapkan aturan yang memicu saat AWS Health peristiwa yang cocok dibuat untuk akun atau organisasi Anda. Untuk mempelajari cara menyiapkan aturan EventBridge untuk menangkap AWS Health peristiwa, lihat [Membuat aturan di Amazon EventBridge](#) dan [Membuat aturan yang bereaksi terhadap peristiwa di Amazon EventBridge](#) di Panduan EventBridge Pengguna Amazon.

Bergantung pada integrasi Anda, EventBridge memungkinkan Anda menambahkan parameter ke EventBridge aturan untuk memfilter hanya AWS Health peristiwa yang ingin Anda integrasikan dengan kasus penggunaan Anda. Untuk kasus penggunaan respons insiden, Anda mungkin ingin fokus pada kategori `issue` acara dan layanan penting tertentu. Untuk kasus penggunaan manajemen perubahan seperti peristiwa siklus hidup yang direncanakan, Anda mungkin ingin fokus pada AWS Health peristiwa dengan `ACTION_REQUIRED` di bidang `Actionability`. Untuk mengintegrasikan dengan kasus penggunaan keamanan, Anda mungkin ingin fokus pada semua peristiwa dan AWS Health peristiwa AWS Health Penyalahgunaan dengan bidang `SECURITY` persona.

Anda dapat menggunakan contoh kasus penggunaan untuk memverifikasi bahwa aturan Anda menangkap peristiwa yang Anda butuhkan. Contoh kasus penggunaan tersedia di [Referensi: Amazon EventBridge skema AWS Health acara](#). Anda juga dapat menemukannya di EventBridge konsol di bawah opsi `Use Sample events provided in the Test event pattern - optional panel`

Menggunakan API atau AWS Command Line Interface

Untuk aturan baru atau yang sudah ada, gunakan operasi [PutRule](#) API atau `aws events put-rule` perintah untuk memperbarui pola peristiwa. Untuk melihat AWS CLI perintah contoh, lihat [put-rule](#) di AWS CLI Command Reference.

Example Contoh: Menyiapkan aturan untuk masalah hanya untuk layanan Amazon EC2

Pola peristiwa berikut membuat aturan untuk memantau peristiwa masalah untuk layanan Amazon EC2.

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

Example Contoh: Menyiapkan aturan untuk semua AWS Health peristiwa yang diperlukan tindakan, termasuk peristiwa siklus hidup yang direncanakan

Pola peristiwa berikut membuat aturan untuk memantau semua AWS Health peristiwa yang memerlukan tindakan, termasuk peristiwa siklus hidup yang direncanakan.

```
{
  "detail": {
    "eventTypeCategory": [
      "accountNotification",
      "scheduledChange"
    ],
    "actionability": [
```

```
    "ACTION_REQUIRED"
  ]
},
"detail-type": [
  "AWS Health Event"
],
"source": [
  "aws.health"
]
}
```

Example Contoh: Menyiapkan aturan untuk semua AWS Health acara untuk beberapa layanan dan kategori jenis acara

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

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

Mengkonfigurasi Pengembang Amazon Q dalam aplikasi obrolan untuk mengirim pemberitahuan tentang peristiwa di AWS Health

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 Pengembang Amazon Q dalam aplikasi obrolan. Anda dapat mengkonfigurasi Amazon Chime dan Slack. Untuk informasi selengkapnya, lihat [Memulai Pengembang Amazon Q di aplikasi obrolan](#) di Panduan Administrator Pengembang Amazon Q dalam aplikasi obrolan.
- 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 Pengembang Amazon Q di aplikasi obrolan

1. Ikuti prosedur [Mengkonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di 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 [Melihat daftar AWS Health acara berpaginasi di EventBridge](#).

```
"detail.page": ["1"]
```
 - b. Saat Anda memilih target di langkah 16, pilih topik SNS. Anda akan menggunakan topik SNS yang sama ini di Pengembang Amazon Q di konsol aplikasi obrolan.
 - c. Selesaikan prosedur lainnya untuk membuat aturan.
2. Arahkan ke [Pengembang Amazon Q di konsol aplikasi obrolan](#).

