Panduan Pengguna

AWS CloudTrail



Versi 1.0

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

AWS CloudTrail: Panduan Pengguna

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

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

Table of Contents

Apa itu AWS CloudTrail? 1
Mengakses CloudTrail 3
CloudTrail konsol 3
AWS CLI 4
CloudTrail API 4
AWS SDK 4
Bagaimana cara CloudTrail kerja 4
CloudTrail Riwayat acara 5
CloudTrail Penyimpanan data danau dan acara 5
CloudTrail Dasbor danau 9
CloudTrail jalan setapak 10
CloudTrail Insights acara 15
CloudTrail saluran 16
Konsep 17
CloudTrail acara 17
Riwayat acara 69
Jalan setapak 69
Jejak organisasi 71
CloudTrail Penyimpanan data danau dan acara 73
CloudTrail Wawasan 74
Tanda 74
AWS Security Token Service dan CloudTrail 74
Acara layanan global 75
Wilayah yang Didukung 76
Layanan dan integrasi yang didukung 80
AWS integrasi layanan dengan log CloudTrail 81
CloudTrail Integrasi dengan Amazon EventBridge 83
CloudTrail Integrasi dengan AWS Organizations 84
CloudTrail Integrasi dengan AWS Control Tower 84
CloudTrail integrasi dengan Amazon Security Lake 85
CloudTrail Integrasi danau dengan Amazon Athena 85
CloudTrail Integrasi danau dengan AWS Config 85
CloudTrail Integrasi danau dengan AWS Audit Manager 85
AWS topik layanan untuk CloudTrail 85

Layanan tidak didukung 113
Kuota di AWS CloudTrail 114
CloudTrail kuota sumber daya 114
Kuota transaksi per detik (TPS) dalam CloudTrail 121
CloudTrail tutorial 122
Berikan izin untuk digunakan CloudTrail 122
Lihat riwayat acara 124
Buat jejak untuk mencatat peristiwa manajemen 126
Melihat file log Anda 130
Membuat penyimpanan data peristiwa untuk peristiwa data S3 131
Melihat CloudTrail biaya dan penggunaan 139
Penggunaan AWS Budgets untuk mengelola biaya 143
Membuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake 144
Mengelola biaya CloudTrail jejak 145
Konfigurasi jejak 145
Lihat juga 146
Mengelola biaya CloudTrail Danau 147
Opsi harga toko data acara 147
Memahami biaya CloudTrail Danau 148
Rekomendasi tentang bagaimana Anda dapat mengurangi biaya 151
Lihat juga 152
Bekerja dengan riwayat CloudTrail acara 153
Keterbatasan sejarah acara 154
Melihat acara manajemen terbaru dengan konsol 155
Menavigasi antar halaman 156
Menyesuaikan tampilan 156
Acara penyaringan CloudTrail 158
Melihat detail untuk suatu acara 160
Mengunduh acara 160
Melihat sumber daya yang direferensikan dengan AWS Config 161
Melihat acara manajemen terbaru dengan AWS CLI 162
Prasyarat 164
Mendapatkan bantuan baris perintah 164
Mencari acara 165
Menentukan jumlah acara untuk kembali 166

Mencari acara berdasarkan rentang waktu 166
Mencari acara berdasarkan atribut 167
Menentukan halaman hasil berikutnya 168
Mendapatkan masukan JSON dari sebuah file 169
Bidang keluaran pencarian 170
Bekerja dengan CloudTrail Wawasan 173
Biaya untuk acara Insights 174
Penyampaian acara Insights 178
Pencatatan peristiwa Wawasan dengan CloudTrail konsol 179
Mengaktifkan CloudTrail Wawasan pada jejak yang ada dengan konsol 180
Mengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang ada dengan konsol 180
Pencatatan peristiwa Wawasan dengan AWS CLI 181
Pencatatan peristiwa Wawasan untuk jejak menggunakan AWS CLI 182
Pencatatan peristiwa Wawasan untuk penyimpanan data peristiwa menggunakan AWS CLI 184
Melihat acara Wawasan untuk jalur 187
Melihat peristiwa Wawasan untuk jalur dengan konsol 188
Melihat acara Wawasan untuk jalur dengan AWS CLI 197
Melihat peristiwa Wawasan untuk penyimpanan data acara 215
Melihat dasbor Wawasan untuk penyimpanan data peristiwa 216
Melihat contoh kueri untuk acara Insights 217
Bekerja dengan CloudTrail Danau 219
CloudTrail Perubahan ketersediaan danau 219
Dukungan berkelanjutan untuk penyimpanan data acara yang ada 220
Opsi migrasi 221
Membandingkan arsitektur 221
Prosedur migrasi 223
Sumber daya tambahan 226
CloudTrail Penyimpanan data acara danau 226
CloudTrail Kueri danau 228
CloudTrail Dasbor danau 228
CloudTrail Integrasi danau 229
Sumber daya tambahan 230
CloudTrail Daerah yang didukung Danau 230
CloudTrail Konsep dan terminologi danau 232

Menyimpan data acara ... 233
Integrasi ... 235
Kueri ... 236
Dasbor ... 236
Penyimpanan data acara ... 237
Buat, perbarui, dan kelola penyimpanan data peristiwa dengan konsol ... 239
Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI ... 299
Mengelola siklus hidup penyimpanan data acara ... 332
Salin peristiwa jejak ke penyimpanan data peristiwa ... 334
Menyatukan penyimpanan data acara ... 356
Menyimpan data acara organisasi ... 369
Integrasi ... 376
Buat integrasi dengan CloudTrail mitra dengan konsol ... 377
Buat integrasi khusus dengan konsol ... 380
Buat, perbarui, dan kelola integrasi CloudTrail Lake dengan AWS CLI ... 384
Informasi tambahan tentang mitra integrasi ... 393
CloudTrail Skema acara integrasi danau ... 395
Dasbor ... 403
Prasyarat ... 404
Batasan ... 405
Dukungan Wilayah ... 405
Izin yang diperlukan ... 406
Lihat dasbor terkelola ... 410
Aktifkan dasbor Sorotan ... 427
Nonaktifkan dasbor Sorotan ... 428
Buat dasbor khusus ... 428
Mengatur jadwal penyegaran untuk dasbor kustom ... 432
Nonaktifkan jadwal penyegaran untuk dasbor khusus ... 433
Ubah perlindungan penghentian ... 433
Hapus dasbor khusus ... 434
Buat, perbarui, dan kelola dasbor dengan AWS CLI ... 435
Kueri ... 228
Alat editor kueri ... 453
Buat kueri CloudTrail Danau dari petunjuk bahasa alami ... 454
Lihat contoh kueri ... 462
Membuat atau mengedit kueri ... 464

Menjalankan kueri dan menyimpan hasil kueri ... 466
Lihat hasil kueri ... 471
Meringkas hasil kueri dalam bahasa alami ... 473
Unduh hasil kueri yang disimpan ... 475
Validasi hasil kueri yang disimpan ... 477
Optimalkan kueri ... 491
Jalankan dan kelola kueri CloudTrail Lake dengan AWS CLI ... 495
CloudTrail Kendala Lake SQL ... 501
Fungsi, kondisi, dan bergabung dengan operator yang didukung ... 502
Dukungan kueri multi-tabel tingkat lanjut ... 503
Skema SQL yang didukung untuk penyimpanan data acara ... 504
Skema yang didukung untuk bidang catatan CloudTrail acara ... 504
Skema yang didukung untuk bidang catatan acara CloudTrail Insights ... 508
Skema yang didukung untuk AWS Config file catatan item konfigurasi ... 510
Skema yang didukung untuk laporan catatan AWS Audit Manager bukti ... 511
Skema yang didukung untuk bidang AWS non-acara ... 513
CloudWatch Metrik yang didukung ... 514
Bekerja dengan jalan CloudTrail setapak ... 518
Membuat jejak untuk Anda Akun AWS ... 519
Membuat dan memperbarui jejak dengan konsol ... 520
Membuat, memperbarui, dan mengelola jalur dengan AWS CLI ... 554
Membuat beberapa jalur ... 588
Membuat jejak untuk sebuah organisasi ... 591
Pindah dari jejak akun anggota ke jalur organisasi ... 595
Bersiaplah untuk membuat jejak untuk organisasi Anda ... 596
Membuat jejak untuk organisasi Anda di konsol ... 600
Membuat jejak untuk organisasi dengan AWS CLI ... 610
Pemecahan masalah ... 618
Memahami jalur Multi-wilayah dan Wilayah keikutsertaan ... 620
Apa keuntungan dari jalur Multi-wilayah? ... 621
Apa yang terjadi ketika Anda membuat jejak Multi-wilayah? ... 621
Apa yang terjadi jika Anda mengaktifkan Region keikutsertaan? ... 622
Apa yang terjadi jika Anda menonaktifkan Wilayah keikutsertaan? ... 622
Menyalin acara jejak ke Danau CloudTrail ... 622
Pertimbangan untuk menyalin acara jejak ... 624
Izin yang diperlukan untuk menyalin peristiwa jejak ... 626

Salin peristiwa jejak ke penyimpanan data acara yang ada menggunakan CloudTrail konsol ... 630
Mendapatkan dan melihat file CloudTrail log Anda ... 633
Menemukan file CloudTrail log Anda ... 634
Mengunduh file CloudTrail log Anda ... 636
Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail ... 637
Mengkonfigurasi CloudTrail untuk mengirim notifikasi ... 638
Menggunakan AWS CloudTrail dengan antarmuka VPC endpoint ... 640
Wilayah ... 641
Buat titik akhir VPC untuk CloudTrail ... 641
Membuat kebijakan titik akhir VPC untuk CloudTrail ... 641
Subnet bersama ... 645
Persyaratan penamaan ... 645
CloudTrail persyaratan penamaan sumber daya ... 646
Persyaratan penamaan ember Amazon S3 ... 646
AWS KMS persyaratan penamaan alias ... 647
Akun AWS penutupan dan jalan setapak ... 647
Konfigurasikan CloudTrail pengaturan ... 649
Administrator delegasi dalam organisasi ... 649
Izin yang diperlukan untuk menetapkan administrator yang didelegasikan ... 653
Menambahkan administrator yang CloudTrail didelegasikan ... 655
Menghapus administrator yang CloudTrail didelegasikan ... 656
Saluran terkait layanan ... 656
Melihat saluran terkait layanan dengan menggunakan konsol ... 657
Melihat saluran terkait layanan dengan menggunakan AWS CLI ... 657
Memahami CloudTrail peristiwa ... 661
Peristiwa manajemen ... 662
Peristiwa data ... 664
Peristiwa data yang didukung oleh AWS CloudTrail ... 665
Acara aktivitas jaringan ... 714
Insights acara ... 718
Peristiwa manajemen ... 721
Peristiwa manajemen ... 722
Membaca dan menulis acara ... 723
Pencatatan acara manajemen dengan Konsol Manajemen AWS ... 724
Pencatatan acara manajemen dengan AWS CLI ... 728

Pencatatan acara manajemen dengan AWS SDK 743
Peristiwa data 743
Peristiwa data 746
Read-only dan acara khusus tulis 796
Mencatat peristiwa data dengan Konsol Manajemen AWS 797
Mencatat peristiwa data dengan AWS Command Line Interface 807
Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut 820
Mengagregasikan peristiwa data 834
Peristiwa data pencatatan untuk AWS Config kepatuhan 839
Mencatat peristiwa data dengan AWS SDK 839
Menekan peristiwa rekursif dengan logging rekursif 840
Acara aktivitas jaringan 841
Bidang pemilih acara lanjutan untuk acara aktivitas jaringan 845
Mencatat peristiwa aktivitas jaringan dengan Konsol Manajemen AWS 849
Mencatat peristiwa aktivitas jaringan dengan AWS Command Line Interface 852
Mencatat peristiwa dengan AWS SDK 875
Tambahkan kunci tag sumber daya dan kunci kondisi global IAM ke acara 875
Layanan AWS tag sumber daya pendukung 877
Layanan AWS mendukung kunci kondisi global IAM 879
Contoh acara 882
CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan 883
Urutan pemotongan bidang untuk ukuran acara maksimum 1 MB 897
Contoh ShareDeventid 898
CloudTrail merekam konten untuk acara agregat 899
Contoh acara agregat 904
CloudTrail merekam konten untuk acara Insights untuk jalur 906
Contoh blok `InsightDetails` 912
CloudTrail merekam konten untuk acara Wawasan untuk penyimpanan data acara 914
CloudTrail elemen userIdentity 919
Contoh 919
Bidang 922
Nilai untuk AWS STS API dengan SAFL dan federasi identitas web 932
AWS STS identitas sumber 933
Peristiwa non-API yang ditangkap oleh CloudTrail 936
Layanan AWS acara 937
Konsol Manajemen AWS acara masuk 938

CloudTrail file log 953
Menerima file CloudTrail log dari beberapa Wilayah 955
Mengelola konsistensi data 956
Memantau file CloudTrail log dengan Amazon CloudWatch Logs 957
Mengirim acara ke CloudWatch Log 958
Membuat CloudWatch alarm untuk CloudTrail acara: contoh 966
Berhenti CloudTrail dari mengirim acara ke CloudWatch Log 973
CloudWatch grup log dan penamaan aliran log untuk CloudTrail 974
Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan 975
Menerima file CloudTrail log dari beberapa akun 977
Menyunting akun pemilik bucket IDs untuk peristiwa data yang dipanggil oleh akun lain 978
Menyetel kebijakan bucket untuk beberapa akun 979
Buat jejak di akun tambahan 981
Berbagi file CloudTrail log antar AWS akun 984
Bagikan file log antar akun dengan mengambil peran 984
Memvalidasi CloudTrail integritas file log 994
Mengapa menggunakannya? 995
Cara kerjanya 995
Mengaktifkan validasi integritas file log untuk CloudTrail 996
Memvalidasi integritas file CloudTrail log dengan AWS CLI 997
CloudTrail struktur file digest 1008
Implementasi kustom validasi integritas file CloudTrail log 1016
CloudTrail contoh file log 1027
CloudTrail format nama file log 1028
Contoh file log 1028
Menggunakan Pustaka CloudTrail Pemrosesan 1041
Persyaratan minimum 1042
Memproses CloudTrail log 1042
Topik lanjutan 1048
Sumber daya tambahan 1054
Keamanan 1055
Perlindungan data 1056
Identity and Access Management 1057
Audiens 1058
Mengautentikasi dengan identitas 1058

Mengelola akses menggunakan kebijakan 1060
Bagaimana AWS CloudTrail bekerja dengan IAM 1061
Identity-based contoh kebijakan 1069
Resource-based contoh kebijakan 1087
Kebijakan bucket Amazon S3 untuk CloudTrail 1095
Kebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake 1104
Kebijakan topik Amazon SNS untuk CloudTrail 1107
Pemecahan masalah 1114
Menggunakan Peran Terkait Layanan 1118
AWS kebijakan terkelola 1125
Validasi kepatuhan 1128
Ketahanan 1128
Keamanan infrastruktur 1129
Pencegahan "confused deputy" lintas layanan 1130
Praktik terbaik keamanan 1131
CloudTrail praktik terbaik keamanan detektif 1131
CloudTrail praktik terbaik keamanan preventif 1133
Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS) 1137
Mengaktifkan enkripsi file log 1138
Memberikan izin untuk membuat kunci KMS 1140
Konfigurasi AWS KMS kebijakan utama untuk CloudTrail 1140
Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol 1156
Mengaktifkan dan menonaktifkan enkripsi untuk file CloudTrail log, mencerna file dan penyimpanan data peristiwa dengan AWS CLI 1160
Bagaimana AWS CloudTrail menggunakan AWS KMS 1164
Riwayat dokumen 1171
Pembaruan lebih awal 1242
..... mcclxi

Apa itu AWS CloudTrail?

> **Tip**
>
> Jika Anda menggunakan peristiwa CloudTrail data, Anda dapat mempelajari teknik pemantauan lanjutan melalui lokakarya dan rangkaian acara Cloud Operations Enablement, serta Menggunakan CloudTrail untuk Keamanan dan Praktik Terbaik AI.

AWS CloudTrail adalah sebuah Layanan AWS yang membantu Anda mengaktifkan audit operasional dan risiko, tata kelola, dan kepatuhan Anda. Akun AWS Tindakan yang diambil oleh pengguna, peran, atau AWS layanan dicatat sebagai peristiwa di CloudTrail. Peristiwa mencakup tindakan yang diambil dalam Konsol Manajemen AWS, AWS Command Line Interface, dan AWS SDK dan API.

CloudTrail menyediakan tiga cara untuk merekam peristiwa:

- Riwayat acara — Riwayat acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir peristiwa manajemen dalam file. Wilayah AWS Anda dapat mencari acara dengan memfilter pada satu atribut. Anda secara otomatis memiliki akses ke riwayat Acara saat membuat akun. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.

  Tidak ada CloudTrail biaya untuk melihat riwayat Acara.
- CloudTrail AWS CloudTrail Danau adalah danau data terkelola untuk menangkap, menyimpan, mengakses, dan menganalisis aktivitas pengguna dan API AWS untuk tujuan audit dan keamanan. CloudTrail Lake mengubah peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Anda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika Anda memilih opsi harga retensi yang One-year dapat diperpanjang, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi. Seven-year Anda dapat membuat penyimpanan data acara untuk satu Akun AWS atau beberapa Akun AWS dengan menggunakan AWS Organizations. Anda dapat mengimpor CloudTrail log yang ada dari bucket S3 Anda ke penyimpanan data peristiwa yang ada atau yang baru. Anda juga dapat memvisualisasikan tren CloudTrail acara teratas dengan dasbor Danau. Untuk informasi selengkapnya, lihat Bekerja dengan AWS CloudTrail Danau.

CloudTrail Penyimpanan data acara danau dan kueri dikenakan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Ketika Anda menjalankan kueri di Lake, Anda membayar berdasarkan jumlah data yang dipindai. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Lake, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

- Trails — Trails menangkap catatan AWS aktivitas, mengirimkan dan menyimpan peristiwa ini dalam bucket Amazon S3, dengan pengiriman opsional ke CloudWatch Log dan Amazon. EventBridge Anda dapat memasukkan peristiwa ini ke dalam solusi pemantauan keamanan Anda. Anda juga dapat menggunakan solusi atau solusi pihak ketiga Anda sendiri seperti Amazon Athena untuk mencari dan menganalisis log Anda CloudTrail . Anda dapat membuat jejak untuk satu Akun AWS atau beberapa Akun AWS dengan menggunakan AWS Organizations. Anda dapat mencatat peristiwa Insights untuk menganalisis peristiwa manajemen Anda untuk perilaku anomali dalam tingkat panggilan API dan tingkat kesalahan. Untuk informasi selengkapnya, lihat Membuat jejak untuk Anda Akun AWS.

  Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

Visibilitas ke dalam aktivitas AWS akun Anda adalah aspek kunci dari praktik terbaik keamanan dan operasional. Anda dapat menggunakan CloudTrail untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi aktivitas akun di seluruh AWS infrastruktur Anda. Anda dapat mengidentifikasi siapa atau apa yang mengambil tindakan apa, sumber daya apa yang ditindaklanjuti, kapan peristiwa itu terjadi, dan detail lainnya untuk membantu Anda menganalisis dan menanggapi aktivitas di AWS akun Anda.

Anda dapat mengintegrasikan CloudTrail ke dalam aplikasi menggunakan API, mengotomatiskan pembuatan penyimpanan data jejak atau peristiwa untuk organisasi Anda, memeriksa status penyimpanan dan jejak data peristiwa yang Anda buat, dan mengontrol cara pengguna melihat CloudTrail peristiwa.

Mengakses CloudTrail

Anda dapat bekerja CloudTrail dengan salah satu cara berikut.

Topik

- CloudTrail konsol
- AWS CLI
- CloudTrail API
- AWS SDK

CloudTrail konsol

Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.

CloudTrail Konsol menyediakan antarmuka pengguna untuk melakukan banyak CloudTrail tugas seperti:

- Melihat peristiwa terbaru dan riwayat acara untuk AWS akun Anda.
- Mengunduh file yang difilter atau lengkap dari 90 hari terakhir acara manajemen dari riwayat Acara.
- Membuat dan mengedit CloudTrail jejak.
- Membuat dan mengedit penyimpanan data acara CloudTrail Lake.
- Menjalankan kueri pada penyimpanan data acara.
- Mengkonfigurasi CloudTrail jalur, termasuk:
  - Memilih bucket Amazon S3 untuk jalur.
  - Mengatur awalan.
  - Mengkonfigurasi pengiriman ke CloudWatch Log.
  - Menggunakan AWS KMS kunci untuk enkripsi data jejak.
  - Mengaktifkan notifikasi Amazon SNS untuk pengiriman file log di jalur.
  - Menambahkan dan mengelola tag untuk jalur Anda.
- Mengkonfigurasi penyimpanan data acara CloudTrail Lake, termasuk:
  - Mengintegrasikan penyimpanan data acara dengan CloudTrail mitra atau dengan aplikasi Anda sendiri, untuk mencatat peristiwa dari sumber di luar. AWS
  - Menyatukan penyimpanan data acara untuk menjalankan kueri dari Amazon Athena.

- Menggunakan AWS KMS kunci untuk enkripsi data penyimpanan data acara.
- Menambahkan dan mengelola tag untuk penyimpanan data acara Anda.

Untuk informasi lebih lanjut tentang Konsol Manajemen AWS, lihat Konsol Manajemen AWS.

AWS CLI

AWS Command Line Interface Ini adalah alat terpadu yang dapat Anda gunakan untuk berinteraksi CloudTrail dari baris perintah. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Command Line Interface. Untuk daftar lengkap perintah CloudTrail CLI, lihat cloudtrail dan cloudtrail-data di Referensi Perintah.AWS CLI

CloudTrail API

Selain konsol dan CLI, Anda juga dapat menggunakan CloudTrail RESTful API untuk memprogram secara langsung. CloudTrail Untuk informasi selengkapnya, lihat Referensi AWS CloudTrail API dan Referensi CloudTrail-Data API.

AWS SDK

Sebagai alternatif untuk menggunakan CloudTrail API, Anda dapat menggunakan salah satu AWS SDK. Setiap SDK terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman. SDK menyediakan cara mudah untuk membuat akses terprogram ke. CloudTrail Misalnya, Anda dapat menggunakan SDK untuk menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba ulang permintaan secara otomatis. Untuk informasi selengkapnya, lihat AWS halaman Tools to Build on.

Bagaimana cara CloudTrail kerja

Anda secara otomatis memiliki akses ke riwayat CloudTrail Acara saat Anda membuat Akun AWS. Riwayat Acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir dari peristiwa manajemen yang direkam dalam file. Wilayah AWS

Untuk catatan acara yang sedang berlangsung dalam 90 hari Akun AWS terakhir Anda, buat jejak atau penyimpanan data acara CloudTrail Danau.

Topik

- CloudTrail Riwayat acara

- CloudTrail Penyimpanan data danau dan acara
- CloudTrail Dasbor danau
- CloudTrail jalan setapak
- CloudTrail Insights acara
- CloudTrail saluran

CloudTrail Riwayat acara

Anda dapat dengan mudah melihat 90 hari terakhir acara manajemen di CloudTrail konsol dengan membuka halaman Riwayat acara. Anda juga dapat melihat riwayat peristiwa dengan menjalankan aws cloudtrail lookup-eventsperintah, atau operasi `LookupEvents`API. Anda dapat mencari peristiwa dalam riwayat Acara dengan memfilter acara pada satu atribut. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.

Riwayat acara tidak terhubung ke jejak atau penyimpanan data peristiwa apa pun yang ada di akun Anda dan tidak terpengaruh oleh perubahan konfigurasi yang Anda buat pada jejak dan penyimpanan data acara Anda.

Tidak ada CloudTrail biaya untuk melihat halaman riwayat acara atau menjalankan `lookup-events` perintah.

CloudTrail Penyimpanan data danau dan acara

Anda dapat membuat penyimpanan data peristiwa untuk mencatat CloudTrail peristiwa (peristiwa manajemen, peristiwa data, peristiwa aktivitas jaringan), peristiwa CloudTrailWawasan, AWS Audit Manager bukti, item AWS Config konfigurasi, atau peristiwa di luar. AWS

Penyimpanan data acara dapat mencatat peristiwa dari saat ini Wilayah AWS, atau dari semua yang Wilayah AWS ada di AWS akun Anda. Penyimpanan data peristiwa yang Anda gunakan untuk mencatat peristiwa Integrasi dari luar AWS harus hanya untuk satu Wilayah saja; mereka tidak dapat berupa penyimpanan data acara Multi-wilayah.

Jika Anda telah membuat organisasi AWS Organizations, Anda dapat membuat penyimpanan data acara organisasi yang mencatat semua peristiwa untuk semua AWS akun di organisasi tersebut. Penyimpanan data acara organisasi dapat berlaku untuk semua AWS Wilayah, atau Wilayah saat ini. Penyimpanan data acara organisasi harus dibuat menggunakan akun manajemen atau akun administrator yang didelegasikan, dan ketika ditentukan sebagai aplikasi ke organisasi,

secara otomatis diterapkan ke semua akun anggota dalam organisasi. Akun anggota tidak dapat melihat penyimpanan data acara organisasi, juga tidak dapat memodifikasi atau menghapusnya. Penyimpanan data acara organisasi tidak dapat digunakan untuk mengumpulkan acara dari luar AWS. Untuk informasi selengkapnya, lihat Memahami penyimpanan data acara organisasi.

Secara default, semua peristiwa di penyimpanan data acara dienkripsi oleh. CloudTrail Ketika Anda mengkonfigurasi penyimpanan data acara, Anda dapat memilih untuk menggunakan milik Anda sendiri AWS KMS key. Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah. Untuk informasi selengkapnya, lihat Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS).

Tabel berikut memberikan informasi tentang tugas yang dapat Anda lakukan pada penyimpanan data acara.

Tugas	Deskripsi
Lihat dan buat dasbor	Anda dapat menggunakan dasbor CloudTrail Danau untuk melihat tren acara untuk penyimpanan data acara di akun Anda. Anda dapat melihat dasbor terkelola, membuat dasbor khusus, dan mengaktifkan dasbor Sorotan untuk melihat sorotan data acara yang dikuratori dan dikelola oleh Lake. CloudTrail
Peristiwa manajemen log	Konfigurasikan penyimpanan data acara Anda untuk mencatat read-only, write-only, atau semua peristiwa manajemen. Secara default, data acara menyimpan peristiwa manajemen log. Anda dapat memfilter peristiwa manajemen pada bidang pemilih acara lanjutan berikut:`eventName` ,,`eventSource` ,`eventType` , `readOnlysessionCredentialFromConsole` , dan`userIdentity.arn` .
Peristiwa data log	Anda dapat menggunakan penyeleksi acara lanjutan untuk membuat penyeleksi berbutir halus untuk mencatat hanya peristiwa data yang menarik. Misalnya, Anda dapat memfilter di `eventName` bidang untuk menyertakan atau mengecualikan pencatatan panggilan API tertentu, yang dapat membantu mengontrol biaya. Untuk informasi selengkapnya, lihat Memfilter

Tugas	Deskripsi
	peristiwa data dengan menggunakan pemilih acara tingkat lanjut.
Log peristiwa aktivitas jaringan	Konfigurasikan penyimpanan data acara Anda untuk mencatat peristiwa aktivitas jaringan. Anda dapat menggunakan pemilih acara lanjutan untuk memfilter pada `eventName` ,`errorCode` , dan `vpcEndpointId` bidang untuk mencatat hanya peristiwa yang menarik.
Peristiwa Log Insights	Konfigurasikan penyimpanan data acara Anda untuk mencatat peristiwa Wawasan untuk membantu Anda mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan panggilan API manajemen. Untuk informasi selengkapnya, lihat Bekerja dengan CloudTrail Wawasan. Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jejak dan acara. Untuk informasi selengkapnya, silakan lihat Harga AWS CloudTrail.
Salin acara jejak	Anda dapat menyalin peristiwa jejak ke penyimpanan data peristiwa baru atau yang sudah ada untuk membuat snapshot point-in-time dari peristiwa yang dicatat ke jejak.
Aktifkan federasi pada penyimpanan data acara	Anda dapat menggabungkan penyimpanan data peristiwa untuk melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL pada data peristiwa menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri.

Tugas	Deskripsi
Menghentikan atau memulai konsumsi acara di penyimpanan data acara	Anda dapat menghentikan dan memulai konsumsi acara pada penyimpanan data acara yang mengumpulkan peristiwa CloudTrail manajemen dan data, atau item AWS Config konfigurasi.
Buat integrasi dengan sumber acara di luar AWS	Anda dapat menggunakan integrasi CloudTrail Lake untuk mencatat dan menyimpan data aktivitas pengguna dari luar AWS; dari sumber apa pun di lingkungan hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau wadah. Untuk informasi tentang mitra integrasi yang tersedia, lihat Integrasi AWS CloudTrail Danau.
Lihat contoh kueri Lake di konsol CloudTrail	CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri.
Membuat atau mengedit kueri	Kueri di CloudTrail ditulis dalam SQL. Anda dapat membuat kueri di tab CloudTrail Lake Editor dengan menulis kueri di SQL dari awal, atau dengan membuka kueri yang disimpan atau sampel dan mengeditnya.
Menyimpan hasil kueri ke bucket S3	Saat menjalankan kueri, Anda dapat menyimpan hasil kueri ke bucket S3.
Unduh hasil kueri yang disimpan	Anda dapat mengunduh file CSV yang berisi hasil kueri CloudTrail Lake yang disimpan.
Validasi hasil kueri yang disimpan	Anda dapat menggunakan validasi integritas hasil CloudTrail kueri untuk menentukan apakah hasil kueri diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan hasil kueri ke bucket S3.

Untuk informasi lebih lanjut tentang CloudTrail Danau, lihatBekerja dengan AWS CloudTrail Danau.

CloudTrail Penyimpanan data acara danau dan kueri dikenakan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa,

dan periode retensi default dan maksimum untuk penyimpanan data acara. Ketika Anda menjalankan kueri di Lake, Anda membayar berdasarkan jumlah data yang dipindai. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

CloudTrail Dasbor danau

Anda dapat menggunakan dasbor CloudTrail Danau untuk melihat tren acara untuk penyimpanan data acara di akun Anda. CloudTrail Lake menawarkan jenis dasbor berikut:

- Dasbor terkelola — Anda dapat melihat dasbor terkelola untuk melihat tren acara untuk penyimpanan data acara yang mengumpulkan peristiwa manajemen, peristiwa data, atau peristiwa Wawasan. Dasbor ini secara otomatis tersedia untuk Anda dan dikelola oleh CloudTrail Lake. CloudTrail menawarkan 14 dasbor terkelola untuk dipilih. Anda dapat menyegarkan dasbor terkelola secara manual. Anda tidak dapat memodifikasi, menambah, atau menghapus widget untuk dasbor ini, namun, Anda dapat menyimpan dasbor terkelola sebagai dasbor khusus jika Anda ingin memodifikasi widget atau mengatur jadwal penyegaran.
- Dasbor khusus - Dasbor khusus memungkinkan Anda untuk menanyakan peristiwa dalam jenis penyimpanan data acara apa pun. Anda dapat menambahkan hingga 10 widget ke dasbor kustom. Anda dapat menyegarkan dasbor kustom secara manual, atau Anda dapat mengatur jadwal penyegaran.
- Dasbor Sorotan — Aktifkan dasbor Sorotan untuk melihat ikhtisar sekilas tentang AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Dasbor Sorotan dikelola oleh CloudTrail dan menyertakan widget yang relevan dengan akun Anda. Widget yang ditampilkan di dasbor Sorotan unik untuk setiap akun. Widget ini dapat muncul aktivitas abnormal atau anomali yang terdeteksi. Misalnya, dasbor Sorotan Anda dapat menyertakan widget akses lintas akun Total, yang menunjukkan jika ada peningkatan aktivitas lintas akun yang tidak normal. CloudTrail memperbarui dasbor Sorotan setiap 6 jam. Dasbor menunjukkan 24 jam terakhir data dari pembaruan terakhir.

Setiap dashboard terdiri dari satu atau lebih widget dan setiap widget mewakili query SQL.

Untuk informasi selengkapnya, lihat CloudTrail Dasbor danau.

CloudTrail jalan setapak

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa ke bucket Amazon S3 yang Anda tentukan. Anda juga dapat mengirimkan dan menganalisis peristiwa dalam jejak dengan Amazon CloudWatch Logs dan Amazon EventBridge.

Trails dapat mencatat peristiwa CloudTrail manajemen, peristiwa data, peristiwa aktivitas jaringan, dan peristiwa Wawasan.

Anda dapat membuat jalur Multi-wilayah dan Single-region untuk Anda. Akun AWS

Multi-Region jalan setapak

Saat Anda membuat jejak Multi-wilayah, CloudTrail merekam peristiwa di semua peristiwa Wilayah AWS yang diaktifkan di Anda Akun AWS dan mengirimkan file log CloudTrail peristiwa ke bucket S3 yang Anda tentukan. Sebagai praktik terbaik, kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Anda dapat mengonversi jejak wilayah Tunggal menjadi jejak Multi-wilayah dengan menggunakan. AWS CLI Lihat informasi selengkapnya di Memahami jalur Multi-wilayah dan Wilayah keikutsertaan, Membuat jejak dengan konsol, dan Mengkonversi jalur satu wilayah ke jalur multi-wilayah.

Single-Region jalan setapak

Saat Anda membuat jejak wilayah Tunggal, hanya CloudTrail mencatat peristiwa di Wilayah tersebut. Kemudian mengirimkan file log CloudTrail peristiwa ke bucket Amazon S3 yang Anda tentukan. Anda hanya dapat membuat jejak wilayah Tunggal dengan menggunakan. AWS CLI Jika Anda membuat jalur tunggal tambahan, Anda dapat meminta jejak tersebut mengirimkan file log CloudTrail peristiwa ke bucket S3 yang sama atau ke bucket terpisah. Ini adalah opsi default saat Anda membuat jejak menggunakan AWS CLI atau CloudTrail API. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola jalur dengan AWS CLI.

> **Note**
>
> Untuk kedua jenis jalur, Anda dapat menentukan bucket Amazon S3 dari Wilayah mana pun.

Jika Anda telah membuat organisasi AWS Organizations, Anda dapat membuat jejak organisasi yang mencatat semua peristiwa untuk semua AWS akun di organisasi tersebut. Jalur organisasi

dapat berlaku untuk semua AWS Wilayah, atau Wilayah saat ini. Jejak organisasi harus dibuat menggunakan akun manajemen atau akun administrator yang didelegasikan, dan ketika ditentukan sebagai berlaku untuk organisasi, secara otomatis diterapkan ke semua akun anggota dalam organisasi. Akun anggota dapat melihat jejak organisasi, tetapi tidak dapat memodifikasi atau menghapusnya. Secara default, akun anggota tidak memiliki akses ke file log untuk jejak organisasi di bucket Amazon S3.

Secara default, saat Anda membuat jejak di CloudTrail konsol, file log peristiwa dan file intisari Anda dienkripsi dengan kunci KMS. Jika Anda memilih untuk tidak mengaktifkan SSE-KMSenkripsi, file log peristiwa dan file intisari Anda dienkripsi menggunakan enkripsi sisi server Amazon S3 (SSE). Anda dapat menyimpan file log Anda di ember Anda selama yang Anda inginkan. Anda juga dapat mendefinisikan aturan siklus hidup Amazon S3 untuk mengarsipkan atau menghapus berkas log secara otomatis. Jika ingin pemberitahuan tentang pengiriman dan validasi file log, Anda dapat mengatur notifikasi Amazon SNS.

CloudTrail menerbitkan file log beberapa kali dalam satu jam, sekitar setiap 5 menit. File log ini berisi panggilan API dari layanan di akun yang mendukung CloudTrail. Untuk informasi selengkapnya, lihat CloudTrail layanan dan integrasi yang didukung.

> **Note**
>
> CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian Tingkat AWS CloudTrail Layanan untuk informasi lebih lanjut.
>
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan peristiwa yang dicoba dikirim ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.
>
> CloudTrail menangkap tindakan yang dilakukan langsung oleh pengguna atau atas nama pengguna oleh suatu AWS layanan. Misalnya, CloudFormation `CreateStack` panggilan dapat menghasilkan panggilan API tambahan ke Amazon EC2, Amazon RDS, Amazon EBS, atau layanan lain seperti yang dipersyaratkan oleh template. CloudFormation Perilaku ini normal dan diharapkan. Anda dapat mengidentifikasi apakah tindakan itu diambil oleh AWS layanan dengan `invokedby` bidang dalam CloudTrail acara tersebut.

Tabel berikut memberikan informasi tentang tugas yang dapat Anda lakukan di jalur.

Tugas	Deskripsi
Mencatat log peristiwa manajemen	Konfigurasikan jejak Anda untuk mencatat read-only, write-only, atau semua peristiwa manajemen.
Peristiwa data log	Anda dapat menggunakan penyeleksi acara lanjutan untuk membuat penyeleksi berbutir halus untuk mencatat hanya peristiwa data yang menarik. Misalnya, Anda dapat memfilter di `eventName` bidang untuk menyertakan atau mengecualikan pencatatan panggilan API tertentu, yang dapat membantu mengontro l biaya. Untuk informasi selengkapnya, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut.
Log peristiwa aktivitas jaringan	Konfigurasikan jejak Anda untuk mencatat peristiwa aktivitas jaringan. Anda dapat mengonfigurasi penyeleksi acara lanjutan untuk memfilter pada`eventName` ,`errorCode` ,`vpcEndpointId` , dan `userIdent ity.arn` bidang untuk mencatat hanya peristiwa yang menarik.
Peristiwa Log Insights	Konfigurasikan jejak Anda untuk mencatat peristiwa Wawasan untuk membantu Anda mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan panggilan API manajemen. Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpan an data jejak dan acara. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Tugas	Deskripsi
Lihat acara Wawasan	Setelah mengaktifkan CloudTrail Insights on a trail, Anda dapat melihat hingga 90 hari peristiwa Insights menggunakan CloudTrail konsol atau. AWS CLI
Unduh acara Insights	Setelah mengaktifkan CloudTrail Insights on a trail, Anda dapat mengunduh file CSV atau JSON yang berisi acara Insights hingga 90 hari terakhir untuk jejak Anda.
Salin acara jejak ke CloudTrail Danau	Anda dapat menyalin peristiwa jejak yang ada ke penyimpanan data acara CloudTrail Lake untuk membuat snapshot point-in-time dari peristiwa yang dicatat ke jejak.
Buat dan berlangganan topik Amazon SNS	Berlangganan topik untuk menerima pemberitahuan tentang pengiriman file log ke bucket Anda. Amazon SNS dapat memberi tahu Anda dengan berbagai cara, termasuk secara terprogram dengan Amazon Simple Queue Service. **Note** Jika Anda ingin menerima pemberitahuan SNS tentang pengiriman file log dari semua Wilayah, tentukan hanya satu topik SNS untuk jejak Anda. Jika Anda ingin memproses semua acara secara terprogram, lihat. Menggunakan Pustaka CloudTrail Pemrosesan
Lihat file log Anda	Temukan dan unduh file log Anda dari bucket S3.

Tugas	Deskripsi
Memantau peristiwa dengan CloudWatch Log	Anda dapat mengonfigurasi jejak Anda untuk mengirim acara ke CloudWatch Log. Anda kemudian dapat menggunakan CloudWatch Log untuk memantau akun Anda untuk panggilan dan peristiwa API tertentu. **Note** Jika Anda mengonfigurasi jejak Multi-wilayah untuk mengirim peristiwa ke grup CloudWatch log Log, CloudTrail mengirimkan peristiwa dari semua Wilayah ke grup log tunggal.
Aktifkan SSE-KMS enkripsi	Mengenkripsi file log Anda dan mencerna file dengan kunci KMS memberikan lapisan keamanan ekstra untuk data Anda. CloudTrail
Aktifkan integritas file log	Validasi integritas file log membantu Anda memverifikasi bahwa file log tetap tidak berubah sejak CloudTrail dikirimkan.
Bagikan file log dengan yang lain Akun AWS	Anda dapat berbagi file log antar akun.
Log agregat dari beberapa akun	Anda dapat menggabungkan file log dari beberapa akun ke satu bucket.
Bekerja dengan solusi mitra	Analisis CloudTrail output Anda dengan solusi mitra yang terintegrasi dengan CloudTrail. Solusi mitra menawarkan serangkaian kemampuan yang luas, seperti pelacakan perubahan, pemecahan masalah, dan analisis keamanan.

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

CloudTrail Insights acara

AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan tingkat panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen. CloudTrail Insights menganalisis pola normal volume panggilan API dan tingkat kesalahan API, juga disebut baseline, dan menghasilkan peristiwa Insights saat volume panggilan atau tingkat kesalahan berada di luar pola normal. Peristiwa wawasan tentang rasio panggilan API dibuat untuk API `write` manajemen, dan peristiwa Insights tentang tingkat kesalahan API dibuat untuk keduanya `read` dan API `write` manajemen.

Secara default, CloudTrail jejak dan penyimpanan data acara tidak mencatat peristiwa Wawasan. Anda harus mengonfigurasi penyimpanan data jejak atau peristiwa untuk mencatat peristiwa Wawasan. Untuk informasi selengkapnya, lihat Pencatatan peristiwa Wawasan dengan CloudTrail konsol dan Pencatatan peristiwa Wawasan dengan AWS CLI.

Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jejak dan acara. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Melihat peristiwa Wawasan untuk jejak dan penyimpanan data acara

CloudTrail mendukung peristiwa Wawasan untuk penyimpanan data jejak dan peristiwa, namun, ada beberapa perbedaan dalam cara Anda melihat dan mengakses peristiwa Wawasan.

Melihat acara Wawasan untuk jalur

Jika peristiwa Insights diaktifkan di jejak, dan CloudTrail mendeteksi aktivitas yang tidak biasa, peristiwa Insights dicatat ke folder atau awalan lain di bucket S3 tujuan untuk jejak Anda. Anda juga dapat melihat jenis wawasan dan periode waktu kejadian saat melihat peristiwa Wawasan di CloudTrail konsol. Untuk informasi selengkapnya, lihat Melihat peristiwa Wawasan untuk jalur dengan konsol.

Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di jalur, CloudTrail mungkin perlu waktu hingga 36 jam untuk mulai menyampaikan acara Insights setelah Anda mengaktifkan peristiwa Insights di jalur, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Melihat peristiwa Wawasan untuk penyimpanan data acara

Untuk mencatat peristiwa Insights di CloudTrail Lake, Anda memerlukan penyimpanan data acara tujuan yang mencatat peristiwa Insights dan penyimpanan data peristiwa sumber yang memungkinkan Insights dan peristiwa manajemen log. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk acara Insights dengan konsol.

Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data peristiwa sumber, CloudTrail mungkin memerlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Insights, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Jika Anda mengaktifkan CloudTrail Insights di penyimpanan data peristiwa sumber dan CloudTrail mendeteksi aktivitas yang tidak biasa, kirimkan peristiwa CloudTrail Insights ke penyimpanan data acara tujuan Anda. Anda kemudian dapat menanyakan penyimpanan data acara tujuan untuk mendapatkan informasi tentang peristiwa Insights dan secara opsional dapat menyimpan hasil kueri ke bucket S3. Untuk informasi selengkapnya, lihat Membuat atau mengedit kueri dengan CloudTrail konsol dan Lihat contoh kueri dengan konsol CloudTrail.

Anda dapat melihat dasbor acara Insights untuk memvisualisasikan peristiwa Wawasan di penyimpanan data acara tujuan Anda. Untuk informasi lebih lanjut tentang dasbor Danau, lihatCloudTrail Dasbor danau.

CloudTrail saluran

CloudTrail mendukung dua jenis saluran:

Saluran untuk integrasi CloudTrail Danau dengan sumber acara di luar AWS

> CloudTrail Lake menggunakan saluran untuk membawa acara dari luar AWS ke CloudTrail Danau dari mitra eksternal yang bekerja dengan CloudTrail, atau dari sumber Anda sendiri. Saat membuat saluran, Anda memilih satu atau beberapa penyimpanan data acara untuk menyimpan peristiwa yang datang dari sumber saluran. Anda dapat mengubah penyimpanan data peristiwa tujuan untuk saluran sesuai kebutuhan, selama penyimpanan data peristiwa tujuan disetel ke peristiwa aktivitas log. Saat Anda membuat saluran untuk acara dari mitra eksternal, Anda menyediakan saluran ARN ke mitra atau aplikasi sumber. Kebijakan sumber daya yang dilampirkan ke saluran memungkinkan sumber untuk mengirimkan peristiwa melalui saluran. Untuk informasi selengkapnya, lihat Buat integrasi dengan sumber acara di luar AWS dan `CreateChannel`di Referensi AWS CloudTrail API.

Service-linked saluran

AWS layanan dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWS Layanan yang membuat saluran terkait layanan mengonfigurasi pemilih peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semua Wilayah, atau Wilayah saat ini.