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 selengkapnya 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.

**AWS** APP 11:46 AM**AWS Health Event | us-east-1 | Account: 123456789012 | open**

Event type code: AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED

EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.\\n\\nYou can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>\\n\\n* What will happen to my instance?\\nYour instance will be stopped after the specified retirement date. You can start it agai...

[Show more](#)

Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT

**AWS** APP 12:08 PM**AWS Health Event | us-east-1 | Account: 123456789012 | open**

Event type code: AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION

We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain \\\\"Principal\\\\": \\\\"*\\\\" unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to \\\\"Authenticated Users\\\\" or \\\\"Everyone\\\\" unless your use case requires it.\\n\\nThe list of buckets with this configuration is associated with this event.\\n\\nThe following links provide an overv...

[Show more](#)

Start time: Sat, 20 Mar 2021 01:35:40 GMT

End time: Sat, 20 Mar 2021 01:36:40 GMT

Menjalankan operasi pada instans EC2 secara otomatis sebagai respons terhadap peristiwa di AWS Health

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 Konsol Manajemen AWS 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.

JSON

```
{
```

```
"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 ulasan, masukkan Nama, seperti *AutomationEVRolePolicy* 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 Konsol Manajemen AWS 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 *AutomationEVRolePolicy*, 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 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 Konsol Manajemen AWS 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 pilih Ubah hubungan kepercayaan.
5. Untuk Dokumen Kebijakan, salin JSON berikut, hapus kebijakan default, dan tempel JSON yang disalin di tempatnya.

JSON

```
{
  "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.

Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SSM Automation

Document

AWS-RestartEC2Instance

► **Configure document version**

▼ **Configure automation parameter(s)**

No Parameter(s)

Constant

Input Transformer

```
["Instances": "$resources"]
```

```
["InstanceId": <Instances>]
```

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

Create a new role for this specific resource

Use existing role

AutomationEVRole

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.

Referensi: Amazon EventBridge skema AWS Health acara


Berikut ini adalah skema untuk AWS Health acara. Isi parameter detail mengikuti tabel kedua. Sampel muatan disediakan setelah tabel skema.

AWS Health skema acara


AWS Health skema acara

Parameter	Deskripsi	Diperlukan
versi	EventBridge versi, saat ini "0".	Ya
id	Pengenal unik untuk EventBridge acara tersebut.	Ya
detail-tipe	Jenis detailnya. Untuk AWS Health acara, nilai yang didukung adalah &AWS Health Event dan AWS Health Abuse Event	Ya

Parameter	Deskripsi	Diperlukan
sumber	Sumber bus acara. Untuk AWS Health acara, nilai yang didukung adalah <code>aws.health</code>	Ya

Parameter	Deskripsi	Diperlukan
akun	<p>ID akun tempat AWS Health acara dikirim.</p> <div data-bbox="1068 445 1269 1759" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Untuk tampilan organisasi, ini adalah akun yang berbeda dari akun yang terpengaruh jika diterima di akun manajemen atau akun administrator yang didelegasikan.</p></div>	Ya

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

Parameter	Deskripsi	Diperlukan
region	<p>Tempat Wilayah AWS notifikasi dikirimkan ke.</p> <div data-bbox="1068 445 1273 1619"><p> Note</p><p>Bidang ini tidak menunjukkan Wilayah yang terkena dampak untuk AWS Health acara ini. Informasi tersebut dilaporkan dalam detail. entRegion</p></div>	Ya


Parameter	Deskripsi	Diperlukan
sumber daya	Menjelaskan daftar sumber daya yang terpengaruh, jika ada, dalam akun. Bidang ini kosong jika tidak ada sumber daya yang direferensikan.	Tidak
detail	Bagian yang berisi rincian AWS Health acara, seperti yang dijelaskan dalam tabel segera setelah yang satu ini.	Ya


Isi skema parameter 'detail'

Tabel berikut mendokumentasikan isi parameter detail dalam skema AWS Health acara.