Anda dapat menggunakan CloudTrail konsol atau AWS CLIuntuk melihat informasi tentang saluran CloudTrail terkait layanan apa pun yang dibuat oleh. Layanan AWS

CloudTrail konsep

Bagian ini merangkum konsep-konsep dasar yang terkait CloudTrail dengan.

Konsep:

- CloudTrail acara
- Riwayat acara
- Jalan setapak
- Jejak organisasi
- CloudTrail Penyimpanan data danau dan acara
- CloudTrail Wawasan
- Tanda
- AWS Security Token Service dan CloudTrail
- Acara layanan global

CloudTrail acara

Peristiwa di CloudTrail adalah catatan aktivitas dalam AWS akun. Kegiatan ini dapat berupa tindakan yang diambil oleh identitas IAM, atau layanan yang dapat dipantau oleh. CloudTrail CloudTrailevent menyediakan riwayat aktivitas akun API dan non-API yang dibuat melalui Konsol Manajemen AWS, AWS SDK, alat baris perintah, dan layanan lainnya AWS .

CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

CloudTrail mencatat empat jenis acara:

- Acara manajemen
- Peristiwa data
- Acara aktivitas jaringan
- Insights acara

Semua jenis acara menggunakan format log CloudTrail JSON.

Secara default, jejak dan data peristiwa menyimpan peristiwa manajemen log, tetapi bukan data atau peristiwa Wawasan.

Untuk informasi tentang cara Layanan AWS mengintegrasikan dengan CloudTrail, lihatAWS topik layanan untuk CloudTrail.

Peristiwa manajemen

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi pesawat kontrol.

Contoh acara manajemen meliputi:

- Mengkonfigurasi keamanan (misalnya, operasi AWS Identity and Access Management `AttachRolePolicy` API).
- Mendaftarkan perangkat (misalnya, operasi `CreateDefaultVpc` API Amazon EC2).
- Mengkonfigurasi aturan untuk merutekan data (misalnya, operasi Amazon `CreateSubnet` EC2 API).
- Menyiapkan logging (misalnya, operasi AWS CloudTrail `CreateTrail` API).

Peristiwa manajemen juga dapat mencakup peristiwa non-API yang terjadi di akun Anda. Misalnya, saat pengguna masuk ke akun Anda, CloudTrail mencatat `ConsoleLogin` peristiwa tersebut. Untuk informasi selengkapnya, lihat Peristiwa non-API yang ditangkap oleh CloudTrail.

Secara default, CloudTrail jejak dan data acara CloudTrail Lake menyimpan peristiwa manajemen log. Untuk informasi selengkapnya tentang peristiwa manajemen logging, lihatMencatat log peristiwa manajemen.

Peristiwa data

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya. Ini juga dikenal sebagai operasi pesawat data. Peristiwa data sering kali merupakan aktivitas bervolume tinggi.

Contoh peristiwa data meliputi:

- Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject`, `DeleteObject`, dan operasi `PutObject` API) pada objek di bucket S3.
- AWS Lambda aktivitas eksekusi fungsi (`Invoke`API).
- CloudTrail `PutAuditEvents`aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS.
- Operasi Amazon SNS `Publish`dan `PublishBatch`API pada topik.

Tabel berikut menunjukkan jenis sumber daya yang tersedia untuk jejak dan penyimpanan data peristiwa. Kolom tipe sumber daya (konsol) menunjukkan pilihan yang sesuai di konsol. Kolom nilai resources.type menunjukkan `resources.type` nilai yang akan Anda tentukan untuk menyertakan peristiwa data dari jenis tersebut di penyimpanan data jejak atau peristiwa Anda menggunakan API atau. AWS CLI CloudTrail

Untuk jejak, Anda dapat menggunakan pemilih peristiwa dasar atau lanjutan untuk mencatat peristiwa data untuk objek Amazon S3 di bucket tujuan umum, fungsi Lambda, dan tabel DynamoDB (ditampilkan dalam tiga baris pertama tabel). Anda hanya dapat menggunakan pemilih acara lanjutan untuk mencatat jenis sumber daya yang ditampilkan di baris yang tersisa.

Untuk penyimpanan data acara, Anda hanya dapat menggunakan pemilih acara lanjutan untuk menyertakan peristiwa data.

Peristiwa data yang didukung oleh AWS CloudTrail

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
OMWDevice CommunicationService	Aktivitas API pada `AWS::Account::Cont`	AWS: :Akun:: ControlledDomain	`AWS::Account::ControlledDomain`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
	`rolledDomain` sumber daya.		
WorkSpaces Aplikasi Amazon	Agen mengakses acara alat MCP WorkSpaces Aplikasi	Alat MCP Akses Agen	`AWS::AgentAccessMCP::Tools`
AWS Registri Agen	Aktivitas API pada `AWS::AgentRegistry::Registry` sumber daya.	AWS Registri Agen	`AWS::AgentRegistry::Registry`
Amazon AIDevOps	AIDevOps Aktivitas API pada ruang agen.	Agen Ruang	`AWS::AIDevOps::AgentSpace`
Amazon AIDevOps	AIDevOps Aktivitas API pada asosiasi.	AIDevOps asosiasi	`AWS::AIDevOps::Association`
Amazon AIDevOps	AIDevOps Aktivitas API di tim aplikasi operator.	AIDevOps tim aplikasi operator	`AWS::AIDevOps::OperatorAppTeam`
Amazon AIDevOps	AIDevOps Aktivitas API pada metadata pipeline.	AIDevOps Metadata Pipa	`AWS::AIDevOps::PipelineMetadata`
Amazon AIDevOps	AIDevOps Aktivitas API pada layanan.	AIDevOps layanan	`AWS::AIDevOps::Service`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada investigasi operasional. Untuk informasi selengkapnya, lihat Pengembang Amazon Q.	Grup Investigasi AIOps	`AWS::AIOps::InvestigationGroup`
Amazon Tanpa OpenSearch Server	Aktivitas API pada `AWS::AOSS::Collection` sumber daya.	AWS: :AOSS: :I	`AWS::AOSS::Collection`
AWS AppConfig	AWS AppConfig Aktivitas API untuk operasi konfigurasi seperti panggilan ke StartConfigurationSession dan GetLatestConfiguration. Untuk informasi selengkapnya, lihat AWS AppConfig.	AWS AppConfig	`AWS::AppConfig::Configuration`
CloudWatch Sinyal Aplikasi	Aktivitas API pada `AWS::ApplicationSignals::InstrumentationConfig` sumber daya.	AWS::ApplicationSignals::InstrumentationConfig	`AWS::ApplicationSignals::InstrumentationConfig`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS AppSync	AWS AppSync Aktivitas API pada AppSync GraphQL API. Untuk informasi selengkapnya, lihat AWS AppSync.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`
Ruang kerja antropik eksternal	Aktivitas API pada `AWS::AWSExternalAnthropic::Workspace` sumber daya.	Ruang kerja antropik eksternal	`AWS::AWSExternalAnthropic::Workspace`
AWS Pertukaran Data B2B	Aktivitas API Pertukaran Data B2B untuk operasi Transformer seperti panggilan ke dan. GetTransformerJob StartTransformerJob	Pertukaran Data B2B	`AWS::B2BI::Transformer`
AWS Titik akses Backup	Aktivitas API pada `AWS::Backup::BackupAccessPoint` sumber daya.	AWS Titik akses Backup	`AWS::Backup::BackupAccessPoint`
AWS Backup	AWS Aktivitas Backup Search Data API pada pekerjaan pencarian.	AWS API Data Pencarian Cadangan	`AWS::Backup::SearchJob`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API dasar pada pekerjaan prompt optimasi lanjutan.	AdvancedOptimizePromptJob	`AWS::Bedrock::AdvancedOptimizePromptJob`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias agen. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Alias agen batuan dasar	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada pemanggilan asinkron.	Panggilan asinkron batuan dasar	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada kebijakan penalaran otomatis.	Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada versi kebijakan penalaran otomatis.	Versi Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicyVersion`
Amazon Bedrock	Aktivitas API cetak biru Amazon Bedrock.	Cetak biru batuan dasar	`AWS::Bedrock::Blueprint`
Amazon Bedrock	Aktivitas API pemanggilan otomatisasi data batuan dasar.	Pemanggilan Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationInvocation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API profil otomatisasi data Amazon Bedrock.	Profil Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProfile`
Amazon Bedrock	Aktivitas API proyek otomatisasi data Amazon Bedrock.	Proyek Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProject`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias flow.	Alias aliran batuan dasar	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada eksekusi aliran.	Eksekusi Aliran	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	Aktivitas Amazon Bedrock API di pagar pembatas.	Pagar pembatas batuan dasar	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada agen inline.	Memohon Batuan Dasar Inline-Agent	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada basis pengetahuan. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Basis pengetahuan batuan dasar	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada model.	Model batuan dasar	`AWS::Bedrock::Model`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock API pada prompt.	Permintaan batuan dasar	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada sesi.	Sesi batuan dasar	`AWS::Bedrock::Session`
Amazon Bedrock	Aktivitas API Amazon Bedrock Tool.	Alat Batuan Dasar	`AWS::Bedrock::Tool`
Bedrock-AgentCore ABTest	Aktivitas API pada `AWS::BedrockAgentCore::ABTest` sumber daya.	Bedrock-AgentCore ABTest	`AWS::BedrockAgentCore::ABTest`
Amazon Bedrock	Aktivitas API Amazon Bedrock ApiKey CredentialProvider .	Bedrock-AgentCore apiKey CredentialProvider	`AWS::BedrockAgentCore::APIKeyCredentialProvider`
BedrockAgentCore evaluasi batch	Aktivitas API pada `AWS::BedrockAgentCore::BatchEvaluate` sumber daya.	BedrockAgentCore evaluasi batch	`AWS::BedrockAgentCore::BatchEvaluate`
Amazon Bedrock	Aktivitas API Browser Amazon Bedrock.	Bedrock-AgentCore Browser	`AWS::BedrockAgentCore::Browser`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock Browser-Custom API.	Bedrock-AgentCore Browser-Custom	`AWS::BedrockAgentCore::BrowserCustom`
Bedrock-AgentCore Profil Browser	Aktivitas API pada `AWS::BedrockAgentCore::BrowserProfile` sumber daya.	Bedrock-AgentCore Profil Browser	`AWS::BedrockAgentCore::BrowserProfile`
BedrockAgentCore CapacityProvider	Aktivitas API pada `AWS::BedrockAgentCore::CapacityProvider` sumber daya.	BedrockAgentCore CapacityProvider	`AWS::BedrockAgentCore::CapacityProvider`
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter API.	Bedrock-AgentCore Code-Interpreter	`AWS::BedrockAgentCore::CodeInterpreter`
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter-Custom API.	Bedrock-AgentCore Code-Interpreter-Custom	`AWS::BedrockAgentCore::CodeInterpreterCustom`
Batuan Dasar Amazon AgentCore	Aktivitas AgentCore API batuan dasar pada evaluator.	Bedrock-AgentCore Penilai	`AWS::BedrockAgentCore::Evaluator`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Amazon Bedrock Gateway.	Bedrock-AgentCore Gerbang	`AWS::BedrockAgentCore::Gateway`
Amazon Bedrock	Aktivitas API Memori Amazon Bedrock.	Bedrock-AgentCore Memori	`AWS::BedrockAgentCore::Memory`
Amazon Bedrock	Aktivitas API Amazon Bedrock Oauth2 CredentialProvider .	Bedrock-AgentCore Oauth2 CredentialProvider	`AWS::BedrockAgentCore::OAuth2CredentialProvider`
Bedrock-AgentCore pembayaran	Aktivitas API pada `AWS::BedrockAgentCore::Payments` sumber daya.	Bedrock-AgentCore pembayaran	`AWS::BedrockAgentCore::Payments`
Bedrock-AgentCore kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::Policy` sumber daya.	Bedrock-AgentCore kebijakan	`AWS::BedrockAgentCore::Policy`
Bedrock-AgentCore mesin kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::PolicyEngine` sumber daya.	Bedrock-AgentCore mesin kebijakan	`AWS::BedrockAgentCore::PolicyEngine`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Bedrock-AgentCore Rekomendasi	Aktivitas API pada `AWS::BedrockAgentCore::Recommendation` sumber daya.	Bedrock-AgentCore Rekomendasi	`AWS::BedrockAgentCore::Recommendation`
Bedrock-AgentCore Registri	Aktivitas API pada `AWS::BedrockAgentCore::Registry` sumber daya.	Bedrock-AgentCore Registri	`AWS::BedrockAgentCore::Registry`
Amazon Bedrock	Aktivitas API Amazon Bedrock Runtime.	Bedrock-AgentCore Runtime	`AWS::BedrockAgentCore::Runtime`
Amazon Bedrock	Aktivitas Amazon Bedrock Runtime-Endpoint API.	Bedrock-AgentCore Runtime-Endpoint	`AWS::BedrockAgentCore::RuntimeEndpoint`
Amazon Bedrock	Aktivitas API Amazon Bedrock Token Vault.	Bedrock-AgentCore Brankas Token	`AWS::BedrockAgentCore::TokenVault`
Amazon Bedrock	Aktivitas API Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentity`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Direktori Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Direktori Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentityDirectory`
Proyek Mantel Batuan Dasar	Aktivitas API pada `AWS::BedrockMantle::Project` sumber daya.	Proyek Mantel Batuan Dasar	`AWS::BedrockMantle::Project`
Alat Pencarian Web Bedrock	Aktivitas API pada `AWS::BedrockWebSearch::Tool` sumber daya.	Alat Pencarian Web Bedrock	`AWS::BedrockWebSearch::Tool`
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces (untuk Apache Cassandra) di aliran Cassandra CDC.	Aliran CDC Cassandra	`AWS::Cassandra::Stream`
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces di atas meja. Untuk informasi selengkapnya, lihat Amazon Keyspaces (untuk Apache Cassandra).	Meja Cassandra	`AWS::Cassandra::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Certificate Manager	Aktivitas API pada `AWS::CertificateManager::AcmeEndpoint` sumber daya.	AWS::CertificateManager::AcmeEndpoint	`AWS::CertificateManager::AcmeEndpoint`
Uji Klinis Daftar kode teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Codelist` sumber daya.	Uji Klinis Daftar kode teknologi	`AWS::ClinicalTrialsTech::Codelist`
Dataset Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Dataset` sumber daya.	Dataset Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Dataset`
Uji Klinis Eksekusi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Execution` sumber daya.	Uji Klinis Eksekusi teknologi	`AWS::ClinicalTrialsTech::Execution`
Contoh Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Instance` sumber daya.	Contoh Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Instance`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Uji Klinis Pemetaan teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Mapping` sumber daya.	Uji Klinis Pemetaan teknologi	`AWS::ClinicalTrialsTech::Mapping`
Jadwal Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Schedule` sumber daya.	Jadwal Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Schedule`
Uji Klinis Studi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Study` sumber daya.	Uji Klinis Studi teknologi	`AWS::ClinicalTrialsTech::Study`
Amazon CloudFront	CloudFront Aktivitas API pada a KeyValueStore. Untuk informasi selengkapnya, lihat Amazon CloudFront.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API pada profil.	AWS::CloudOptimization: :Profil	`AWS::CloudOptimization::Profile`
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API berdasarkan rekomendasi.	AWS::CloudOptimization: :Rekomendasi	`AWS::CloudOptimization::Recommendation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS CloudTrail	CloudTrail PutAuditEvents aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS. Untuk informasi selengkapnya, lihat AWS CloudTrail.	CloudTrail saluran	`AWS::CloudTrail::Channel`
CloudWatch dataset	Aktivitas API pada `AWS::CloudWatch::Dataset` sumber daya.	CloudWatch dataset	`AWS::CloudWatch::Dataset`
Titik akhir konsumsi observabilitas	Aktivitas API pada `AWS::CloudWatch::IngestionEndpoint` sumber daya.	Titik akhir konsumsi observabilitas	`AWS::CloudWatch::IngestionEndpoint`
Amazon CloudWatch	Aktivitas Amazon CloudWatch API pada metrik. Untuk informasi selengkapnya, lihat Amazon CloudWatch.	CloudWatch metrik	`AWS::CloudWatch::Metric`
Amazon CodeGuru Profiler	CodeGuru Aktivitas API profiler pada grup profil.	CodeGuru Grup profil profiler	`AWS::CodeGuruProfiler::ProfilingGroup`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API pada kustomisasi.	CodeWhisperer kustomisasi	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API di profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Aktivitas API Amazon Cognito di kumpulan identitas Amazon Cognito. Untuk informasi lebih lanjut, lihat Amazon Cognito.	Kolam Identitas Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Aktivitas API Data Exchange pada aset.	Aset Data Exchange	`AWS::DataExchange::Asset`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada armada. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Armada Cloud	`AWS::Deadline::Fleet`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerjaan. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Lowongan kerja Deadline Cloud	`AWS::Deadline::Job`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada antrian. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu antrian Cloud	`AWS::Deadline::Queue`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerja. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Pekerja Cloud	`AWS::Deadline::Worker`
Peringatan Diode Alerting terkait	Aktivitas API pada `AWS::DiodeAlerting::LinkedAlert` sumber daya.	Peringatan Diode Alerting terkait	`AWS::DiodeAlerting::LinkedAlert`
Amazon Aurora DSQL	Aktivitas Amazon Aurora DSQL API pada sumber daya cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
Amazon DynamoDB	Aktivitas Amazon DynamoDB API di stream. Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB Streams	`AWS::DynamoDB::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon DynamoDB	Aktivitas API tingkat item Amazon DynamoDB pada tabel (misalnya, PutItem,, DeleteItem dan operasi API). UpdateItem Untuk tabel dengan aliran diaktifkan, bidang sumber daya dalam peristiwa data berisi: :DynamoDB : :Stream dan AWS AWS: :DynamoDB : :Table. Jika Anda menentukan AWS: :DynamoDB : :Table untuk resources.type, itu akan mencatat tabel DynamoDB dan peristiwa aliran DynamoDB secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter pada bidang EventName . Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB	`AWS::DynamoDB::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Elastic Compute Cloud	Instans Amazon EC2 menghubungkan aktivitas API titik akhir.	Instans EC2 menghubungkan titik akhir	`AWS::EC2::InstanceConnectEndpoint`
Amazon Elastic Block Store	API langsung Amazon Elastic Block Store (EBS), seperti, PutSnapshotBlock, GetSnapshotBlock dan pada snapshot ListChangedBlocks Amazon EBS. Untuk informasi selengkapnya, lihat Amazon Elastic Block Store.	API langsung EBS	`AWS::EC2::Snapshot`
Amazon Elastic Container Service	Aktivitas API Amazon Elastic Container Service pada instance container.	Contoh kontainer ECS	`AWS::ECS::ContainerInstance`
LAYANAN AMAZON ELASTIC KUBERNETES	Aktivitas API Amazon Elastic Kubernetes Service di dasbor.	Dasbor EKS	`AWS::EKS::Dashboard`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon EMR	Aktivitas Amazon EMR API di ruang kerja log tulis di depan. Untuk informasi selengkapnya, lihat Amazon EMR.	Ruang kerja log tulis ke depan EMR	`AWS::EMRWAL::Workspace`
pesan pengguna akhir	Aktivitas API pada `AWS::EndUserMessaging::NotifyCodeVerification` sumber daya.	AWS::EndUserMessaging::NotifyCodeVerification	`AWS::EndUserMessaging::NotifyCodeVerification`
EventBridge titik akhir	Aktivitas API pada `AWS::Events::Endpoint` sumber daya.	EventBridge titik akhir	`AWS::Events::Endpoint`
EventBridge Bus acara khusus - klasik	Aktivitas API pada `AWS::Events::EventBus` sumber daya.	EventBridge Bus acara khusus - klasik	`AWS::Events::EventBus`
EventBridge sumber acara mitra	Aktivitas API pada `AWS::Events::EventSource` sumber daya.	EventBridge sumber acara mitra	`AWS::Events::EventSource`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
EventBridge aturan	Aktivitas API pada `AWS::Events::Rule` sumber daya.	EventBridge aturan	`AWS::Events::Rule`
EventBridge Bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventBus` sumber daya.	EventBridge Bus peristiwa kustom	`AWS::EventsV2::EventBus`
EventBridge Sumber acara bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventSource` sumber daya.	EventBridge Sumber acara bus acara khusus	`AWS::EventsV2::EventSource`
Amazon FinSpace	Aktivitas Amazon FinSpace API di lingkungan. Untuk informasi selengkapnya, lihat Amazon FinSpace.	FinSpace	`AWS::FinSpace::Environment`
Amazon FSx	Aktivitas Amazon FSx API pada volume.	Volume FSx	`AWS::FSx::Volume`
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada aplikasi. Untuk informasi selengkapnya, lihat Amazon GameLift Streams.	GameLift Aplikasi Streams	`AWS::GameLiftStreams::Application`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada grup streaming. Untuk informasi selengkap nya, lihat Amazon GameLift Streams.	GameLift Streaming grup aliran	`AWS::GameLiftStreams::StreamGroup`
Peta Lokasi Amazon	Aktivitas API Peta Lokasi Amazon.	Peta Geo	`AWS::GeoMaps::Provider`
Tempat Lokasi Amazon	Aktivitas API Tempat Lokasi Amazon.	Tempat Geo	`AWS::GeoPlaces::Provider`
Rute Lokasi Amazon	Aktivitas API Rute Lokasi Amazon.	Rute Geo	`AWS::GeoRoutes::Provider`
AWS Glue	AWS Aktivitas Glue API pada tabel yang dibuat oleh Lake Formation.	Formasi Danau	`AWS::Glue::Table`
AWS IoT Greengrass Versi 2	Aktivitas API Greengrass dari perangkat inti Greengrass pada versi komponen. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Versi komponen Greengrass IoT	`AWS::GreengrassV2::ComponentVersion`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT Greengrass Versi 2	Greengrass aktivitas API dari perangkat inti Greengrass pada penerapan. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Penyebaran Greengrass IoT	`AWS::GreengrassV2::Deployment`
Amazon GuardDuty	Aktivitas Amazon GuardDuty API untuk detektor. Untuk informasi selengkapnya, lihat Amazon GuardDuty.	GuardDuty detektor	`AWS::GuardDuty::Detector`
Amazon GuardDuty	GuardDuty Aktivitas API pada pemindaian malware.	GuardDuty pemindaian malware	`AWS::GuardDuty::MalwareScan`
Domain agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Domain` sumber daya.	Domain agen kesehatan	`AWS::HealthAgent::Domain`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Integration` sumber daya.	AWS::HealthAgent: :Integri	`AWS::HealthAgent::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::PatientInsightsJob` sumber daya.	health-agent.amazonaws.com	`AWS::HealthAgent::PatientInsightsJob`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Session` sumber daya.	AWS::HealthAgent: :Sesi	`AWS::HealthAgent::Session`
Berlangganan agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Subscription` sumber daya.	Berlangganan agen kesehatan	`AWS::HealthAgent::Subscription`
Profil transformasi data Health Lake	Aktivitas API pada `AWS::HealthLake::DataTransformationProfile` sumber daya.	Profil transformasi data Health Lake	`AWS::HealthLake::DataTransformationProfile`
AWS IoT	AWS Aktivitas API IoT pada sertifikat. Untuk informasi selengkapnya, lihat AWS IoT.	Sertifikat IoT	`AWS::IoT::Certificate`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT	AWS Aktivitas API IoT pada berbagai hal. Untuk informasi selengkapnya, lihat AWS IoT.	Hal IoT	`AWS::IoT::Thing`
AWS Terowongan IoT	Aktivitas API pada `AWS::IoT::Tunnel` sumber daya.	AWS Terowongan IoT	`AWS::IoT::Tunnel`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada aset. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Aset IoT SiteWise	`AWS::IoTSiteWise::Asset`
Dataset IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Dataset` sumber daya.	Dataset IoT SiteWise	`AWS::IoTSiteWise::Dataset`
Pipa IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Pipeline` sumber daya.	Pipa IoT SiteWise	`AWS::IoTSiteWise::Pipeline`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada deret waktu. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Deret waktu IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Ruang kerja IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Workspace` sumber daya.	Ruang kerja IoT SiteWise	`AWS::IoTSiteWise::Workspace`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT pada entitas. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Entitas IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT di ruang kerja. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Ruang kerja IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Peringkat Cerdas Amazon Kendra	Aktivitas API Peringkat Cerdas Amazon Kendra pada rencana eksekusi skor ulang. Untuk informasi selengkapnya, lihat Peringkat Cerdas Amazon Kendra.	Peringkat Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Kinesis Data Streams	Aktivitas API Kinesis Data Streams pada stream. Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Aliran kinesis	`AWS::Kinesis::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Kinesis Data Streams	Kinesis Data Streams aktivitas API pada konsumen streaming . Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Konsumen aliran kinesis	`AWS::Kinesis::StreamConsumer`
Amazon Data Firehose	Aktivitas API aliran pengiriman Amazon Data Firehose.	Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`
Amazon Kinesis Video Streams	Kinesis Video Streams aktivitas API saluran pensinyalan video.	Saluran pensinyalan video Kinesis	`AWS::KinesisVideo::SignalingChannel`
Amazon Kinesis Video Streams	Aktivitas API Kinesis Video Streams pada aliran video, seperti panggilan ke dan. GetMedia PutMedia	Aliran video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Aktivitas eksekusi fungsi Lambda (API Invoke).	Lambda	`AWS::Lambda::Function`
Gambar microvm Lambda	Aktivitas API pada `AWS::Lambda::MicrovmImage` sumber daya.	Gambar microvm Lambda	`AWS::Lambda::MicrovmImage`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Fungsi Web Lambda	Aktivitas API pada `AWS::Lambda::WebFunction` sumber daya.	Lambda WebFunction	`AWS::Lambda::WebFunction`
Lex Bot	Aktivitas API pada `AWS::Lex::Bot` sumber daya.	Lex Bot	`AWS::Lex::Bot`
AWS Lex Bot Alias	Aktivitas API pada `AWS::Lex::BotAlias` sumber daya.	AWS Lex Bot Alias	`AWS::Lex::BotAlias`
CloudWatch Otorisasi grup log log	Aktivitas API pada `AWS::Logs::LogGroupAuthorization` sumber daya.	CloudWatch Otorisasi grup log log	`AWS::Logs::LogGroupAuthorization`
Log Scheduled Query	Aktivitas API pada `AWS::Logs::ScheduledQuery` sumber daya.	Log Scheduled Query	`AWS::Logs::ScheduledQuery`
Amazon Machine Learning	Aktivitas Machine Learning API pada model ML.	Machine Learning MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	Aktivitas API Amazon Managed Blockchain di jaringan.	Jaringan Blockchain yang dikelola	`AWS::ManagedBlockchain::Network`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Managed Blockchain	Amazon Managed Blockchain JSON-RPC memanggil node Ethereum, seperti ETH_getBalance atau eth_get. BlockByNumber Untuk informasi selengkapnya, lihat Amazon Managed Blockchain.	Blockchain yang Dikelola	`AWS::ManagedBlockchain::Node`
Kueri Blockchain yang Dikelola Amazon	Aktivitas API Kueri Blockchain Terkelola Amazon.	Kueri Blockchain Terkelola	`AWS::ManagedBlockchainQuery::QueryAPI`
AWS HealthImaging	AWS HealthImaging Aktivitas API pada penyimpanan data.	MedicalImaging penyimpanan data	`AWS::MedicalImaging::Datastore`
AWS HealthImaging	AWS HealthImaging image set aktivitas API.	MedicalImaging set gambar	`AWS::MedicalImaging::ImageSet`
Amazon Managed Workflows for Apache Airflow	Aktivitas API Amazon MWAA di lingkungan.	Apache Airflow yang Dikelola	`AWS::MWAA::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Grafik Amazon Neptunus	Aktivitas API data, misalnya kueri, algoritme , atau pencarian vektor, pada Grafik Neptunus.	Grafik Neptunus	`AWS::NeptuneGraph::Graph`
Monitor Aliran CloudWatch Jaringan Amazon	Aktivitas API Monitor Aliran CloudWatch Jaringan Amazon pada monitor.	Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Monitor`
Monitor Aliran CloudWatch Jaringan Amazon	Amazon CloudWatch Network Flow Monitor aktivitas API pada cakupan.	Lingkup Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Scope`
Amazon NovaAct	Aktivitas Amazon NovaAct API pada definisi alur kerja.	Definisi alur kerja	`AWS::NovaAct::WorkflowDefinition`
Amazon NovaAct	Aktivitas NovaAct API Amanzon pada alur kerja berjalan.	Alur kerja berjalan	`AWS::NovaAct::WorkflowRun`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise di UKey.	Amazon Satu uKey	`AWS::One::UKey`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise pada pengguna.	Amazon Satu Pengguna	`AWS::One::User`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada alias.	Alias Kriptografi Pembayaran	`AWS::PaymentCryptography::Alias`
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada kunci.	Kunci Kriptografi Pembayaran	`AWS::PaymentCryptography::Key`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API Direktori Aktif.	Konektor CA Pribadi untuk Direktori Aktif	`AWS::PCAConnectorAD::Connector`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API SCEP.	Konektor CA Pribadi untuk SCEP	`AWS::PCAConnectorSCEP::Connector`
Amazon Pinpoint	Amazon Pinpoint aktivitas API pada aplikasi penargetan seluler.	Aplikasi Penargetan Seluler	`AWS::Pinpoint::App`
Aplikasi Amazon Q	Aktivitas API data di Amazon Q Apps. Untuk informasi selengkapnya, lihat Amazon Q Apps.	Aplikasi Amazon Q	`AWS::QApps::QApp`
Aplikasi Amazon Q	Aktivitas API data di sesi Amazon Q App.	Sesi Aplikasi Amazon Q	`AWS::QApps::QAppSession`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada aplikasi. Untuk informasi selengkapnya, lihat Amazon Q Business.	Aplikasi Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada sumber data. Untuk informasi selengkapnya, lihat Amazon Q Business.	Sumber data Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Bisnis	Aktivitas API Amazon Q Business pada indeks. Untuk informasi selengkapnya, lihat Amazon Q Business.	Amazon Q Indeks Bisnis	`AWS::QBusiness::Index`
Amazon Q Bisnis	Aktivitas API integrasi Amazon Q Business.	Integrasi Amazon Q Bisnis	`AWS::QBusiness::Integration`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada pengalaman web. Untuk informasi selengkapnya, lihat Amazon Q Business.	Pengalaman web Amazon Q Bisnis	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada integrasi.	Q Integrasi pengembang	`AWS::QDeveloper::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Cepat Amazon pada konektor tindakan.	AWS QuickSuite Tindakan	`AWS::Quicksight::ActionConnector`
QuickSight Aplikasi Amazon	Aktivitas API pada `AWS::QuickSight::App` sumber daya.	QuickSight Aplikasi Amazon	`AWS::QuickSight::App`
QuickSight otomatisasi	Aktivitas API pada `AWS::QuickSight::Automation` sumber daya.	QuickSight otomatisasi	`AWS::QuickSight::Automation`
QuickSight pekerjaan otomatisasi	Aktivitas API pada `AWS::QuickSight::AutomationJob` sumber daya.	QuickSight pekerjaan otomatisasi	`AWS::QuickSight::AutomationJob`
AWS QuickSight Ekstensi	Aktivitas API pada `AWS::QuickSight::Extension` sumber daya.	AWS QuickSight Ekstensi	`AWS::QuickSight::Extension`
AWS QuickSight Akses Ekstensi	Aktivitas API pada `AWS::QuickSight::ExtensionAccess` sumber daya.	AWS QuickSight Akses Ekstensi	`AWS::QuickSight::ExtensionAccess`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Aliran Cepat Amazon.	AWS QuickSight aliran	`AWS::QuickSight::Flow`
Amazon Quick	Aktivitas FlowSession API Cepat Amazon.	AWS QuickSight sesi aliran	`AWS::QuickSight::FlowSession`
QuickSight Halaman Amazon	Aktivitas API pada `AWS::QuickSight::Page` sumber daya.	QuickSight Halaman Amazon	`AWS::QuickSight::Page`
QuickSight Tugas	Aktivitas API pada `AWS::QuickSight::Task` sumber daya.	QuickSight Tugas	`AWS::QuickSight::Task`
Amazon RDS	Aktivitas Amazon RDS API di Cluster DB. Untuk informasi selengkapnya, lihat Amazon RDS.	API Data RDS - Kluster DB	`AWS::RDS::DBCluster`
Amazon Redshift	Aktivitas Redshift API pada cluster.	Gugus Pergeseran Merah	`AWS::Redshift::Cluster`
AWS Tampilan terkelola Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::ManagedView` sumber daya.	AWS Tampilan terkelola Resource Explorer	`AWS::ResourceExplorer2::ManagedView`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Tampilan Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::View` sumber daya.	AWS Tampilan Resource Explorer	`AWS::ResourceExplorer2::View`
Amazon CloudWatch RUM	Aktivitas Amazon CloudWatch RUM API di monitor aplikasi.	Monitor aplikasi RUM	`AWS::RUM::AppMonitor`
Amazon S3	Aktivitas API Amazon S3 pada titik akses. Untuk informasi selengkapnya, lihat Amazon S3.	Titik Akses S3	`AWS::S3::AccessPoint`
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket tujuan umum. Untuk informasi selengkapnya, lihat Amazon S3.	S3	`AWS::S3::Object`
Titik Akses Ekspres S3	Aktivitas API pada `AWS::S3Express::AccessPoint` sumber daya.	Titik Akses Ekspres S3	`AWS::S3Express::AccessPoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket direktori . Untuk informasi selengkapnya, lihat Amazon S3.	S3 Ekspres	`AWS::S3Express::Object`
Amazon S3	Aktivitas API titik akses Objek Lambda Amazon S3, seperti panggilan ke dan. CompleteMultipartU pload GetObject Untuk informasi selengkapnya, lihat Amazon S3.	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 pada aktivitas API tingkat objek Outposts. Untuk informasi selengkap nya, lihat Amazon S3 on Outposts.	Outposts S3	`AWS::S3Outposts::Object`
Tabel Amazon S3	Aktivitas API Amazon S3 pada tabel. Untuk informasi selengkap nya, lihat Tabel Amazon S3.	Tabel S3	`AWS::S3Tables::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Tabel Amazon S3	Aktivitas API Amazon S3 pada bucket meja. Untuk informasi selengkapnya, lihat Tabel Amazon S3.	Ember meja S3	`AWS::S3Tables::TableBucket`
Vektor Amazon S3	Aktivitas API Amazon S3 pada indeks vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Indeks vektor S3	`AWS::S3Vectors::Index`
Vektor Amazon S3	Aktivitas API Amazon S3 pada bucket vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Ember vektor S3	`AWS::S3Vectors::VectorBucket`
Amazon SageMaker AI	InvokeEndpointWithResponseStream Aktivitas Amazon SageMaker AI di titik akhir. Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker titik akhir	`AWS::SageMaker::Endpoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API pada komponen percobaan percobaan . Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker komponen uji coba eksperimen metrik	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API di toko fitur.	SageMaker Toko Fitur	`AWS::SageMaker::FeatureGroup`
SageMaker hub	Aktivitas API pada `AWS::SageMaker::Hub` sumber daya.	SageMaker hub	`AWS::SageMaker::Hub`
SageMaker Lowongan kerja	Aktivitas API pada `AWS::SageMaker::Job` sumber daya.	SageMaker Lowongan	`AWS::SageMaker::Job`
AWS SageMaker MlflowApp	Aktivitas API pada `AWS::SageMaker::MlflowApp` sumber daya.	AWS SageMaker MlflowApp	`AWS::SageMaker::MlflowApp`
Amazon SageMaker AI	Aktivitas API Amazon SageMaker AI MLFlow.	SageMaker MLFlow	`AWS::SageMaker::MlflowTrackingServer`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
SageMaker sesi pelatihan	Aktivitas API pada `AWS::SageMaker::TrainingSession` sumber daya.	SageMaker sesi pelatihan	`AWS::SageMaker::TrainingSession`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::BusinessRule` sumber daya.	AWS: :SCN:: BusinessRule	`AWS::SCN::BusinessRule`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::DataLakeException` sumber daya.	AWS: :SCN:: DataLakeException	`AWS::SCN::DataLakeException`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionInvestigation` sumber daya.	AWS: :SCN:: Exception Investigation	`AWS::SCN::ExceptionInvestigation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionRule` sumber daya.	AWS: :SCN:: Exception Rule	`AWS::SCN::ExceptionRule`
AWS Rantai Pasokan	Aktivitas API Rantai Pasokan pada sebuah instance.	Keputusan Amazon Connect	`AWS::SCN::Instance`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Metric` sumber daya.	AWS: :SCN: :M	`AWS::SCN::Metric`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::MetricEvaluation` sumber daya.	AWS: :SCN:: MetricEva luation	`AWS::SCN::MetricEvaluation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Outcome` sumber daya.	AWS: :SCN: :H	`AWS::SCN::Outcome`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::OutcomeTemplate` sumber daya.	AWS: :SCN:: OutcomeTe mplate	`AWS::SCN::OutcomeTemplate`
Amazon SimpleDB	Aktivitas API Amazon SimpleDB di domain.	Domain SimpleDB	`AWS::SDB::Domain`
AWS Cloud Map	AWS Aktivitas Cloud Map API pada namespace. Untuk informasi selengkap nya, lihat AWS Cloud Map.	AWS Ruang nama Cloud Map	`AWS::ServiceDiscovery::Name space`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Cloud Map	AWS Aktivitas Cloud Map API pada suatu layanan. Untuk informasi selengkapnya, lihat AWS Cloud Map.	AWS Layanan Cloud Map	`AWS::ServiceDiscovery::Service`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada set konfigurasi.	Set konfigurasi SES	`AWS::SES::ConfigurationSet`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada identitas email.	Identitas SES	`AWS::SES::EmailIdentity`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada template.	Templat SES	`AWS::SES::Template`
AWS Penandatangan	Aktivitas API penandatangan saat menandatangani pekerjaan.	Pekerjaan penandatanganan penandatangan	`AWS::Signer::SigningJob`
AWS Penandatangan	Aktivitas API penandatangan pada profil penandatanganan.	Profil penandatanganan penandatangan	`AWS::Signer::SigningProfile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Asisten IoT SiteWise	Aktivitas API Asisten Sitewise pada percakapan.	Percakapan Asisten Sitewise	`AWS::SitewiseAssistant::Conversation`
Pencarian Operator	Aktivitas API pada `AWS::SMSVoice::CarrierLookup` sumber daya.	Pencarian Operator	`AWS::SMSVoice::CarrierLookup`
Set Konfigurasi	Aktivitas API pada `AWS::SMSVoice::ConfigurationSet` sumber daya.	Set Konfigurasi	`AWS::SMSVoice::ConfigurationSet`
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada pesan. Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Pesan Suara SMS	`AWS::SMSVoice::Message`
Beritahu Konfigurasi	Aktivitas API pada `AWS::SMSVoice::NotifyConfiguration` sumber daya.	Beritahu Konfigurasi	`AWS::SMSVoice::NotifyConfiguration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada identitas originasi . Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Identitas originasi SMS Voice	`AWS::SMSVoice::OriginationIdentity`
Amazon SNS	Amazon SNS Publikasikan operasi API pada titik akhir platform. Untuk informasi selengkapnya, lihat Amazon SNS.	Titik akhir platform SNS	`AWS::SNS::PlatformEndpoint`
Amazon SNS	Amazon SNS Publish dan operasi PublishBatch API pada topik. Untuk informasi selengkapnya, lihat Amazon SNS.	Topik SNS	`AWS::SNS::Topic`
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID nomor telepon. Untuk informasi selengkapnya, lihat AWS End User Messaging Sosial.	Social-Messaging ID Nomor Telepon	`AWS::SocialMessaging::PhoneNumberId`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID Waba.	Social-Messaging ID Waba	`AWS::SocialMessaging::WabaId`
Amazon SQS	Aktivitas Amazon SQS API pada pesan. Untuk informasi selengkapnya, lihat Amazon SQS.	SQS	`AWS::SQS::Queue`
AWS Systems Manager	Aktivitas API Systems Manager pada penilaian dampak.	Penilaian Dampak SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Aktivitas API Systems Manager pada node terkelola. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Node terkelola Systems Manager	`AWS::SSM::ManagedNode`
AWS Systems Manager	Aktivitas API Systems Manager pada saluran kontrol. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Step Functions	Aktivitas Step Functions API pada aktivitas. Untuk informasi selengkapnya, lihat AWS Step Functions.	Aktivitas Step Functions	`AWS::StepFunctions::Activity`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Step Functions	Aktivitas Step Functions API pada mesin state. Untuk informasi selengkapnya, lihat AWS Step Functions.	Mesin status Step Functions	`AWS::StepFunctions::StateMachine`
Amazon Support	SupportAccess Aktivitas API pada penyewa.	SupportAccess penyewa	`AWS::SupportAccess::Tenant`
Amazon Support	SupportAccess Aktivitas API pada akun yang mempercayai.	SupportAccess akun kepercayaan	`AWS::SupportAccess::TrustingAccount`
Amazon Support	SupportAccess Aktivitas API tentang peran kepercayaan.	SupportAccess peran percaya	`AWS::SupportAccess::TrustingRole`
Amazon SWF	Aktivitas API Amazon SWF di domain. Untuk informasi selengkapnya, lihat Amazon SWF.	Domain SWF	`AWS::SWF::Domain`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Perangkat.	Perangkat Klien Tipis	`AWS::ThinClient::Device`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Lingkungan.	Lingkungan Klien Tipis	`AWS::ThinClient::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Token stempel waktu	Aktivitas API pada `AWS::Timestamp::TimestampToken` sumber daya.	Token stempel waktu	`AWS::Timestamp::TimestampToken`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream di database. Untuk informasi selengkapnya, lihat Amazon Timestream.	Database Timestream	`AWS::Timestream::Database`
Amazon Timestream	Aktivitas API Amazon Timestream di titik akhir regional.	Titik akhir regional Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream pada tabel. Untuk informasi selengkapnya, lihat Amazon Timestream.	Tabel Timestream	`AWS::Timestream::Table`
Transformasi Amazon	Mengubah aktivitas API pada instance agen.	Contoh agen transformasi	`AWS::Transform::AgentInstance`
Amazon Q Transform AKA AWS Transformasi	Aktivitas API pada `AWS::Transform::Profile` sumber daya.	mengubah	`AWS::Transform::Profile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada kampanye.	Transform -Custom kampanye	`AWS::TransformCustom::Campaign`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada percakapan.	Transform -Custom percakapan	`AWS::TransformCustom::Conversation`
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada item pengetahuan.	Transform- Custom item pengetahuan	`AWS::TransformCustom::KnowledgeItem`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada paket.	Transform- Custom paket	`AWS::TransformCustom::Package`
Kustomisasi akun UXC	Aktivitas API pada `AWS::UXC::AccountCustomization` sumber daya.	Kustomisasi akun UXC	`AWS::UXC::AccountCustomization`
Izin Terverifikasi Amazon	Aktivitas API Izin Terverifikasi Amazon di toko kebijakan.	Izin Terverifikasi Amazon	`AWS::VerifiedPermissions::PolicyStore`
Well-Architected rekomendasi agen	Aktivitas API pada `AWS::WellArchitected::AgentRecommendation` sumber daya.	Well-Architected rekomendasi agen	`AWS::WellArchitected::AgentRecommendation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS X-Ray	X-Ray Aktivitas API pada jejak. Untuk informasi selengkapnya, lihat AWS X-Ray.	X-Ray jejak	`AWS::XRay::Trace`

Peristiwa data tidak dicatat secara default saat Anda membuat penyimpanan data jejak atau peristiwa. Untuk merekam peristiwa CloudTrail data, Anda harus secara eksplisit menambahkan setiap jenis sumber daya yang ingin Anda kumpulkan aktivitasnya. Untuk informasi selengkapnya tentang peristiwa data pencatatan, lihatMencatat log peristiwa data.

Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Acara aktivitas jaringan

CloudTrail peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Peristiwa aktivitas jaringan memberikan visibilitas ke dalam operasi sumber daya yang dilakukan dalam VPC.