AWS Health skema acara: konten parameter detail


konten parameter 'detail'	Deskripsi	Diperlukan
EventARN	Pengenal unik untuk AWS Health acara untuk Wilayah	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
	<p>tertentu, termasuk Wilayah dan ID peristiwa.</p> <div data-bbox="591 331 1029 604" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Acara ARN tidak unik untuk spesifik Akun AWS atau Wilayah.</p></div>	
layanan	yang Layanan AWS terpengaruh oleh AWS Health peristiwa tersebut. Misalnya, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift, atau Amazon Relational Database Service.	Ya


konten parameter 'detail'	Deskripsi	Diperlukan
eventTypeCode	<p>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 waktu mulai.</p> <div data-bbox="591 831 1029 1339" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Semua peristiwa siklus hidup baru yang direncanakan memiliki jenis acara. AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT</p> </div>	Ya
eventTypeCategory	Kode kategori peristiwa . Nilai yang didukung meliputi issue, accountNotification , investigation , dan scheduledChange .	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
eventScopeCode	Menunjukkan apakah AWS Health acara tersebut spesifik akun atau publik. Nilai yang didukung adalah ACCOUNT_SPECIFIC atau PUBLIC.	Ya
CommunicationID	<p>Pengidentifikasi unik untuk komunikasi ini untuk AWS Health acara tersebut.</p> <p>Pesan dengan ID komunikasi yang sama mungkin berupa pesan cadangan atau halaman dari satu AWS Health peristiwa. Pengenal ini dapat digunakan dengan ID akun untuk membantu menghapus duplikat pesan.</p> <p>Dengan dukungan pagination AWS Health acara, ID komunikasi menyertakan nomor halaman untuk menjaga ID komunikasi tetap unik di seluruh halaman, misalnya, 12345678910-1. Untuk informasi selengkapnya, lihat Melihat daftar AWS Health acara berpaginasi di EventBridge.</p>	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
startTime	<p>Waktu mulai AWS Health acara, dalam formatDoW, DD, MMM, YYYY, HH:MM:SS TZ.</p> <p>Waktu mulai bisa di masa depan untuk acara yang dijadwalkan.</p>	Ya
EndTime	<p>Waktu akhir AWS Health acara, dalam format:DoW, DD MMM YYYY HH:MM:SS TZ.</p> <p>Waktu akhir tidak dapat disediakan untuk acara yang dijadwalkan untuk masa depan.</p>	Tidak
lastUpdatedTime	<p>Waktu pembaruan terakhir untuk AWS Health acara tersebut, dalam formatDoW, DD MMM YYYY HH:MM:SS TZ.</p>	Ya
StatusCode	<p>Status AWS Health acara.</p> <p>Nilai yang didukung meliputiopen,closed, danupcoming.</p>	Ya
EventRegion	<p>Wilayah yang terkena dampak dijelaskan oleh AWS Health peristiwa ini.</p>	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
Deskripsi Acara	<p>Bagian yang menjelaskan an AWS Health peristiwa tersebut. Ini termasuk bidang untuk bahasa dan teks untuk menggambarkan acara.</p> <ul style="list-style-type: none">• <code>bahasa</code> — Kode untuk bahasa yang digunakan dalam AWS Health acara tersebut. Ini biasanya ditentukan oleh Wilayah tempat acara tersebut dipublikasikan. Misalnya, di <code>us-east-1</code> Wilayah, ini biasanya <code>en_US</code>.• <code>LatestDescription</code> — Menjelaskan AWS Health peristiwa seperti yang dirender dari AWS Health API dan biasanya muncul di dasbor. AWS Health <div data-bbox="623 1251 1029 1612" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"><p> Note</p><p>Untuk acara publik, ini hanya berisi pembaruan terbaru dan bukan seluruh riwayat acara.</p></div>	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
EventMetadata	<p>Metadata acara tambahan yang dapat disediakan untuk acara tersebut. AWS Health</p> <ul style="list-style-type: none"> • <metadata key 1>— String pasangan nilai kunci metadata: "keysting1": "keyvalue1" <p>Pasangan kunci-nilai untuk metadata peristiwa ditentukan oleh layanan yang mengirim acara. AWS Health</p>	Tidak
TerpengaruhDentitas	<p>Array yang menjelaskan nilai sumber daya dan status sumber daya yang terpengaruh dalam AWS Health acara.</p> <ul style="list-style-type: none"> • EntityValue — ID. resource/entity • LastUpdatedTime — Waktu ketika resource/entity status ini terakhir diperbarui, dalam format. DoW, DD MMM YYYY HH:MM:SS TZ • status — Status sumber daya/entitas yang terpengaruh. Nilai yang didukung meliputiIMPAIRED,UNIMPAIRED ,PENDING,RESOLVED, danUNKNOWN. 	Tidak

konten parameter 'detail'	Deskripsi	Diperlukan
halaman	<p>Halaman yang diwakili pesan ini. Untuk informasi selengkapnya, lihat Melihat daftar AWS Health acara berpaginasi di EventBridge.</p> <div data-bbox="591 493 1029 953" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Pagination hanya terjadi pada sumber daya. Jika batas ukuran 256KB terlampaui karena alasan lain, komunikasi gagal.</p> </div>	Ya
TotalPages	<p>Jumlah total halaman untuk acara kesehatan ini. Untuk informasi selengkapnya, lihat Melihat daftar AWS Health acara berpaginasi di EventBridge.</p> <p>Anda dapat menggunakan nilai ini untuk menentukan apakah Anda menerima semua halaman komunikasi multi-halaman untuk sebuah akun.</p>	Ya

konten parameter 'detail'	Deskripsi	Diperlukan
BackupEvent	<p>Bendera ini menyaring peristiwa pencadangan di wilayah cadangan yang ditunjuk dalam partisi jika pelanggan tidak ingin memanfaatkan redundansi. Nilai ini bisa benar atau salah.</p>	Ya
TerpengaruhAkun	<p>ID akun dari akun yang terkena dampak.</p> <p>Ini mungkin berbeda dari nilai di account bidang jika acara kesehatan ini dikirim ke akun yang merupakan bagian dari AWS Organizations dan diterima di akun manajemen atau akun administrator yang didelegasikan.</p>	Ya
kemampuan ditindaklanjuti	<p>Metadata untuk mengaktifkan penentuan terprogram peristiwa mana yang memerlukan tindakan tanpa inspeksi manual. Nilai yang mungkin (tunggal) dapat berupa ACTION_REQUIRED , ACTION_MAY_BE_REQUIRED , atau INFORMATIONAL .</p>	Tidak

konten parameter 'detail'	Deskripsi	Diperlukan
persona	Daftar metadata ini mengaktifkan penentuan terprogram dari pemangku kepentingan mana yang akan mengarahkan acara tersebut. Kemungkinan (beberapa) nilai adalah OPERATIONAL, SECURITY, dan BILLING.	Tidak

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",
    "backupEvent": "false",
    "affectedAccount": "123456789012",
    "personas": ["OPERATIONS"]
  }
}

```

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",
    "backupEvent": "false",
    "affectedAccount": "123456789012",

```

```

    "personas": ["OPERATIONS"]
  }
}

```

AWS Health Acara khusus akun - acara pencadangan untuk Amazon EC2 Instance Store Drive Performance Terdegradasi

```

{
  "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-east-1::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-east-1",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "affectedEntities": [{
      "entityValue": "i-abcd1111"
    }],
    "page": "1",
    "totalPages": "1",
    "backupEvent": "true",
    "affectedAccount": "123456789012",
    "personas": ["OPERATIONS"]
  }
}