Anda dapat mencatat peristiwa aktivitas jaringan untuk layanan berikut:

- Amazon Aurora DSQL
- Amazon Bedrock
- ID Suara Amazon Connect
- EventBridge Penjadwal Amazon
- Amazon Fraud Detector
- Amazon HealthLake
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Langganan Amazon Q
- Amazon QuickSight

- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Layanan Streaming Amazon Transcribe
- Izin Terverifikasi Amazon
- Amazon WorkMail
- Platform Pengembang Anthropic Claude di AWS
- Athena
- AWS Registri Agen
- AWS AppConfig
- jaminan aws
- AWS Pertukaran Data B2B
- AWS Kalkulator Harga BCM
- AWS Penagihan
- AWS Cloud Map
- AWS Peringatan Dioda
- AWS Glue
- AWS IdentityStore Layanan
- AWS Faktur
- AWS IoT FleetWise
- AWS Terowongan Aman IoT
- AWS IoT SiteWise
- AWS License Manager
- AWS Pengukuran Pendapatan Pusat Mitra
- AWS Secrets Manager
- AWS SSO
- AWS Step Functions
- AWS Transfer Family
- AWS Transformasi

- AWSBillingAndCostManagementDataExports
- AWSLakeFormation
- Gerbang Cadangan
- Inti Agen Batuan Dasar
- API Kontrol Awan
- CloudFormation
- CloudHSM
- CloudTrail
- CodeDeploy
- Comprehend medis
- Otomatisasi Compute Optimizer
- DynamoDB
- Penskalaan Otomatis EC2
- Elastic Compute Cloud (EC2)
- Sistem File Elastis (EFS)
- pesan pengguna akhir
- IoT
- Layanan Manajemen Kunci (KMS)
- Lambda
- Relational Database Service (RDS) Core Control Plane
- Route 53 DNS Publik
- Vektor S3
- Layanan Token Keamanan (STS)
- Sign-In Portal
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- LAYANAN ANTRIAN SEDERHANA (SQS)
- Simple Storage Service (S3)
- Layanan Alur Kerja Sederhana (SWF)

- Kontak SSM
- Storage Gateway

Peristiwa aktivitas jaringan tidak dicatat secara default saat Anda membuat penyimpanan data jejak atau peristiwa. Untuk merekam peristiwa aktivitas CloudTrail jaringan, Anda harus secara eksplisit menetapkan sumber acara yang ingin Anda kumpulkan aktivitasnya. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.

Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Insights acara

CloudTrail Peristiwa Insights menangkap tingkat panggilan API atau aktivitas tingkat kesalahan yang tidak biasa di AWS akun Anda dengan menganalisis aktivitas CloudTrail manajemen. Peristiwa wawasan memberikan informasi yang relevan, seperti API terkait, kode kesalahan, waktu kejadian, dan statistik, yang membantu Anda memahami dan bertindak berdasarkan aktivitas yang tidak biasa. Tidak seperti jenis peristiwa lain yang ditangkap dalam penyimpanan data CloudTrail jejak atau peristiwa, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda atau pencatatan tingkat kesalahan yang berbeda secara signifikan dari pola penggunaan biasa akun. Untuk informasi selengkapnya, lihat Bekerja dengan CloudTrail Wawasan.

Contoh aktivitas yang mungkin menghasilkan peristiwa Insights meliputi:

- Akun Anda biasanya mencatat tidak lebih dari 20 panggilan `deleteBucket` API Amazon S3 per menit, tetapi akun Anda mulai mencatat rata-rata 100 panggilan `deleteBucket` API per menit. Peristiwa Insights dicatat pada awal aktivitas yang tidak biasa, dan peristiwa Insights lainnya dicatat untuk menandai akhir dari aktivitas yang tidak biasa.
- Akun Anda biasanya mencatat 20 panggilan per menit ke Amazon EC2 `AuthorizeSecurityGroupIngress` API, tetapi akun Anda mulai mencatat nol panggilan. `AuthorizeSecurityGroupIngress` Peristiwa Insights dicatat pada awal aktivitas yang tidak biasa, dan sepuluh menit kemudian, ketika aktivitas yang tidak biasa berakhir, peristiwa Insights lain dicatat untuk menandai akhir dari aktivitas yang tidak biasa.
- Akun Anda biasanya mencatat kurang dari satu `AccessDeniedException` kesalahan dalam periode tujuh hari di API. AWS Identity and Access Management `DeleteInstanceProfile` Akun Anda mulai mencatat rata-rata 12 `AccessDeniedException` kesalahan per menit pada

panggilan `DeleteInstanceProfile` API. Peristiwa Insights dicatat pada awal aktivitas tingkat kesalahan yang tidak biasa, dan peristiwa Insights lainnya dicatat untuk menandai akhir aktivitas yang tidak biasa.

Contoh-contoh ini disediakan untuk tujuan ilustrasi saja. Hasil Anda dapat bervariasi tergantung pada kasus penggunaan Anda.

Untuk mencatat peristiwa CloudTrail Insights, Anda harus secara eksplisit mengaktifkan peristiwa Insights di penyimpanan data jejak atau peristiwa baru atau yang sudah ada. Untuk informasi selengkapnya tentang membuat jejak, lihatMembuat jejak dengan CloudTrail konsol. Untuk informasi selengkapnya tentang membuat penyimpanan data acara, lihatMembuat penyimpanan data acara untuk acara Insights dengan konsol.

Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jejak dan acara. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Riwayat acara

CloudTrail riwayat acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir peristiwa manajemen dalam file. CloudTrail Wilayah AWS Anda dapat menggunakan riwayat ini untuk mendapatkan visibilitas ke tindakan yang diambil di AWS akun Anda di Konsol Manajemen AWS, AWS SDK, alat baris perintah, dan layanan lainnya AWS . Anda dapat menyesuaikan tampilan riwayat acara di CloudTrail konsol dengan memilih kolom mana yang ditampilkan. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.

Jalan setapak

Trail adalah konfigurasi yang memungkinkan pengiriman CloudTrail peristiwa ke bucket S3, dengan pengiriman opsional ke CloudWatch Log dan Amazon EventBridge. Anda dapat menggunakan jejak untuk memilih CloudTrail peristiwa yang ingin dikirimkan, mengenkripsi file log CloudTrail peristiwa dengan AWS KMS kunci, dan mengatur notifikasi Amazon SNS untuk pengiriman file log. Untuk informasi selengkapnya tentang cara membuat dan mengelola jejak, lihatMembuat jejak untuk Anda Akun AWS.

Multi-Region dan jalur Single-region

Anda dapat membuat jalur Multi-wilayah dan Single-region untuk Anda. Akun AWS

Multi-Region jalan setapak

Saat Anda membuat jejak Multi-wilayah, CloudTrail merekam peristiwa di semua peristiwa Wilayah AWS yang diaktifkan di dalam Anda Akun AWS dan mengirimkan file log CloudTrail peristiwa ke bucket S3 yang Anda tentukan. Sebagai praktik terbaik, kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Anda dapat mengonversi jejak wilayah Tunggal menjadi jejak Multi-wilayah dengan menggunakan. AWS CLI Lihat informasi selengkapnya di Memahami jalur Multi-wilayah dan Wilayah keikutsertaan, Membuat jejak dengan konsol, dan Mengkonversi jalur satu wilayah ke jalur multi-wilayah.

Single-Region jalan setapak

Saat Anda membuat jejak wilayah Tunggal, hanya CloudTrail mencatat peristiwa di Wilayah tersebut. Kemudian mengirimkan file log CloudTrail peristiwa ke bucket Amazon S3 yang Anda tentukan. Anda hanya dapat membuat jejak wilayah Tunggal dengan menggunakan. AWS CLI Jika Anda membuat jalur tunggal tambahan, Anda dapat meminta jejak tersebut mengirimkan file log CloudTrail peristiwa ke bucket S3 yang sama atau ke bucket terpisah. Ini adalah opsi default saat Anda membuat jejak menggunakan AWS CLI atau CloudTrail API. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola jalur dengan AWS CLI.

> **Note**
>
> Untuk kedua jenis jalur, Anda dapat menentukan bucket Amazon S3 dari Wilayah mana pun.

Jejak multi-wilayah memiliki keuntungan sebagai berikut:

- Pengaturan konfigurasi untuk jejak berlaku secara konsisten di semua yang diaktifkan Wilayah AWS.
- Anda menerima CloudTrail peristiwa dari semua yang diaktifkan Wilayah AWS dalam satu bucket Amazon S3 dan, secara opsional, dalam grup CloudWatch log Log.
- Anda mengelola konfigurasi jejak untuk semua yang diaktifkan Wilayah AWS dari satu lokasi.

Membuat jejak Multi-region, memiliki efek sebagai berikut:

- CloudTrail mengirimkan file log untuk aktivitas akun dari semua yang diaktifkan Wilayah AWS ke bucket Amazon S3 tunggal yang Anda tentukan, dan, secara opsional, ke CloudWatch grup log Log.
- Jika Anda mengonfigurasi topik Amazon SNS untuk jejak, pemberitahuan SNS tentang pengiriman file log di semua yang diaktifkan Wilayah AWS akan dikirim ke topik SNS tunggal tersebut.
- Anda dapat melihat jejak Multi-wilayah di semua diaktifkan Wilayah AWS, tetapi Anda hanya dapat memodifikasi jejak di Wilayah asal tempat ia dibuat.

Terlepas dari apakah jejak itu Multi-wilayah atau Single-region, acara yang dikirim ke Amazon EventBridge diterima di bus acara masing-masing Wilayah, bukan dalam satu bus acara tunggal.

Beberapa jalur per Wilayah

Jika Anda memiliki grup pengguna yang berbeda tetapi terkait, seperti pengembang, petugas keamanan, dan auditor TI, Anda dapat membuat beberapa jejak per Wilayah. Hal ini memungkinkan setiap grup untuk menerima salinan sendiri dari file log.

CloudTrail mendukung lima jalur per Wilayah. Jejak multi-wilayah dihitung sebagai satu jalur per Wilayah.

Berikut ini adalah contoh Wilayah dengan lima jalur:

- Anda membuat dua jalur di Wilayah AS Barat (California Utara) yang hanya berlaku untuk Wilayah ini.
- Anda membuat dua jalur Multi-wilayah lagi di Wilayah AS Barat (California Utara).
- Anda membuat jalur Multi-wilayah lainnya di Wilayah Asia Pasifik (Sydney). Jejak ini juga ada sebagai jejak di Wilayah AS Barat (California N.).

Anda dapat melihat daftar jejak di halaman Trails konsol. Wilayah AWS CloudTrail Untuk informasi selengkapnya, lihat Memperbarui jejak dengan CloudTrail konsol. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Jejak organisasi

Jejak organisasi adalah konfigurasi yang memungkinkan pengiriman CloudTrail peristiwa di akun manajemen dan semua akun anggota dalam AWS Organizations organisasi ke bucket Amazon S3, CloudWatch Log, dan Amazon yang sama. EventBridge Membuat jejak organisasi membantu Anda menentukan strategi pencatatan peristiwa yang seragam untuk organisasi Anda.

Semua jejak organisasi yang dibuat menggunakan konsol adalah jejak organisasi multi-wilayah yang mencatat peristiwa dari diaktifkan di setiap akun anggota Wilayah AWS di organisasi. Untuk mencatat peristiwa di semua AWS partisi di organisasi Anda, buat jejak organisasi Multi-region di setiap partisi. Anda dapat membuat jejak organisasi Single-region atau Multi-region dengan menggunakan. AWS CLI Jika Anda membuat jejak wilayah Tunggal, Anda mencatat aktivitas hanya di jalur Wilayah AWS (juga disebut sebagai Wilayah Asal).

Meskipun sebagian besar Wilayah AWS diaktifkan secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual (juga disebut sebagai Wilayah keikutsertaan). Untuk informasi tentang Wilayah mana yang diaktifkan secara default, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi.AWS Account Management Untuk daftar CloudTrail dukungan Wilayah, lihatCloudTrail Daerah yang didukung.

Saat Anda membuat jejak organisasi, salinan jejak dengan nama yang Anda berikan dibuat di akun anggota milik organisasi Anda.

- Jika jejak organisasi adalah untuk Wilayah Tunggal dan Wilayah asal jejak bukan Wilayah keikutsertaan, salinan jejak dibuat di Wilayah asal jejak organisasi di setiap akun anggota.
- Jika jejak organisasi adalah untuk Wilayah Tunggal dan Wilayah asal jejak adalah Wilayah keikutsertaan, salinan jejak tersebut dibuat di Wilayah asal jejak organisasi di akun anggota yang telah mengaktifkan Wilayah tersebut.
- Jika jejak organisasi adalah Multi-wilayah dan Wilayah asal jejak bukan merupakan Wilayah keikutsertaan, salinan jejak dibuat di setiap akun yang diaktifkan Wilayah AWS di setiap akun anggota. Ketika akun anggota mengaktifkan Wilayah keikutsertaan, salinan jejak Multi-wilayah dibuat di Wilayah yang baru dipilih untuk akun anggota setelah aktivasi Wilayah tersebut selesai.
- Jika jejak organisasi adalah Multi-wilayah dan Wilayah asal adalah Wilayah keikutsertaan, akun anggota tidak akan mengirim aktivitas ke jejak organisasi kecuali mereka memilih Wilayah AWS tempat jejak Multi-wilayah dibuat. Misalnya, jika Anda membuat jejak Multi-wilayah dan memilih Wilayah Eropa (Spanyol) sebagai Wilayah asal untuk jejak tersebut, hanya akun anggota yang mengaktifkan Wilayah Eropa (Spanyol) untuk akun mereka yang akan mengirimkan aktivitas akun mereka ke jejak organisasi.

> **Note**
>
> CloudTrail membuat jejak organisasi di akun anggota meskipun validasi sumber daya gagal. Contoh kegagalan validasi meliputi:

- kebijakan bucket Amazon S3 yang salah
- kebijakan topik Amazon SNS yang salah
- ketidakmampuan untuk mengirimkan ke grup CloudWatch log Log
- izin yang tidak memadai untuk mengenkripsi menggunakan kunci KMS

Akun anggota dengan CloudTrail izin dapat melihat kegagalan validasi untuk jejak organisasi dengan melihat halaman detail jejak di CloudTrail konsol, atau dengan menjalankan perintah. AWS CLI get-trail-status

Pengguna dengan CloudTrail izin di akun anggota akan dapat melihat jejak organisasi (termasuk jejak ARN) saat mereka masuk ke CloudTrail konsol dari AWS akun mereka, atau ketika mereka menjalankan AWS CLI perintah seperti `describe-trails` (meskipun akun anggota harus menggunakan ARN untuk jejak organisasi, dan bukan nama, saat menggunakan). AWS CLI Namun, pengguna di akun anggota tidak akan memiliki izin yang cukup untuk menghapus jejak organisasi, mengaktifkan atau menonaktifkan log, mengubah jenis peristiwa apa yang dicatat, atau mengubah jejak organisasi dengan cara apa pun. Untuk informasi selengkapnya AWS Organizations, lihat Organizations Terminology and Concepts. Untuk informasi selengkapnya tentang membuat dan bekerja dengan jalur organisasi, lihatMembuat jejak untuk sebuah organisasi.

CloudTrail Penyimpanan data danau dan acara

CloudTrail Lake memungkinkan Anda menjalankan SQL-based kueri halus pada acara Anda, dan mencatat peristiwa dari sumber di luar AWS, termasuk dari aplikasi Anda sendiri, dan dari mitra yang terintegrasi dengannya. CloudTrail Anda tidak perlu memiliki jejak yang dikonfigurasi di akun Anda untuk menggunakan CloudTrail Lake.

Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Anda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika Anda memilih opsi harga retensi yang One-year dapat diperpanjang, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi. Seven-year Anda dapat menyimpan kueri Lake untuk penggunaan di masa mendatang, dan melihat hasil kueri hingga tujuh hari. Anda juga dapat menyimpan hasil kueri ke bucket S3. CloudTrail Danau juga dapat menyimpan acara dari organisasi di AWS Organizations dalam penyimpanan data acara, atau acara dari beberapa Wilayah dan akun. CloudTrail Lake adalah bagian dari solusi audit yang membantu

Anda melakukan investigasi keamanan dan pemecahan masalah. Untuk informasi selengkapnya, lihat Bekerja dengan AWS CloudTrail Danau dan CloudTrail Konsep dan terminologi danau.

CloudTrail Wawasan

CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons volume panggilan API yang tidak biasa atau kesalahan yang dicatat pada panggilan API dengan terus menganalisis peristiwa CloudTrail manajemen. Peristiwa Insights adalah catatan tingkat aktivitas API `write` manajemen yang tidak biasa, atau tingkat kesalahan yang tidak biasa yang ditampilkan pada aktivitas API manajemen. Secara default, jejak dan penyimpanan data acara tidak mencatat peristiwa CloudTrail Wawasan. Di konsol, Anda dapat memilih untuk mencatat peristiwa Wawasan saat membuat atau memperbarui penyimpanan data jejak atau peristiwa. Saat menggunakan CloudTrail API, Anda dapat mencatat peristiwa Insights dengan mengedit pengaturan penyimpanan data jejak atau peristiwa yang ada dengan `PutInsightSelectors`API. Biaya tambahan berlaku untuk acara logging CloudTrail Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jejak dan acara. Untuk informasi selengkapnya, lihat Bekerja dengan CloudTrail Wawasan dan Harga AWS CloudTrail.

Tanda

Tag adalah kunci yang ditentukan pelanggan dan nilai opsional yang dapat ditetapkan ke AWS sumber daya, seperti CloudTrail jejak, penyimpanan data peristiwa, dan saluran, bucket S3 yang digunakan untuk menyimpan file CloudTrail log, organisasi dan unit AWS Organizations organisasi, dan banyak lagi. Dengan menambahkan tag yang sama ke jejak dan ke bucket S3 yang Anda gunakan untuk menyimpan file log untuk jejak, Anda dapat mempermudah pengelolaan, pencarian, dan memfilter sumber daya ini. AWS Resource Groups Anda dapat menerapkan strategi penandaan untuk membantu Anda secara konsisten, efektif, dan mudah menemukan dan mengelola sumber daya Anda. Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Menandai AWS Sumber Daya.

AWS Security Token Service dan CloudTrail

AWS Security Token Service (AWS STS) adalah layanan yang memiliki titik akhir global dan juga mendukung titik Region-specific akhir. Endpoint adalah URL yang merupakan titik masuk untuk permintaan layanan web. Misalnya, `https://cloudtrail.us-west-2.amazonaws.com` adalah titik masuk regional AS Barat (Oregon) untuk AWS CloudTrail layanan ini. Titik akhir regional membantu mengurangi latensi dalam aplikasi Anda.

Saat Anda menggunakan AWS STS Region-specific titik akhir, jejak di Wilayah itu hanya mengirimkan AWS STS peristiwa yang terjadi di Wilayah tersebut. Misalnya, jika Anda menggunakan

titik akhir`sts.us-west-2.amazonaws.com`, jejak di us-west-2 hanya memberikan peristiwa yang berasal dari us-west-2. AWS STS Untuk informasi selengkapnya tentang titik akhir AWS STS regional, lihat Mengaktifkan dan Menonaktifkan AWS STS di AWS Wilayah di Panduan Pengguna IAM.

Untuk daftar lengkap titik akhir AWS regional, lihat AWS Wilayah dan Titik Akhir di. Referensi Umum AWS Untuk detail tentang peristiwa dari AWS STS titik akhir global, lihatAcara layanan global.

Acara layanan global

> **Important**
>
> Per 22 November 2021, AWS CloudTrail mengubah cara jejak menangkap peristiwa layanan global. Sekarang, peristiwa yang dibuat oleh Amazon CloudFront AWS Identity and Access Management,, dan AWS STS dicatat di Wilayah di mana mereka diciptakan, Wilayah AS Timur (Virginia N.), us-east-1. Hal ini membuat bagaimana CloudTrail memperlakukan layanan ini konsisten dengan layanan AWS global lainnya. Untuk terus menerima acara layanan global di luar US East (Virginia N.), pastikan untuk mengubah jalur Single-region menggunakan acara layanan global di luar US East (Virginia N.) menjadi jalur Multi-wilayah. Untuk informasi selengkapnya tentang menangkap peristiwa layanan global, lihat Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global nanti di bagian ini. Sebaliknya, Riwayat acara di CloudTrail konsol dan aws cloudtrail lookup-events perintah akan menampilkan peristiwa ini di Wilayah AWS tempat kejadian.

Untuk sebagian besar layanan, peristiwa dicatat di Wilayah tempat terjadinya tindakan. Untuk layanan global seperti AWS Identity and Access Management (IAM), dan Amazon AWS STS CloudFront, acara dikirimkan ke jalur apa pun yang mencakup layanan global.

Untuk sebagian besar layanan global, peristiwa dicatat sebagai terjadi di Wilayah AS Timur (Virginia N.), tetapi beberapa peristiwa layanan global dicatat sebagai terjadi di Wilayah lain, seperti Wilayah AS Timur (Ohio) atau Wilayah AS Barat (Oregon).

Untuk menghindari menerima duplikat acara layanan global, ingat hal berikut:

- Acara layanan global dikirimkan secara default ke jejak yang dibuat menggunakan CloudTrail konsol. Acara dikirim ke ember untuk jalan setapak.

- Jika Anda memiliki beberapa jalur Wilayah tunggal, pertimbangkan untuk mengonfigurasi jalur Anda sehingga acara layanan global dikirimkan hanya di salah satu jalur. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global.
- `IncludeGlobalServiceEvents`Kapan`true`, CloudTrail mengirimkan acara layanan global hanya ke jalur Single-region di AS Timur (Virginia N.). Untuk jalur Multi-wilayah, `IncludeGlobalServiceEvents` harus. `true`

  Untuk informasi selengkapnya tentang mengubah pencatatan peristiwa layanan global untuk jejak, lihatMengaktifkan dan menonaktifkan pencatatan peristiwa layanan global.

Contoh:

1. Anda membuat jejak di CloudTrail konsol. Secara default, jejak ini mencatat peristiwa layanan global.
2. Anda memiliki beberapa jalur Wilayah tunggal.
3. Anda tidak perlu menyertakan layanan global untuk jalur Wilayah tunggal. Acara layanan global dikirimkan untuk jalur pertama. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola jalur dengan AWS CLI.

> **Note**
>
> Saat membuat atau memperbarui jejak dengan AWS CLI, AWS SDK, atau CloudTrail API, Anda dapat menentukan apakah akan menyertakan atau mengecualikan peristiwa layanan global untuk jejak. Anda tidak dapat mengonfigurasi pencatatan peristiwa layanan global dari CloudTrail konsol.