```

```
}
}
```

AWS Health Acara Khusus Akun - Pensiun Instans Amazon EC2

```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2026-01-27T01:43:21Z",
  "region": "us-east-1",
  "detail": {
    "eventArn": "arn:aws:health:us-east-1::event/
AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED_90353408594353983",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED",
    "eventTypeCategory": "scheduledChange",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "1234abc01232a4012345678-1",
    "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
    "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
    "statusCode": "open",
    "eventRegion": "us-east-1",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "eventMetadata": {
      "keystring1": "valuestring1",
      "keystring2": "valuestring2",
      "keystring3": "valuestring3",
      "keystring4": "valuestring4",
      "truncated": "true"
    },
    "affectedEntities": [{
      "entityValue": "arn:aws:ec2:us-east-1:123456789012:instance/
i-1234567890abcdef0",
      "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
      "status": "PENDING"
    }],
    "affectedAccount": "123456789012",
```

```

    "page": "1",
    "totalPages": "1",
    "backupEvent": "false",
    "personas": ["OPERATIONS"],
    "actionability": "ACTION_REQUIRED"
  }
}

```

AWS Health Acara Khusus Akun - Acara Siklus Hidup yang Direncanakan Lambda

```

{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-01-27T01:43:21Z",
  "region": "us-west-2",
  "resources": ["arn:lambda-1-101002929", "arn:lambda-1-101002930",
"arn:lambda-1-101002931", "arn:lambda-1-101002932"],
  "detail": {
    "eventArn": "arn:aws:health:us-west-2::event/
AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT_90353408594353980",
    "service": "LAMBDA",
    "eventTypeCode": "AWS_LAMBDA_PLANNED_LIFECYCLE_EVENT",
    "eventTypeCategory": "scheduledChange",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "1234abc01232a4012345678-1",
    "startTime": "Thu, 27 Aug 2026 13:19:03 GMT",
    "lastUpdatedTime": "Thu, 27 Jan 2026 13:44:13 GMT",
    "statusCode": "open",
    "eventRegion": "us-west-2",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "eventMetadata": {
      "keystring1": "valuestring1",
      "keystring2": "valuestring2",
      "keystring3": "valuestring3",
      "keystring4": "valuestring4",

```

```
    "truncated": "true"
  },
  "affectedEntities": [{
    "entityValue": "arn:lambda-1-101002929",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:01:55 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002930",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:05:12 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002931",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:07:13 GMT",
    "status": "PENDING"
  }, {
    "entityValue": "arn:lambda-1-101002932",
    "lastUpdatedTime": "Thu, 26 Jan 2026 19:10:59 GMT",
    "status": "RESOLVED"
  }],
  "affectedAccount": "123456789012",
  "page": "1",
  "totalPages": "10",
  "backupEvent": "false",
  "personas": ["OPERATIONS"],
  "actionability": "ACTION_REQUIRED"
}
}
```

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 peristiwa AWS Health 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](#)

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 lain, lihat [Elemen userIdentity CloudTrail](#).