CloudTrail Daerah yang didukung

> **Note**
>
> Untuk informasi tentang Wilayah yang didukung oleh CloudTrail Danau, lihatCloudTrail Daerah yang didukung Danau.
> Untuk informasi tentang titik akhir bidang data, lihat Titik akhir bidang data di. Referensi Umum AWS

Nama wilayah	Region	Kontrol titik akhir pesawat	Protokol	Tanggal Support
US East (Northern Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	11/13/2013
AS Timur (Ohio)	us–east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	10/17/2016
AS Barat (California Utara)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	05/13/2014
AS Barat (Oregon)	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	11/13/2013
Africa (Cape Town)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	04/22/2020
Asia Pasifik (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	04/24/2019
Asia Pasifik (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	11/22/2022
Asia Pasifik (Jakarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
Asia Pasifik (Malaysia)	ap-southeast-5	cloudtrail.ap-southeast-5.amazonaws.com	HTTPS	08/22/2024
Asia Pacific (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	01/23/2023
Asia Pasifik (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	06/27/2016

Nama wilayah	Region	Kontrol titik akhir pesawat	Protokol	Tanggal Support
Asia Pacific (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	02/12/2018
Asia Pasifik (Seoul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	01/06/2016
Asia Pasifik (Singapura)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	06/30/2014
Asia Pasifik (Sydney)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	05/13/2014
Asia Pasifik (Thailand)	ap-tenggara7	cloudtrail.ap-southeast-7.amazonaws.com	HTTPS	01/07/2025
Asia Pasifik (Tokyo)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	06/30/2014
Kanada (Pusat)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	12/08/2016
Kanada Barat (Calgary)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	12/20/2023
Tiongkok (Beijing)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	03/01/2014
Tiongkok (Ningxia)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	12/11/2017
Eropa (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	10/23/2014
Eropa (Irlandia)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	05/13/2014

Nama wilayah	Region	Kontrol titik akhir pesawat	Protokol	Tanggal Support
Eropa (London)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	12/13/2016
Europe (Milan)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	04/27/2020
Eropa (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	12/18/2017
Eropa (Spanyol)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
Eropa (Stockholm)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	12/11/2018
Europe (Zurich)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Israel (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	07/31/2023
Meksiko (Tengah)	mx-pusat-1	cloudtrail.mx-central-1.amazonaws.com	HTTPS	01/13/2025
Timur Tengah (Bahrain)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	07/29/2019
Timur Tengah (UAE)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	08/30/2022
Amerika Selatan (Sao Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	06/30/2014

Nama wilayah	Region	Kontrol titik akhir pesawat	Protokol	Tanggal Support
AWS GovCloud (AS-Timur)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	11/12/2018
AWS GovCloud (AS-Barat)	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	08/16/2011

Untuk informasi selengkapnya tentang penggunaan CloudTrail di AWS GovCloud (US) Regions, lihat Titik Akhir Layanan di Panduan AWS GovCloud (US) Pengguna.

Untuk informasi lebih lanjut tentang penggunaan CloudTrail di Wilayah Tiongkok (Beijing), lihat Titik Akhir ARNs dan AWS untuk di Tiongkok di. Referensi Umum Amazon Web Services

CloudTrail layanan dan integrasi yang didukung

CloudTrail mendukung acara logging untuk banyak orang Layanan AWS. Anda dapat menemukan spesifikasi untuk setiap layanan yang didukung dalam panduan layanan itu. Untuk daftar topik khusus layanan, lihat. AWS topik layanan untuk CloudTrail Selain itu, beberapa Layanan AWS dapat digunakan untuk menganalisis dan menindaklanjuti data yang dikumpulkan dalam CloudTrail log.

> **Note**
>
> Untuk melihat daftar Wilayah yang didukung untuk setiap layanan, lihat Titik akhir layanan dan kuota di. Referensi Umum Amazon Web Services

Topik

- AWS integrasi layanan dengan log CloudTrail
- CloudTrail Integrasi dengan Amazon EventBridge
- CloudTrail Integrasi dengan AWS Organizations
- CloudTrail Integrasi dengan AWS Control Tower
- CloudTrail integrasi dengan Amazon Security Lake

- CloudTrail Integrasi danau dengan Amazon Athena
- CloudTrail Integrasi danau dengan AWS Config
- CloudTrail Integrasi danau dengan AWS Audit Manager
- AWS topik layanan untuk CloudTrail
- CloudTrail layanan yang tidak didukung

AWS integrasi layanan dengan log CloudTrail

> **Note**
>
> Anda juga dapat menggunakan CloudTrail Lake untuk menanyakan dan menganalisis acara Anda. CloudTrail Kueri danau menawarkan tampilan acara yang lebih dalam dan lebih dapat disesuaikan daripada pencarian kunci dan nilai sederhana dalam riwayat Acara, atau berjalan. `LookupEvents` CloudTrail Pengguna Lake dapat menjalankan kueri Standard Query Language (SQL) yang kompleks di beberapa bidang dalam suatu CloudTrail peristiwa. Untuk informasi selengkapnya, lihat Bekerja dengan AWS CloudTrail Danau dan Menyalin acara jejak ke Danau CloudTrail.
> CloudTrail Penyimpanan data acara danau dan kueri dikenakan biaya CloudTrail . Untuk informasi lebih lanjut tentang harga CloudTrail Danau, lihat AWS CloudTrail Harga.

Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat topik berikut.

AWS Layanan	Topik	Deskripsi
Amazon Athena	Meminta AWS CloudTrail Log	Menggunakan Athena dengan CloudTrail log adalah cara ampuh untuk meningkat kan analisis aktivitas AWS layanan Anda. Misalnya, Anda dapat menggunakan kueri untuk mengidentifikasi tren dan mengisolasi aktivitas selengkapnya berdasark

AWS Layanan	Topik	Deskripsi
		an atribut seperti alamat IP sumber atau pengguna. Anda dapat secara otomatis membuat tabel untuk menanyakan log langsung dari CloudTrail konsol, dan menggunakan tabel tersebut untuk menjalankan kueri di Athena. Untuk informasi selengkapnya, lihat Membuat Tabel untuk CloudTrail Log di CloudTrail Konsol di Panduan Pengguna Amazon Athena. **Note** Menjalankan kueri di Amazon Athena menimbulkan biaya tambahan. Untuk informasi selengkapnya, lihat Harga Amazon Athena.

AWS Layanan	Topik	Deskripsi
CloudWatch Log Amazon	Memantau File CloudTrail Log dengan CloudWatch Log Amazon	Anda dapat mengonfigurasi CloudTrail dengan CloudWatch Log untuk memantau log jejak Anda dan diberi tahu saat aktivitas tertentu terjadi. Misalnya, Anda dapat menentukan filter metrik CloudWatch Log yang akan memicu CloudWatch alarm dan mengirim pemberitahuan kepada Anda saat alarm tersebut dipicu. **Note** Harga standar untuk Amazon CloudWatch dan Amazon CloudWatch Log berlaku. Untuk informasi lebih lanjut, lihat Amazon CloudWatch Harga.

CloudTrail Integrasi dengan Amazon EventBridge

Amazon EventBridge adalah AWS layanan yang memberikan aliran peristiwa sistem yang mendekati real-time yang menggambarkan perubahan AWS sumber daya. Di EventBridge, Anda dapat membuat aturan yang merespons peristiwa yang direkam oleh CloudTrail. Untuk informasi selengkapnya, lihat Membuat aturan di Amazon EventBridge.

Anda dapat mengirimkan acara yang Anda berlangganan di jalur Anda EventBridge dengan membuat aturan dengan EventBridge konsol.

Dari EventBridge konsol:

- Pilih `AWS API Call via CloudTrail` tipe detail untuk mengirimkan CloudTrail data dan acara manajemen dengan file. `eventType` `AwsApiCall` Untuk merekam peristiwa dengan nilai tipe detail`AWS API Call via CloudTrail`, Anda harus memiliki jejak yang saat ini mencatat manajemen atau peristiwa data.
- Pilih `AWS Console Sign In via CloudTrail` tipe detail untuk mengirimkan Konsol Manajemen AWS acara masuk. Untuk merekam peristiwa dengan tipe detail`AWS Console Sign In via CloudTrail`, Anda harus memiliki jejak yang saat ini mencatat peristiwa manajemen.
- Pilih `AWS Insight via CloudTrail` tipe detail untuk menyampaikan acara Insights. Untuk merekam peristiwa dengan nilai tipe detail`AWS Insight via CloudTrail`, Anda harus memiliki jejak yang saat ini mencatat peristiwa Insights. Untuk informasi tentang mencatat peristiwa Wawasan, lihatBekerja dengan CloudTrail Wawasan.

Untuk informasi selengkapnya tentang cara membuat jejak, lihatMembuat jejak dengan CloudTrail konsol.

CloudTrail Integrasi dengan AWS Organizations

Akun manajemen untuk AWS Organizations organisasi dapat menambahkan administrator yang didelegasikan untuk mengelola CloudTrail sumber daya organisasi. Anda dapat membuat jejak organisasi atau penyimpanan data peristiwa organisasi di akun manajemen atau akun administrator yang didelegasikan untuk organisasi yang mengumpulkan semua data peristiwa untuk semua AWS akun di organisasi. AWS Organizations Membuat jejak organisasi atau penyimpanan data acara organisasi membantu Anda menentukan strategi pencatatan peristiwa yang seragam untuk organisasi Anda.

CloudTrail Integrasi dengan AWS Control Tower

AWS Control Tower menyiapkan acara manajemen pencatatan jejak CloudTrail organisasi baru saat Anda menyiapkan landing zone. Saat Anda mendaftarkan akun AWS Control Tower, akun Anda diatur oleh jejak organisasi untuk organisasi. AWS Control Tower Jika Anda memiliki jejak organisasi yang ada di akun tersebut, Anda mungkin melihat tagihan duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum Anda mendaftarkannya. AWS Control Tower Anda dapat melihat halaman Trails di CloudTrail konsol untuk melihat apakah ada jejak organisasi yang telah dibuat. Untuk informasi selengkapnya AWS Control Tower, lihat Tentang masuk AWS Control Tower di Panduan AWS CloudTrail Pengguna.

CloudTrail integrasi dengan Amazon Security Lake

Security Lake dapat mengumpulkan log yang terkait dengan peristiwa CloudTrail manajemen dan peristiwa CloudTrail data untuk S3 dan Lambda. Untuk informasi selengkapnya, lihat log CloudTrail peristiwa di Panduan Pengguna Amazon Security Lake.

Untuk mengumpulkan acara CloudTrail manajemen di Security Lake, Anda harus memiliki setidaknya satu jejak organisasi CloudTrail Multi-wilayah yang mengumpulkan acara CloudTrail manajemen baca dan tulis.

CloudTrail Integrasi danau dengan Amazon Athena

Anda dapat menggabungkan penyimpanan data peristiwa untuk melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL pada data peristiwa menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

CloudTrail Integrasi danau dengan AWS Config

Anda dapat membuat penyimpanan data peristiwa untuk menyertakan item AWS Config konfigurasi, dan menggunakan penyimpanan data peristiwa untuk menyelidiki perubahan yang tidak sesuai pada lingkungan produksi Anda. Untuk informasi selengkapnya, lihat Buat penyimpanan data acara untuk item konfigurasi dengan konsol.

CloudTrail Integrasi danau dengan AWS Audit Manager

Anda dapat membuat penyimpanan data peristiwa untuk AWS Audit Manager bukti menggunakan konsol Audit Manager. Untuk informasi selengkapnya tentang mengumpulkan bukti di CloudTrail Lake menggunakan Audit Manager, lihat Memahami cara kerja pencari bukti dengan CloudTrail Lake di AWS Audit Manager Panduan Pengguna.

AWS topik layanan untuk CloudTrail

Anda dapat mempelajari lebih lanjut tentang bagaimana peristiwa untuk AWS layanan individual direkam dalam CloudTrail log, termasuk contoh peristiwa untuk layanan tersebut dalam file log. Untuk informasi selengkapnya tentang bagaimana AWS layanan tertentu berintegrasi dengan CloudTrail, lihat topik tentang integrasi dalam panduan individual untuk layanan tersebut.

Layanan yang masih dalam pratinjau, atau belum dirilis untuk ketersediaan umum (GA), atau yang tidak memiliki API publik, tidak dianggap didukung.

> **Note**
>
> Untuk melihat daftar Wilayah yang didukung untuk setiap layanan, lihat Titik akhir layanan dan kuota di. Referensi Umum Amazon Web Services
> Untuk informasi tentang layanan mana yang mencatat peristiwa data, lihatPeristiwa data.

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon API Gateway	Log panggilan manajemen API ke Amazon API Gateway Menggunakan AWS CloudTrai l	07/09/2015
Amazon AppFlow	Mencatat panggilan AppFlow API Amazon dengan AWS CloudTrail	04/22/2020
WorkSpaces Aplikasi Amazon	Mencatat Panggilan API WorkSpaces Aplikasi Amazon dengan AWS CloudTrail	04/25/2019
Amazon Athena	Mencatat Panggilan API Amazon Athena dengan AWS CloudTrail	05/19/2017
Amazon Aurora	Memantau panggilan API Amazon Aurora AWS CloudTrail	08/31/2018
Amazon Bedrock	Log panggilan Amazon Bedrock API menggunakan AWS CloudTrail	10/23/2023

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Braket	Pencatatan API Amazon Braket dengan CloudTrail	08/12/2020
Amazon Chime	Log Panggilan Administrasi Amazon Chime Menggunakan AWS CloudTrail	09/27/2017
Direktori Cloud Amazon	Logging Cloud Directory API Calls Menggunakan AWS CloudTrail	01/26/2017
Amazon CloudFront	Menggunakan AWS CloudTrail untuk Menangkap Permintaan yang Dikirim ke CloudFront API	05/28/2014
Amazon CloudSearch	Pencatatan Panggilan Layanan CloudSearch Konfigurasi Amazon Menggunakan AWS CloudTrail	10/16/2014
Amazon CloudWatch	Mencatat Panggilan CloudWatch API Amazon di AWS CloudTrail	04/30/2014
CloudWatch Log Amazon	Logging Amazon CloudWatch Logs API Panggilan di AWS CloudTrail	03/10/2016
Amazon CodeCatalyst	Pencatatan panggilan CodeCatalyst API saat terhubung Akun AWS menggunakan AWS CloudTrail	12/01/2022

AWS Layanan	CloudTrail Topik	Support dimulai
CodeGuru Peninjau Amazon	Mencatat Panggilan API Amazon CodeGuru Reviewer dengan AWS CloudTrail	12/02/2019
Amazon Cognito	Mencatat Panggilan API Amazon Cognito dengan AWS CloudTrail	02/18/2016
Amazon Comprehend	Logging Amazon Comprehend Panggilan API dengan AWS CloudTrail	01/17/2018
Amazon Comprehend Medical	Logging Amazon Comprehend Medical API Calls dengan Menggunakan AWS CloudTrail	11/27/2018
Pelanggan Amazon Connect	Mencatat Panggilan API Amazon Connect dengan AWS CloudTrail	12/11/2019
Amazon Data Firehose	Memantau Panggilan API Firehose Data Amazon dengan AWS CloudTrail	03/17/2016
Amazon Data Lifecycle Manager	Mencatat Panggilan API Amazon Data Lifecycle Manager Menggunakan AWS CloudTrail	07/24/2018
Amazon Detective	Mencatat panggilan Amazon Detective API dengan AWS CloudTrail	03/31/2020
DevOpsGuru Amazon	Mencatat panggilan Amazon DevOps Guru API dengan AWS CloudTrail	05/04/2021

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon DocumentDB (dengan kompatibilitas MongoDB)	Mencatat Panggilan API Amazon DocumentDB dengan AWS CloudTrail	01/09/2019
Amazon DynamoDB	Logging Operasi DynamoDB Dengan Menggunakan AWS CloudTrail	05/28/2015
Amazon EC2	Log panggilan API Amazon EC2 menggunakan AWS CloudTrail	11/13/2013
Amazon EC2 Auto Scaling	Pencatatan Panggilan API Auto Scaling Dengan Menggunakan CloudTrail	07/16/2014
Blok Kapasitas Amazon EC2	Kapasitas Pencatatan Memblokir panggilan API dengan AWS CloudTrail	10/31/2023
EC2 Image Builder Amazon	Pencatatan panggilan EC2 Image Builder API menggunakan CloudTrail	12/02/2019
Amazon Elastic Block Store (Amazon EBS) API langsung EBS	Logging Panggilan API Menggunakan AWS CloudTrail Log API Panggilan untuk API langsung EBS dengan AWS CloudTrail	Amazon EBS: /2013 11/13 API langsung EBS: /2020 06/30
Amazon Elastic Container Registry (Amazon ECR)	Mencatat Panggilan API ECR Amazon Dengan Menggunakan AWS CloudTrail	12/21/2015

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Elastic Container Service (Amazon ECS)	Pencatatan Panggilan API Amazon ECS Dengan Menggunakan AWS CloudTrail	04/09/2015
Amazon Elastic File System (Amazon EFS)	Mencatat Panggilan API Amazon EFS dengan AWS CloudTrail	06/28/2016
Amazon Elastic Kubernetes Service (Amazon EKS)	Mencatat Panggilan API Amazon EKS dengan AWS CloudTrail	06/05/2018
Amazon ElastiCache	Pencatatan Panggilan ElastiCache API Amazon Menggunakan AWS CloudTrail	09/15/2014
Amazon EMR	Pencatatan Panggilan API EMR Amazon menggunakan AWS CloudTrail	04/04/2014
Amazon EMR di EKS	Logging Amazon EMR pada panggilan EKS API menggunakan AWS CloudTrail	12/09/2020
Amazon EventBridge	Pencatatan panggilan EventBridge API Amazon menggunakan AWS CloudTrail	07/11/2019
Amazon FinSpace	Meminta log AWS CloudTrail	10/18/2022
Amazon Forecast	Mencatat Panggilan API Amazon Forecast dengan AWS CloudTrail	11/28/2018

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Fraud Detector	Mencatat Panggilan API Fraud Detector Amazon dengan AWS CloudTrail	01/09/2020
Amazon FSx for Lustre	Logging Amazon FSx for Lustre API Calls dengan AWS CloudTrail	01/11/2019
Amazon FSx for Windows File Server	Pemantauan dengan AWS CloudTrail	11/28/2018
GameLift Server Amazon	Mencatat Panggilan API GameLift Server Amazon dengan AWS CloudTrail	01/27/2016
GameLift Aliran Amazon	Pencatatan panggilan API Amazon GameLift Streams menggunakan AWS CloudTrai l	03/05/2025
Amazon GuardDuty	Mencatat Panggilan GuardDuty API Amazon dengan AWS CloudTrail	02/12/2018
Amazon Inspector	Mencatat panggilan Amazon Inspector API menggunakan AWS CloudTrail	11/29/2021
Pemindaian Amazon Inspector	Informasi Amazon Inspector Scan di CloudTrail	11/27/2023
Amazon Interactive Video Service	Mencatat Panggilan API Amazon IVS dengan AWS CloudTrail	07/15/2020

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Kendra	Mencatat panggilan API Amazon Kendra dengan AWS CloudTrail dan Mencatat panggilan API Amazon Kendra Intelligent Ranking dengan log AWS CloudTrail	05/11/2020
Amazon Keyspaces (untuk Apache Cassandra)	Mencatat panggilan API Amazon Keyspaces dengan AWS CloudTrail	01/13/2020
Layanan Terkelola Amazon untuk Apache Flink	Logging Managed Service untuk panggilan Apache Flink API dengan AWS CloudTrail	03/22/2019
Amazon Kinesis Data Streams	Mencatat Panggilan API Amazon Kinesis Data Streams Menggunakan AWS CloudTrail	04/25/2014
Amazon Kinesis Video Streams	Mencatat Panggilan API Kinesis Video Streams dengan AWS CloudTrail	05/24/2018
Amazon Lex	Mencatat Panggilan API Amazon Lex dengan CloudTrail	08/15/2017
Amazon Lightsail	Mencatat Panggilan API Lightsail dengan AWS CloudTrail	12/23/2016
Amazon Location Service	Pencatatan dan pemantauan dengan AWS CloudTrail	12/15/2020
Amazon Lookout for Equipment	Memantau Amazon Lookout for Equipment	12/01/2020

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Lookout for Metrics	Melihat aktivitas Amazon Lookout for Metrics API di AWS CloudTrail	12/08/2020
Amazon Machine Learning	Pencatatan Panggilan API Amazon ML Dengan Menggunakan AWS CloudTrail	12/10/2015
Amazon Macie	Log panggilan API Amazon Macie menggunakan AWS CloudTrail	05/13/2020
Amazon Managed Blockchain	Mencatat panggilan API Amazon Managed Blockchain menggunakan AWS CloudTrail Logging Ethereum untuk panggilan API Blockchain Terkelola menggunakan AWS CloudTrail (Pratinjau)	04/01/2019
Amazon Managed Grafana	Mencatat panggilan API Grafana yang Dikelola Amazon menggunakan AWS CloudTrail	12/15/2020
Amazon Managed Service for Prometheus	Logging Amazon Managed Service untuk panggilan API Prometheus menggunakan AWS CloudTrail	12/15/2020
Amazon Managed Streaming untuk Apache Kafka	Pencatatan Panggilan API dengan AWS CloudTrail	12/11/2018

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Managed Workflows for Apache Airflow	Melihat log audit di AWS CloudTrail	11/24/2020
Amazon MemoryDB	Mencatat panggilan API Amazon MemoryDB dengan AWS CloudTrail	08/19/2021
Amazon MQ	Mencatat Panggilan API Amazon MQ Menggunakan AWS CloudTrail	07/19/2018
Amazon Neptune	Pencatatan Panggilan API Amazon Neptunus Menggunakan AWS CloudTrail	05/30/2018
Amazon Satu Perusahaan	Mencatat panggilan API Amazon One Enterprise menggunakan AWS CloudTrail	11/27/2023
OpenSearch Layanan Amazon	Memantau panggilan API OpenSearch Layanan Amazon dengan AWS CloudTrail	10/01/2015
Amazon Personalize	Logging Amazon Personalisasi Panggilan API dengan AWS CloudTrail	11/28/2018
Amazon Pinpoint	Mencatat Panggilan API Amazon Pinpoint dengan AWS CloudTrail	02/06/2018
API SMS dan Suara Amazon Pinpoint	Mencatat Panggilan API Amazon Pinpoint dengan AWS CloudTrail	11/16/2018

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Polly	Mencatat Panggilan API Amazon Polly dengan AWS CloudTrail	11/30/2016
Amazon Q Bisnis	Mencatat panggilan Amazon Q Business API menggunakan AWS CloudTrail	11/28/2023
Amazon Q Developer	Pencatatan panggilan API Pengembang Amazon Q menggunakan AWS CloudTrai l	11/28/2023
Amazon Quantum Ledger Database (Amazon QLDB)	Mencatat Panggilan API QLDB Amazon dengan AWS CloudTrail	09/10/2019
Amazon Quick	Operasi Logging dengan CloudTrail	04/28/2017
Amazon Relational Database Service (Amazon RDS)	Pencatatan Panggilan API Amazon RDS Menggunakan AWS CloudTrail	11/13/2013
Wawasan Performa Amazon RDS	Pencatatan Panggilan API Amazon RDS Menggunakan AWS CloudTrail Amazon RDS Performance Insights API adalah bagian dari Amazon RDS API.	06/21/2018
Amazon Redshift	Mencatat Panggilan API Amazon Redshift dengan AWS CloudTrail	06/10/2014