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 dienkrpsi 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 manapun 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, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan [DescribeEntityAggregates](#) operasi.

```
{
  "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
Diperbarui Mengonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di AWS Health	Menyederhanakan prosedur untuk membuat EventBridge aturan dengan menautkan ke Panduan EventBridge Pengguna Amazon untuk langkah-langkah pembuatan aturan umum. Topik sekarang berfokus pada AWS Health-spesifik penyaringan dan kasus penggunaan. Untuk informasi selengkapnya, lihat Mengonfigurasi EventBridge aturan untuk mengirim pemberitahuan tentang peristiwa di AWS Health .	Maret 13, 2026
Diperbarui AWS Health contoh Amazon EventBridge skema acara	Memperbarui contoh skema untuk menyertakan persona dan bidang tindakan. Contohnya termasuk Peristiwa Kesehatan Masyarakat untuk masalah operasional Amazon EC2, peristiwa khusus Akun untuk Elastic	Maret 13, 2026

Load Balancing API Issue dan peristiwa pencadangan Amazon EC2 Instance Store Drive Performance Degraded, dan Peristiwa Siklus Hidup yang Direncanakan Lambda. Untuk informasi selengkapnya, lihat [Referensi: Amazon EventBridge skema AWS Health acara](#).

[Diperbarui Kelola AWS Health pemberitahuan di Notifikasi Pengguna AWS](#)

Informasi yang diperbarui ke bagian ini untuk mencerminkan migrasi AWS Health acara ke Notifikasi Pengguna AWS. Untuk informasi selengkapnya, lihat [Mengelola AWS Health notifikasi di Notifikasi Pengguna AWS](#).

Desember 22, 2025

[Pemantauan yang diperbarui khusus akun dan acara publik untuk AWS Health](#)

Menambahkan informasi ke bagian ini yang merinci perilaku aturan cadangan untuk acara publik dan peristiwa khusus akun. Untuk informasi selengkapnya, lihat [Aturan cadangan untuk AWS Health acara](#).

Desember 11, 2025

[Menambahkan informasi tentang bidang Actionability dan Personas untuk acara Kesehatan](#)

Menambahkan informasi untuk bidang Actionability dan Personas di AWS Health bagian Konsep untuk dan isi Skema dari parameter 'detail' di bagian Referensi: AWS Health skema peristiwa . Amazon EventBridge Untuk informasi selengkapnya, lihat [Konsep untuk AWS Health](#) dan [Referensi: Amazon EventBridge skema AWS Health acara](#).

November 20, 2025

[Bagian yang diperbarui: Membuat EventBridge aturan untuk Wilayah AWS cakupan](#)

Informasi yang diperbarui untuk membuat EventBridge aturan. Untuk informasi selengkapnya, lihat [Membuat EventBridge aturan untuk Wilayah AWS cakupan](#).

November 3, 2025

[Bagian yang diperbarui: Kelola AWS Health pemberitahuan di Notifikasi Pengguna AWS](#)

Informasi terbaru untuk langkah-langkah Mengonfigurasi langganan notifikasi AWS terkelola untuk AWS Health acara. Untuk informasi selengkapnya, lihat [Mengelola AWS Health notifikasi di Notifikasi Pengguna AWS](#).

September 16, 2025

[Bagian yang diperbarui: Memantau peristiwa AWS Health dengan Amazon EventBridge](#)

Informasi yang diperbarui dalam catatan untuk AWS Health mengirimkan acara ke EventBridge. Untuk informasi selengkapnya, lihat [Memantau peristiwa AWS Health dengan Amazon EventBridge](#).

September 15, 2025

[Bagian yang diperbarui: AWS Health Dashboard](#)

Menghapus langkah-langkah opsional untuk berlangganan RSS feed untuk acara kesehatan. Ditambahkan catatan bahwa untuk menerima pemberitahuan untuk acara kesehatan, pelanggan dapat menggunakan EventBridge. Untuk informasi selengkapnya, lihat [AWS Health Dasbor](#).

Agustus 15, 2025

[Bagian yang diperbarui: Memantau peristiwa AWS Health dengan Amazon EventBridge](#)

Menghapus topik, Menginstansi peran terkait layanan untuk menggunakan Deteksi dan Respons AWS Insiden dalam [Memantau peristiwa dengan Amazon AWS Health EventBridge](#)

Agustus 8, 2025

[Bagian yang diperbarui: Memantau peristiwa AWS Health dengan Amazon EventBridge](#)

Menambahkan informasi ke bagian Catatan yang menunjukkan bahwa mungkin ada jeda hingga satu jam sebelum Anda mulai menerima pemberitahuan untuk Acara Kesehatan Masyarakat. Untuk informasi selengkapnya, lihat [Memantau peristiwa AWS Health dengan Amazon EventBridge](#)

Juli 22, 2025

[Bagian yang diperbarui: Mengaktifkan tampilan organisasi](#)