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Rekognition	Pencatatan Panggilan API Rekognition Amazon Menggunakan AWS CloudTrail	04/6/2018
Amazon Route 53	Menggunakan AWS CloudTrail untuk Menangkap Permintaan yang Dikirim ke API Route 53	02/11/2015
Pengontrol Pemulihan Aplikasi Amazon (ARC)	Mencatat panggilan API Amazon Application Recovery Controller (ARC) menggunakan AWS CloudTrail	07/27/2021
Amazon S3	Mencatat Panggilan API Amazon S3 Dengan Menggunakan AWS CloudTrail	Acara manajemen: 09/01 /2015 Data peristiwa: 11/21 /2016
Amazon Glacier	Mencatat Panggilan API Amazon Glacier Dengan Menggunakan AWS CloudTrail	12/11/2014
Amazon SageMaker AI	Mencatat Panggilan API SageMaker AI Amazon dengan AWS CloudTrail	01/11/2018
Amazon Security Lake	Mencatat panggilan Amazon Security Lake API menggunakan CloudTrail	05/30/2023
AWS Agen Keamanan	Pencatatan panggilan API Agen AWS Keamanan menggunakan CloudTrail	03/18/2025

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Simple Email Service (Amazon SES)	Pencatatan Panggilan API Amazon SES Dengan Menggunakan AWS CloudTrail	05/07/2015
Amazon Simple Notification Service (Amazon SNS)	Pencatatan Panggilan API Amazon SNS menggunakan AWS CloudTrail	10/09/2014
Amazon Simple Queue Service (Amazon SQS)	Mencatat Tindakan Amazon SQS API Menggunakan AWS CloudTrail	07/16/2014
Amazon Simple Workflow Service (Amazon SWF)	Merekam panggilan API dengan AWS CloudTrail	Acara manajemen: 05/13 /2014 Data peristiwa: 02/14 /2024
Amazon Textract	Mencatat Panggilan API Amazon Texttract dengan AWS CloudTrail	05/29/2019
Amazon Timestream	Mencatat panggilan API Timestream dengan AWS CloudTrail	09/30/2020
Amazon Transcribe	Mencatat Panggilan API Amazon Transcribe dengan AWS CloudTrail	06/28/2018
Amazon Translate	Logging Amazon Translate API Calls dengan AWS CloudTrail	04/04/2018

AWS Layanan	CloudTrail Topik	Support dimulai
Izin Terverifikasi Amazon	Mencatat panggilan API Izin Terverifikasi Amazon menggunakan AWS CloudTrail	06/13/2023
Amazon Virtual Private Cloud (Amazon VPC)	Logging Panggilan API Menggunakan AWS CloudTrail Amazon VPC API adalah bagian dari Amazon EC2 API.	11/13/2013
Kisi VPC Amazon	CloudTrail log	03/31/2023
PENGANALISIS REACHABILITY VPC Amazon	Logging Reachability Analyzer API panggilan menggunakan AWS CloudTrail	11/27/2023
Amazon WorkDocs	Mencatat Panggilan WorkDocs API Amazon Dengan Menggunakan AWS CloudTrail	08/27/2014
Amazon WorkMail	Pencatatan Panggilan WorkMail API Amazon Menggunakan AWS CloudTrail	12/12/2017
Amazon WorkSpaces	Mencatat Panggilan WorkSpaces API Amazon dengan Menggunakan CloudTrail	04/09/2015
Klien WorkSpaces Tipis Amazon	Mencatat panggilan Amazon WorkSpaces Thin Client API menggunakan AWS CloudTrail	11/26/2023

AWS Layanan	CloudTrail Topik	Support dimulai
WorkSpaces Web Amazon	Pencatatan panggilan Amazon WorkSpaces Web API menggunakan AWS CloudTrail	11/30/2021
Penskalaan Otomatis Aplikasi	Logging Application Auto Scaling API panggilan dengan AWS CloudTrail	10/31/2016
AWS Account Management	Logging panggilan AWS Account Management API menggunakan AWS CloudTrail	10/01/2021
AWS Amplify	Logging panggilan Amplify API menggunakan AWS CloudTrail	11/30/2020
AWS App Mesh	Mencatat Panggilan API App Mesh dengan AWS CloudTrail	AWS App Mesh 10/30/2019 Layanan Manajemen Utusan App Mesh /2022 03/18
AWS App Runner	Logging App Runner API panggilan dengan AWS CloudTrail	05/18/2021
AWS AppConfig	Logging panggilan AWS AppConfig API menggunakan AWS CloudTrail	Acara manajemen: 07/31 /2020 Data peristiwa: 01/04 /2024
AWS AppFabric	Pencatatan panggilan AWS AppFabric API menggunakan AWS CloudTrail	06/27/2023

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Application Discovery Service	Logging Application Discovery Service API Calls dengan AWS CloudTrail	05/12/2016
AWS Layanan Transformasi Aplikasi	(Layanan backend yang digunakan oleh AWS alat, seperti AWS Microservice Extractor untuk.NET)	08/26/2023
AWS AppSync	Pencatatan Panggilan AWS AppSync API dengan AWS CloudTrail	02/13/2018
AWS Artifact	Logging panggilan AWS Artifact API dengan AWS CloudTrail	01/27/2023
AWS Audit Manager	Pencatatan panggilan AWS Audit Manager API dengan AWS CloudTrail	12/07/2020
AWS Auto Scaling	Pencatatan Panggilan AWS Auto Scaling API Dengan Menggunakan CloudTrail	08/15/2018
AWS Pertukaran Data B2B	Pencatatan AWS panggilan API Pertukaran Data B2B menggunakan AWS CloudTrail	12/01/2023
AWS Backup	Pencatatan Panggilan AWS Backup API dengan AWS CloudTrail	02/04/2019
AWS Batch	Pencatatan Panggilan AWS Batch API dengan AWS CloudTrail	1/10/2018

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Manajemen Penagihan dan Biaya	Pencatatan Panggilan AWS Manajemen Penagihan dan Biaya API dengan AWS CloudTrail	06/07/2018
AWS Billing Conductor	Logging panggilan AWS Billing Conductor API menggunakan AWS CloudTrail	03/12/2024
AWS BugBust	Logging panggilan BugBust API menggunakan CloudTrail	06/24/2021
AWS Certificate Manager	Menggunakan AWS CloudTrail	03/25/2016
AWS Clean Rooms	Logging panggilan AWS Clean Rooms API menggunakan AWS CloudTrail	03/21/2023
AWS Cloud Map	Pencatatan Panggilan AWS Cloud Map API dengan AWS CloudTrail	11/28/2018
AWS Cloud9	Pencatatan Panggilan AWS Cloud9 API dengan AWS CloudTrail	01/21/2019
AWS CloudFormation	Pencatatan Panggilan AWS CloudFormation API di AWS CloudTrail	04/02/2014
AWS CloudHSM	Pencatatan Panggilan AWS CloudHSM API Dengan Menggunakan AWS CloudTrail	01/08/2015

AWS Layanan	CloudTrail Topik	Support dimulai
AWS CloudShell	Penebangan dan pemantauan di AWS CloudShell	12/15/2020
AWS CloudTrail	AWS CloudTrail Referensi CloudTrail API (Semua panggilan API dicatat oleh CloudTrail.)	11/13/2013
AWS CodeArtifact	Logging panggilan CodeArtifact API dengan AWS CloudTrail	06/10/2020
AWS CodeBuild	Pencatatan Panggilan AWS CodeBuild API dengan AWS CloudTrail	12/01/2016
AWS CodeCommit	Pencatatan Panggilan AWS CodeCommit API dengan AWS CloudTrail	01/11/2017
AWS CodeDeploy	Memantau Deployment dengan AWS CloudTrail	12/16/2014
AWS CodePipeline	Logging panggilan CodePipeline API dengan AWS CloudTrail	07/09/2015
AWS CodeStar	Pencatatan Panggilan AWS CodeStar API dengan AWS CloudTrail	06/14/2017
AWS CodeStar Pemberitahuan	Logging AWS CodeStar Notifications API Panggilan dengan AWS CloudTrail	11/05/2019
AWS Config	Logging AWS Config API Calls By dengan AWS CloudTrail	02/10/2015

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Katalog Kontrol	Logging AWS Control Catalog API panggilan menggunakan AWS CloudTrail	04/08/2024
AWS Control Tower	AWS Control Tower Tindakan Pencatatan dengan AWS CloudTrail	08/12/2019
AWS Data Pipeline	Pencatatan Panggilan AWS Data Pipeline API dengan menggunakan AWS CloudTrail	12/02/2014
AWS Database Migration Service (AWS DMS)	Pencatatan Panggilan AWS Database Migration Service API Menggunakan AWS CloudTrail	02/04/2016
AWS DataSync	Pencatatan Panggilan AWS DataSync API dengan AWS CloudTrail	11/26/2018
AWS Deadline Cloud	Logging panggilan Deadline Cloud API menggunakan AWS CloudTrail	04/02/2024
AWS Device Farm	Pencatatan Panggilan AWS Device Farm API Dengan Menggunakan AWS CloudTrail	07/13/2015
Direct Connect	Pencatatan Panggilan Direct Connect API di AWS CloudTrail	03/08/2014

AWS Layanan	CloudTrail Topik	Support dimulai
Directory Service	Pencatatan Panggilan Directory Service API dengan Menggunakan CloudTrail	05/14/2015
Directory Service Data	Pencatatan panggilan API Directory Service Data menggunakan AWS CloudTrail	09/18/2024
AWS Elastic Beanstalk (Elastic Beanstalk)	Menggunakan Panggilan API Elastic Beanstalk dengan AWS CloudTrail	03/31/2014
AWS Elastic Disaster Recovery	Logging panggilan AWS Elastic Disaster Recovery API menggunakan AWS CloudTrail	11/17/2021
AWS Elemental MediaConnect	Pencatatan Panggilan AWS Elemental MediaConnect API dengan AWS CloudTrail	11/27/2018
AWS Elemental MediaConvert	Pencatatan Panggilan AWS Elemental MediaConvert API dengan CloudTrail	11/27/2017
AWS Elemental MediaLive	Pencatatan Panggilan MediaLive API dengan AWS CloudTrail	01/19/2019
AWS Elemental MediaPackage	Pencatatan Panggilan AWS Elemental MediaPackage API dengan AWS CloudTrail	12/21/2018
AWS Elemental MediaTailor	Pencatatan Panggilan AWS Elemental MediaTailor API dengan AWS CloudTrail	02/11/2019

AWS Layanan	CloudTrail Topik	Support dimulai
AWS SMS Pesan Pengguna Akhir	Pencatatan panggilan API SMS Pesan Pengguna AWS Akhir menggunakan AWS CloudTrail	10/10/2024
AWS Pesan Pengguna Akhir Sosial	Logging AWS End User Messaging Panggilan API Sosial menggunakan AWS CloudTrail	10/10/2024
AWS Resolusi Entitas	Logging AWS Entity Resolution API panggilan menggunakan A AWS CloudTrail	07/26/2023
AWS Fault Injection Service	Log panggilan API dengan AWS CloudTrail	03/15/2021
AWS Firewall Manager	Pencatatan Panggilan AWS Firewall Manager API dengan AWS CloudTrail	04/05/2018
AWS Global Accelerator	Mencatat Panggilan API Akselerator AWS Global dengan AWS CloudTrail	11/26/2018
AWS Glue	AWS Glue Operasi Logging Menggunakan AWS CloudTrail	11/07/2017
AWS Ground Station	Pencatatan Panggilan AWS Ground Station API dengan AWS CloudTrail	05/31/2019
AWS Health	Pencatatan Panggilan AWS Health API dengan AWS CloudTrail	11/21/2016

AWS Layanan	CloudTrail Topik	Support dimulai
Dasbor AWS Health	Pencatatan Panggilan AWS Health API dengan AWS CloudTrail	12/01/2016
AWS HealthImaging	Pencatatan panggilan AWS HealthImaging API menggunakan AWS CloudTrail	07/26/2023
AWS HealthLake	Pencatatan panggilan AWS HealthLake API dengan AWS CloudTrail	12/07/2020
AWS HealthOmics	Pencatatan panggilan AWS HealthOmics API menggunakan AWS CloudTrail	11/29/2022
AWS IAM Identity Center	Mencatat Panggilan API Pusat Identitas IAM dengan AWS CloudTrail	12/07/2017
AWS IAM Identity Center — SCIM	Mencatat Panggilan API Pusat Identitas IAM dengan AWS CloudTrail	10/28/2024
AWS Identity and Access Management (IAM)	Pencatatan Acara IAM dengan AWS CloudTrail	11/13/2013
AWS IoT	Pencatatan Panggilan AWS IoT API dengan AWS CloudTrail	04/11/2016
AWS IoT Greengrass	Pencatatan Panggilan AWS IoT Greengrass API dengan AWS CloudTrail	10/29/2018

AWS Layanan	CloudTrail Topik	Support dimulai
AWS IoT Greengrass V2	Log panggilan API AWS IoT Greengrass V2 dengan AWS CloudTrail	12/14/2020
AWS IoT SiteWise	Pencatatan panggilan AWS IoT SiteWise API dengan AWS CloudTrail	04/29/2020
AWS Key Management Service (AWS KMS)	Pencatatan Panggilan AWS KMS API menggunakan AWS CloudTrail	11/12/2014
AWS Lake Formation	Pencatatan Panggilan AWS Lake Formation API Menggunakan AWS CloudTrail	08/09/2019
AWS Lambda	Pencatatan Panggilan AWS Lambda API Dengan Menggunakan AWS CloudTrail	Acara manajemen: 04/09 /2015 Data peristiwa: 11/30 /2017
AWS Launch Wizard	Logging panggilan AWS Launch Wizard API menggunakan AWS CloudTrail	11/08/2023
AWS License Manager	Logging AWS License Manager API Calls dengan AWS CloudTrail	03/01/2019
AWS Mainframe Modernization	Logging panggilan AWS Mainframe Modernization API menggunakan AWS CloudTrail	06/08/2022

AWS Layanan	CloudTrail Topik	Support dimulai
Integrasi terkelola untuk AWS IoT Device Management	Logging Integrasi terkelola panggilan API menggunakan AWS CloudTrail	03/03/2025
AWS Managed Services	Manajemen log di AMS Accelerate	12/21/2016
AWS Marketplace Perjanjian	Perjanjian Pencatatan Panggilan API menggunakan AWS CloudTrail	09/01/2023
AWS Marketplace Layanan Penyebaran	Panggilan Layanan AWS Marketplace Penyebaran Pencatatan dengan CloudTrail	11/29/2023
AWS Marketplace Penemuan	Pencatatan panggilan API AWS Marketplace Discovery menggunakan AWS CloudTrail	12/15/2022
AWS Marketplace Layanan Metering	Pencatatan Panggilan AWS Marketplace API dengan AWS CloudTrail	08/22/2018
AWS Migration Hub	Mencatat Panggilan API AWS Migration Hub dengan AWS CloudTrail	08/14/2017
AWS Migration Hub Perjalanan	Logging panggilan API AWS Migration Hub Journeys dengan AWS CloudTrail	12/03/2024
Multi-party persetujuan	Logging panggilan API Multi-party persetujuan menggunakan AWS CloudTrail	06/17/2025

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Network Firewall	Mencatat panggilan ke AWS Network Firewall API dengan AWS CloudTrail	11/17/2020
AWS OpsWorks for Chef Automate	Pencatatan Panggilan AWS OpsWorks for Chef Automate API dengan AWS CloudTrail	07/16/2018
AWS OpsWorks for Puppet Enterprise	Logging OpsWorks untuk Panggilan API Perusahaa n Boneka dengan AWS CloudTrail	07/16/2018
AWS OpsWorks Stacks	Pencatatan Panggilan AWS OpsWorks Stacks API dengan AWS CloudTrail	06/04/2014
Database Oracle@AWS	Logging Oracle Database@ AWS Panggilan API dengan AWS CloudTrail	12/01/2024
AWS Organizations	Pencatatan panggilan AWS Organizations API dengan AWS CloudTrail	02/27/2017
AWS Outposts	Pencatatan panggilan AWS Outposts API dengan AWS CloudTrail	02/04/2020
AWS Payment Cryptography	Logging panggilan AWS Payment Cryptography API menggunakan AWS CloudTrai l	06/08/2023
AWS 5G pribadi	Mencatat panggilan API 5G AWS Pribadi menggunakan AWS CloudTrail	08/11/2022

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Private Certificate Authority (AWS Private CA)	Menggunakan CloudTrail	04/04/2018
AWS Proton	Penebangan dan pemantauan di AWS Proton	06/09/2021
AWS re:Post Pribadi	Pencatatan panggilan API AWS re:Post Pribadi menggunakan AWS CloudTrail	11/26/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	Pencatatan Panggilan AWS RAM API dengan AWS CloudTrail	11/20/2018
Penjelajah Sumber Daya AWS	Logging panggilan Penjelajah Sumber Daya AWS API menggunakan AWS CloudTrail	11/07/2022
AWS Resource Groups	Pencatatan dan pemantauan di Resource Groups	06/29/2018
AWS RoboMaker	Pencatatan Panggilan AWS RoboMaker API dengan AWS CloudTrail	01/16/2019
AWS Secrets Manager	Pantau Penggunaan AWS Secrets Manager Rahasia Anda	04/05/2018
AWS Security Hub CSPM	Pencatatan Panggilan AWS Security Hub CSPM API dengan AWS CloudTrail	11/27/2018

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Respon Insiden Keamanan	Pencatatan panggilan API Respons Insiden AWS Keamanan menggunakan AWS CloudTrail	12/01/2024
AWS Security Token Service (AWS STS)	Pencatatan Acara IAM dengan AWS CloudTrail Topik IAM mencakup informasi untuk AWS STS.	11/13/2013
AWS Serverless Application Repository	Pencatatan Panggilan AWS Serverless Application Repository API dengan AWS CloudTrail	02/20/2018
AWS Service Catalog	Logging Service Catalog API Calls dengan AWS CloudTrail	07/06/2016
AWS Shield	Logging Shield Panggilan API Tingkat Lanjut dengan AWS CloudTrail	02/08/2018
AWS Snowball Edge Tepi	Logging AWS Snowball Edge Edge API Panggilan dengan AWS CloudTrail	01/25/2019
AWS Step Functions	Pencatatan Panggilan AWS Step Functions API dengan AWS CloudTrail	12/01/2016
AWS Storage Gateway	Mencatat Panggilan API Storage Gateway dengan Menggunakan AWS CloudTrail	12/16/2014

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Dukungan	Pencatatan panggilan AWS Dukungan API dengan AWS CloudTrail	04/21/2016
Dukungan Rekomendasi (Pratinjau)	Panggilan API Dukungan Rekomendasi Pencatatan dengan AWS CloudTrail	05/22/2024
AWS Systems Manager	Pencatatan Panggilan AWS Systems Manager API dengan AWS CloudTrail	11/29/2017
AWS Systems Manager Manajer Insiden	Panggilan API Manajer AWS Systems Manager Insiden Pencatatan menggunakan AWS CloudTrail	05/10/2021
AWS Pembangun Jaringan Telco (AWS TNB)	AWS Pencatatan panggilan API Pembuat Jaringan Telco menggunakan AWS CloudTrail	02/21/2023
AWS Transfer for SFTP	Pencatatan Panggilan AWS Transfer for SFTP API dengan AWS CloudTrail	01/08/2019
AWS Transit Gateway	Logging API Panggilan untuk Transit Gateway Anda Menggunakan AWS CloudTrail	11/26/2018
AWS Trusted Advisor	Mencatat tindakan AWS Trusted Advisor konsol dengan AWS CloudTrail	10/22/2020

AWS Layanan	CloudTrail Topik	Support dimulai
Akses Terverifikasi AWS	Log panggilan Akses Terverifikasi AWS API menggunakan AWS CloudTrail	04/27/2023
AWS WAF	Pencatatan Panggilan AWS WAF API dengan AWS CloudTrail	04/28/2016
AWS Well-Architected Tool	Pencatatan Panggilan AWS Well-Architected Tool API dengan AWS CloudTrail	12/15/2020
AWS X-Ray	Logging AWS X-Ray API Panggilan Dengan CloudTrail	04/25/2018
Elastic Load Balancing	AWS CloudTrail Logging untuk Classic Load Balancer dan AWS CloudTrail Logging untuk Application Load Balancer	04/04/2014
Pembaruan FreeRTOS (Over-the-Air OTA)	Mencatat Panggilan API AWS IoT OTA dengan AWS CloudTrail	05/22/2019
Service Quotas	Logging Service Quotas API call menggunakan AWS CloudTrail	06/24/2019

CloudTrail layanan yang tidak didukung

Layanan yang masih dalam pratinjau, atau belum dirilis untuk ketersediaan umum (GA), atau yang tidak memiliki API publik, tidak dianggap didukung.

Selain itu, AWS layanan dan acara berikut tidak didukung:

- AWS Import/Export

Untuk daftar AWS layanan yang didukung, lihatAWS topik layanan untuk CloudTrail.

Kuota di AWS CloudTrail

Bagian ini menjelaskan kuota sumber daya (sebelumnya disebut sebagai batas) di. CloudTrail Untuk informasi tentang semua kuota di CloudTrail, lihat Kuota layanan di. Referensi Umum AWS

> **Note**
>
> CloudTrail tidak memiliki kuota yang dapat disesuaikan.

CloudTrail kuota sumber daya

Tabel berikut menjelaskan kuota sumber daya di dalamnya CloudTrail.

Sumber daya	Kuota bawaan	Komentar
Jalur per Wilayah	5	Jumlah maksimum jalur per. Wilayah AWS Di Wilayah bayangan, untuk mendapatkan metrik jumlah sumber daya terbaru, hubungi `ListTrails` API. Kuota ini tidak dapat dinaikkan jumlahnya.
Menyimpan data acara	10	Jumlah maksimum penyimpan an data acara per Wilayah AWS. Ini termasuk penyimpan an data peristiwa wilayah tunggal untuk Wilayah, penyimpanan data acara Multi-wilayah di semua Wilayah AWS, dan penyimpan an data acara organisasi. Ini

Sumber daya	Kuota bawaan	Komentar
		termasuk penyimpanan data acara di setiap tahap siklus hidup. Di Wilayah bayangan, untuk mendapatkan metrik jumlah sumber daya terbaru, hubungi `ListEventDataStores` API. Kuota ini tidak dapat dinaikkan jumlahnya.
Saluran	25	Kuota ini berlaku untuk saluran yang digunakan untuk integrasi CloudTrail Lake dengan sumber acara di luar AWS, dan tidak berlaku untuk saluran terkait layanan. Kuota ini tidak dapat dinaikkan jumlahnya.
Dasbor per Wilayah	100	Jumlah maksimum dasbor khusus CloudTrail Danau per Wilayah AWS. Di Wilayah bayangan, untuk mendapatkan metrik jumlah sumber daya terbaru, hubungi `ListDashboards` API. Kuota ini tidak dapat dinaikkan jumlahnya.