Menambahkan informasi ke bagian Catatan yang menunjukkan bahwa AWS Health secara otomatis menggabungkan semua peristiwa kesehatan historis di seluruh organisasi Anda saat Anda mengaktifkan tampilan organisasi. Peristiwa bersejarah mungkin memakan waktu hingga 24 jam untuk muncul dalam tampilan organisasi Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan tampilan organisasi](#)

Juni 27, 2025

[Bagian yang diperbarui: Menggabungkan AWS Health peristiwa di seluruh akun](#)

Catatan dihapus yang AWS Health tidak menampilkan peristiwa yang terjadi sebelum Anda mengaktifkan tampilan organisasi. Untuk informasi selengkapnya, lihat [Menggabungkan AWS Health peristiwa](#) di seluruh akun

Juni 27, 2025

[WorkDocs usang](#)

Referensi yang dihapus untuk tidak digunakan lagi WorkDocs dalam peristiwa siklus [hidup yang direncanakan untuk](#).
AWS Health

Juni 19, 2025

[Menambahkan catatan untuk timeline migrasi pemberitahuan AWS terkelola](#)

Menambahkan catatan mengenai tanggal-tanggal penting untuk migrasi email ke notifikasi AWS terkelola di Notifikasi Pengguna AWS. Untuk informasi selengkapnya, lihat [Mengelola AWS Health notifikasi di Notifikasi Pengguna AWS](#).

April 28, 2025

[Peristiwa siklus hidup terencana yang diperbarui](#)

Memperbarui peristiwa siklus hidup yang direncanakan untuk menunjukkan bahwa AWS Health acara tetap terbuka selama 4 tahun, bukan 90 hari untuk sumber daya yang belum terselesaikan. Untuk informasi selengkapnya, lihat [Apa yang harus saya harapkan ketika saya menerima pemberitahuan peristiwa siklus hidup yang direncanakan?](#) bagian dalam [Acara siklus hidup yang direncanakan](#) untuk AWS Health

April 18, 2025

Memperbarui deskripsi daftar sumber daya yang terpengaruh untuk peristiwa siklus hidup yang direncanakan	Daftar sumber daya yang terpengaruh untuk peristiwa siklus hidup yang direncanakan biasanya diperbarui setiap 24 jam sekali, tetapi mungkin membutuhkan waktu hingga 72 jam untuk mencerminkan status sumber daya saat ini. Untuk informasi selengkapnya, lihat bagian Detail acara di Melihat peristiwa akun Anda di AWS Health Dasbor .	April 7, 2025
Menambahkan FAQ untuk mengelola AWS Health notifikasi di Notifikasi Pengguna AWS	Untuk informasi selengkapnya, lihat Mengelola notifikasi di Notifikasi Pengguna AWS FAQ .	Februari 18, 2025
Menambahkan informasi mengenai permintaan IPv6 - only ke titik akhir.	Untuk informasi selengkapnya, lihat Memilih titik akhir untuk permintaan AWS Health API .	Januari 28, 2025
Kelola AWS Health notifikasi di Notifikasi Pengguna AWS	Untuk informasi selengkapnya, lihat Mengelola notifikasi di Notifikasi Pengguna AWS .	Januari 16, 2025
JSON yang dikoreksi dalam AWS Health acara Pemantauan dengan Amazon EventBridge	Untuk informasi selengkapnya, lihat Memantau AWS Health peristiwa dengan Amazon EventBridge .	September 3, 2024
Informasi terbaru tentang mengunduh sumber daya yang terpengaruh	Untuk informasi selengkapnya, lihat tampilan Sumber daya yang terpengaruh .	Juli 27, 2024

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 dalam 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 AWS terkelola untuk AWS Health .	16 Oktober 2023
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 lebih lanjut, 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 selengkapnya, 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 CloudWatch Acara Amazon. 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 Pengembang Amazon Q di aplikasi obrolan .	16 Maret 2021

[Dokumentasi diperbarui](#)

Topik berikut diperbarui:

29 Januari 2021

- 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](#)

[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 AWS Health peristiwa di seluruh akun.	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 AWS Health peristiwa di seluruh akun.	18 Desember 2019
Menambahkan bagian baru “Kondisi Berbasis Sumber Daya dan Tindakan” untuk menjelaskan pembatasan Acara yang dijual oleh API. AWS Health	Lihat Identitas dan manajemen akses untuk AWS Health.	2 Agustus 2018
Menambahkan catatan tentang visibilitas AWS Health informasi.	Lihat Identitas dan manajemen akses untuk AWS Health.	16 Agustus 2017
Rilis pelayanan.	AWS Health dirilis.	1 Desember 2016

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