Sumber daya	Kuota bawaan	Komentar
Widget per dasbor	10	Jumlah maksimum widget per dasbor CloudTrail Danau ini. Kuota ini tidak dapat dinaikkan jumlahnya.
Penyegaran dasbor bersamaan	1	Jumlah maksimum refresh yang sedang berlangsung per dasbor. Kuota ini tidak dapat dinaikkan jumlahnya.
Kueri bersamaan	10	Jumlah maksimum kueri antrian atau berjalan yang dapat Anda jalankan secara bersamaan di Lake. CloudTrail Kuota ini tidak dapat dinaikkan jumlahnya.
Acara per PutAuditEvents permintaan	100	Anda dapat menambahk an hingga 100 acara aktivitas (atau hingga 1 MB) per `PutAuditEvents` permintaan. Kuota ini tidak dapat dinaikkan jumlahnya.
Pemilih peristiwa	5 per jejak	Kuota ini tidak dapat dinaikkan jumlahnya.

Sumber daya	Kuota bawaan	Komentar
Penyeleksi acara tingkat lanjut	500 kondisi di semua pemilih acara tingkat lanjut	Jika penyimpanan data jejak atau peristiwa menggunak an pemilih acara lanjutan, maksimum 500 nilai total untuk semua kondisi di semua pemilih acara lanjutan diperbolehkan. Kuota ini tidak dapat dinaikkan jumlahnya.

Sumber daya	Kuota bawaan	Komentar
Sumber daya data dalam pemilih acara	250 di semua penyeleksi acara dalam satu jejak	Jika Anda memilih untuk membatasi peristiwa data dengan menggunakan penyeleksi peristiwa, jumlah total sumber daya data tidak dapat melebihi 250 di semua pemilih acara dalam satu jejak. Batas jumlah sumber daya pada pemilih acara individu dapat dikonfigurasi hingga 250. Batas atas ini hanya diperbolehkan jika jumlah total sumber daya data tidak melebihi 250 di semua pemilih acara. Contoh: • Jejak dengan 5 pemilih acara, masing-masing dikonfigurasi dengan 50 sumber daya data, diperbolehkan. (5* 50 = 250) • Jejak dengan 5 pemilih acara, 3 di antaranya dikonfigurasi dengan 50 sumber daya data, 1 di antaranya dikonfigurasi dengan 99 sumber daya data, dan 1 di antaranya dikonfigurasi dengan 1 sumber daya data, juga diperbolehkan. ((3* 50) +1+99 = 250)

Sumber daya	Kuota bawaan	Komentar
		• Jejak yang dikonfigurasi dengan 5 pemilih acara, yang semuanya dikonfigu rasi dengan 100 sumber daya data, tidak diperbole hkan. (5* 100 = 500) Penyeleksi acara hanya berlaku untuk jalur. Untuk penyimpanan data acara, Anda harus menggunakan pemilih acara lanjutan. Kuota ini tidak dapat dinaikkan jumlahnya. Kuota tidak berlaku jika Anda memilih untuk mencatat peristiwa data pada semua sumber daya, seperti semua bucket S3 atau semua fungsi Lambda.

Sumber daya	Kuota bawaan	Komentar
Ukuran peristiwa	Semua versi acara: peristiwa di atas 256 KB tidak dapat dikirim ke CloudWatch Log Event versi 1.05 dan yang lebih baru: total batas ukuran acara 256 KB	Amazon CloudWatch Logs dan Amazon EventBridge masing-masing memungkin kan ukuran acara maksimum 256 KB. CloudTrail tidak mengirim acara lebih dari 256 KB ke CloudWatch Log atau EventBridge. Dimulai dengan acara versi 1.05, acara memiliki ukuran maksimum 256 KB. Ini untuk membantu mencegah eksploitasi oleh pelaku jahat, dan memungkinkan acara dikonsumsi oleh AWS layanan lain, seperti CloudWatch Log dan EventBridge.
CloudTrail ukuran file dikirim ke Amazon S3	50 MB sebelum kompresi	Untuk peristiwa manajemen , data, dan aktivitas jaringan, CloudTrail kirimkan peristiwa ke S3 dalam file gzip terkompresi. Ukuran file maksimum sebelum kompresi adalah 50 MB. Jika diaktifkan di jalur, pemberitahuan pengiriman log dikirim oleh Amazon SNS setelah CloudTrail mengirim file gzip ke S3.

Kuota transaksi per detik (TPS) dalam CloudTrail

Referensi Umum AWSDaftar kuota transaksi per detik (TPS) untuk. AWS APIs Kuota transaksi per detik (TPS) untuk API menunjukkan berapa banyak permintaan yang dapat Anda buat per detik untuk API tertentu tanpa dibatasi. Misalnya, kuota TPS untuk CloudTrail `LookupEvents` API adalah 2.

Untuk informasi tentang kuota TPS untuk setiap CloudTrail API, lihat Kuota layanan di. Referensi Umum AWS

Memulai dengan AWS CloudTrail tutorial

Jika Anda baru mengenal AWS CloudTrail, tutorial ini dapat membantu Anda mempelajari cara menggunakan fitur-fiturnya. Untuk menggunakan CloudTrail fitur, Anda harus memiliki izin yang memadai. Halaman ini menjelaskan kebijakan terkelola yang tersedia untuk CloudTrail dan memberikan informasi tentang cara Anda dapat memberikan izin.

Contoh:

- Berikan izin untuk digunakan CloudTrail
- Lihat riwayat acara
- Buat jejak untuk mencatat peristiwa manajemen
- Membuat penyimpanan data peristiwa untuk peristiwa data S3

Berikan izin untuk digunakan CloudTrail

Untuk membuat, memperbarui, dan mengelola CloudTrail sumber daya seperti jalur, penyimpanan data acara, dan saluran, Anda perlu memberikan izin untuk digunakan CloudTrail. Bagian ini memberikan informasi tentang kebijakan terkelola yang tersedia untuk CloudTrail.

> **Note**
>
> Izin yang Anda berikan kepada pengguna untuk melakukan tugas CloudTrail administrasi tidak sama dengan izin yang diperlukan CloudTrail untuk mengirimkan file log ke bucket Amazon S3 atau mengirim pemberitahuan ke topik Amazon SNS. Untuk informasi selengkapnya tentang izin tersebut, lihatKebijakan bucket Amazon S3 untuk CloudTrail. Jika Anda mengonfigurasi integrasi dengan Amazon CloudWatch Logs, CloudTrail juga memerlukan peran yang dapat diasumsikan untuk mengirimkan peristiwa ke grup CloudWatch log Amazon Logs. Anda harus membuat peran yang CloudTrail menggunakan. Untuk informasi selengkapnya, lihat Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol dan Mengirim acara ke CloudWatch Log.

Kebijakan ter AWS kelola berikut tersedia untuk CloudTrail:

- AWSCloudTrail_FullAccessKebijakan ini menyediakan akses penuh ke CloudTrail tindakan pada CloudTrail sumber daya, seperti jalur, penyimpanan data acara, dan saluran. Kebijakan ini memberikan izin yang diperlukan untuk membuat, memperbarui, dan menghapus CloudTrail jejak, penyimpanan data peristiwa, dan saluran.

  Kebijakan ini juga memberikan izin untuk mengelola bucket Amazon S3, grup CloudWatch log untuk Log, dan topik Amazon SNS untuk jejak. Namun, kebijakan `AWSCloudTrail_FullAccess` terkelola tidak memberikan izin untuk menghapus bucket Amazon S3, grup CloudWatch log untuk Log, atau topik Amazon SNS. Untuk informasi tentang kebijakan terkelola untuk AWS layanan lain, lihat Panduan Refer AWS ensi Kebijakan Terkelola .

  > **Note**
  >
  > AWSCloudTrail_FullAccessKebijakan ini tidak dimaksudkan untuk dibagikan secara luas di seluruh Anda Akun AWS. Pengguna dengan peran ini dapat mematikan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di dalamnya. Akun AWS Untuk alasan ini, Anda hanya harus menerapkan kebijakan ini kepada administrator akun. Anda harus mengontrol dan memantau penggunaan kebijakan ini secara ketat.

- AWSCloudTrail_ReadOnlyAccessKebijakan ini memberikan izin untuk melihat CloudTrail konsol, termasuk peristiwa terbaru dan riwayat acara. Kebijakan ini juga memungkinkan Anda untuk melihat jalur yang ada, penyimpanan data acara, dan saluran. Peran dan pengguna dengan kebijakan ini dapat mengunduh riwayat acara, tetapi mereka tidak dapat membuat atau memperbarui jejak, penyimpanan data acara, atau saluran.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:

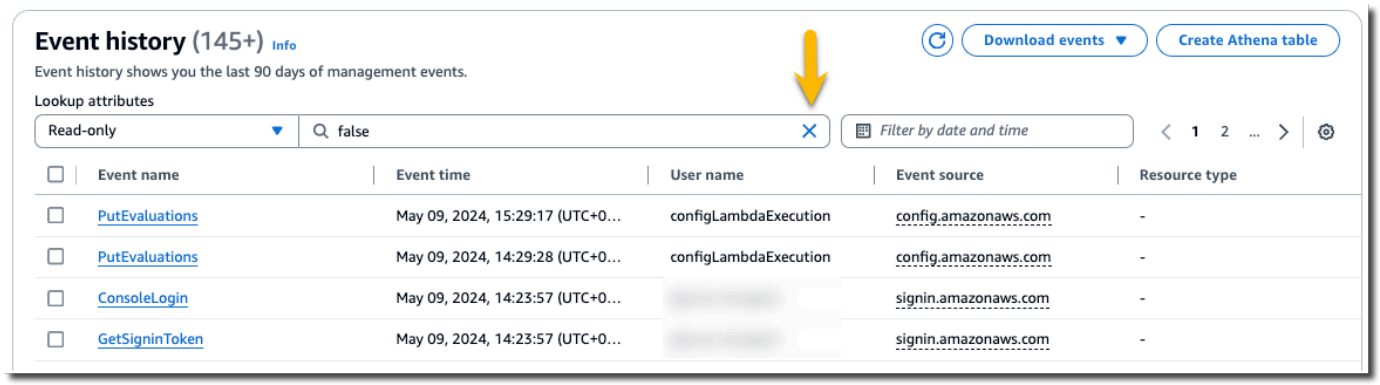
- Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Lihat riwayat acara

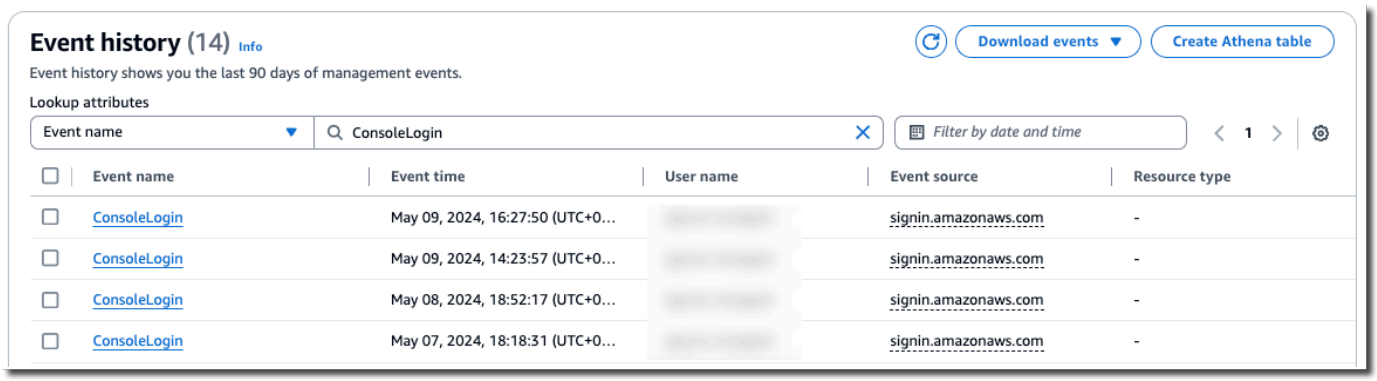
Bagian ini menjelaskan cara menggunakan halaman riwayat CloudTrail acara di CloudTrail konsol untuk melihat 90 hari terakhir acara manajemen Akun AWS untuk Anda saat ini Wilayah AWS.

Untuk melihat Sejarah acara

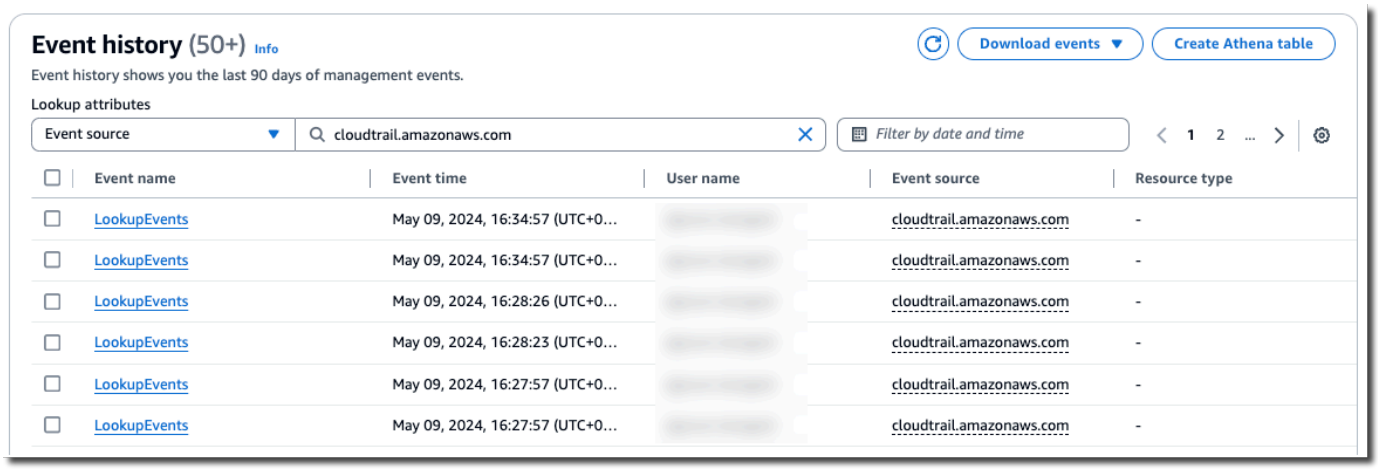
1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa. Anda melihat daftar acara yang difilter, dengan acara terbaru ditampilkan terlebih dahulu. Filter default untuk acara adalah Baca saja, disetel ke false. Anda dapat menghapus filter itu dengan memilih X di sebelah kanan filter. Anda dapat mencari acara di riwayat acara dengan memfilter peristiwa pada atribut tunggal



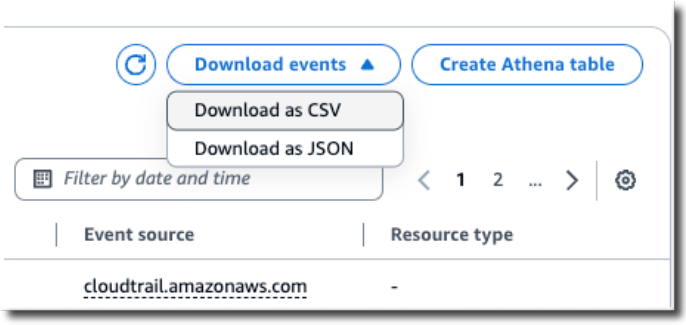
3. Pilih atribut untuk difilter dan masukkan nilai penuh untuk atribut tersebut. CloudTrail tidak dapat memfilter pada nilai parsional. Misalnya, untuk melihat semua acara login konsol, pilih filter nama acara, dan tent ConsoleLogin ukan nilai atribut.



Atau, untuk melihat peristiwa CloudTrail manajemen terbaru, pilih Sumber peristiwa, dan tentukan`cloudtrail.amazonaws.com`. Untuk informasi tentang peristiwa yang dicatat oleh layanan CloudTrail, lihat Referensi API layanan.



4. Untuk melihat acara manajemen tertentu, pilih nama acara. Pada halaman detail acara, Anda dapat melihat detail tentang acara, melihat sumber yang direferensikan, dan melihat catatan acara.
5. Untuk membandingkan acara, pilih hingga lima peristiwa dengan mengisi kotak centangnya di margin kiri tabel riwayat acara. Anda dapat melihat detail untuk acara yang dipilih secara berdampingan di tabel Per bandingan detail acara.
6. Anda dapat menyimpan riwayat acara dengan mengunduhnya sebagai file dalam format CSV atau JSON. Mengunduh riwayat acara Anda dapat memakan waktu beberapa menit.



Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.

Buat jejak untuk mencatat peristiwa manajemen

Untuk jejak pertama Anda, sebaiknya buat jejak yang mencatat semua peristiwa manajemen dan tidak mencatat peristiwa data atau peristiwa Wawasan apa pun. Contoh peristiwa manajemen termasuk peristiwa keamanan seperti IAM `CreateUser` dan `AttachRolePolicy` peristiwa, peristiwa sumber daya seperti `RunInstances` dan`CreateBucket`, dan banyak lagi. Anda akan membuat bucket Amazon S3 tempat Anda akan menyimpan file log untuk jejak sebagai bagian dari pembuatan jejak di CloudTrail konsol.

> **Note**
>
> AWS Control Tower menyiapkan peristiwa manajemen pen CloudTrail catatan jejak baru saat Anda mengatur zona pendaratan. Ini adalah jejak tingkat organisasi, yang berarti mencatat semua peristiwa manajemen untuk akun manajemen dan semua akun anggota dalam organisasi. Untuk informasi selengkapnya, lihat Tentang masuk AWS Control Tower di Panduan AWS CloudTrail Pengguna.
> Tutorial ini mengasumsikan Anda membuat jejak pertama Anda. Bergantung pada jumlah jalur yang Anda miliki di AWS akun Anda, dan bagaimana jalur tersebut dikonfigurasi, prosedur berikut mungkin atau mungkin tidak menimbulkan biaya. CloudTrail menyimpan file log dalam bucket Amazon S3, yang menimbulkan biaya. Untuk informasi selengkapnya tentang harga, lihat AWS CloudTrail Harga dan Harga Amazon S3.

Untuk membuat jejak

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.

2. Di pem ilih Wil ayah, pilih Wil AWS ayah tempat Anda ingin jejak Anda dibuat. Ini adalah wilayah asal untuk jalan setapak.

   > **Note**
   >
   > Wilayah rumah adalah satu-satunya Wilayah AWS tempat Anda dapat memperbarui jejak setelah dibuat.

3. Pada halaman CloudTrail beranda layanan, halaman Jalur, atau bagian Jalur pada halaman Dasbor, pilih Buat jejak.
4. Dalam nama Trail, beri nama jejak Anda, seperti*`management-events`*. Sebagai praktik terbaik, gunakan nama yang dengan cepat mengidentifikasi tujuan jejak. Dalam hal ini, Anda membuat jejak yang mencatat peristiwa manajemen.
5. Tinggalkan setelan default untuk Aktifkan untuk semua akun di organisasi saya. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi di Organisasi.
6. Untuk Lokasi penyimpanan, pilih Buat bucket S3 baru untuk membuat bucket. Saat Anda membuat bucket, buat CloudTrail dan terapkan kebijakan bucket yang diperlukan. Jika Anda memilih untuk membuat bucket S3 baru, kebijakan IAM Anda harus menyertakan izin untuk `s3:PutEncryptionConfiguration` tindakan tersebut karena secara default enkripsi sisi server diaktifkan untuk bucket. Beri bucket Anda nama yang membuatnya mudah diidentifikasi.

   Untuk mempermudah menemukan log Anda, buat folder baru (juga dikenal sebagai awalan) di bucket yang ada untuk menyimpan CloudTrail log Anda.

   > **Note**
   >
   > Nama bucket Amazon S3 Anda harus unik secara global. Untuk informasi selengkapnya, lihat Aturan penamaan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

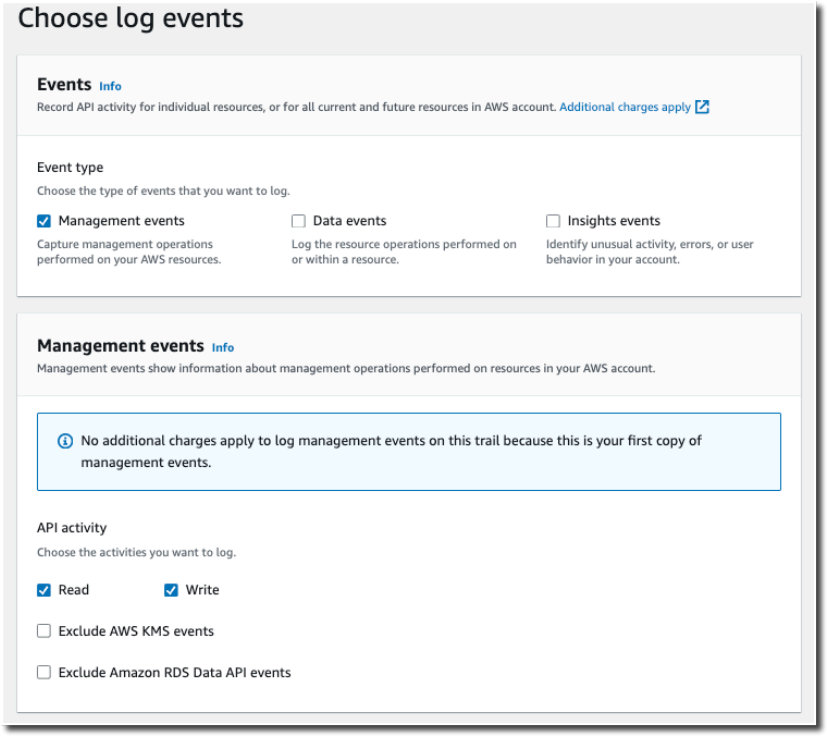
7. Kosongkan kotak centang untuk menonaktifkan SSE-KMS enkripsi file log. Secara default, file log Anda dienkripsi dengan SSE-S3 enkripsi. Untuk informasi selengkapnya tentang pengaturan ini, lihat Menggunakan enkripsi sisi server dengan kunci terkelola Amazon S3 ()SSE-S3.
8. Tinggalkan pengaturan default di Pengaturan tambahan.
9. Tinggalkan pengaturan default untuk CloudWatch Log. Untuk saat ini, jangan mengirim log ke Amazon CloudWatch Logs.

10. (Opsional) Di Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke jejak Anda. Tag dapat membantu Anda mengidentifikasi CloudTrail jejak dan sumber daya lainnya, seperti bucket Amazon S3 yang berisi file CloudTrail log. Misalnya, Anda dapat melampirkan tag dengan nama **`Compliance`** dan nilainya**`Auditing`**.

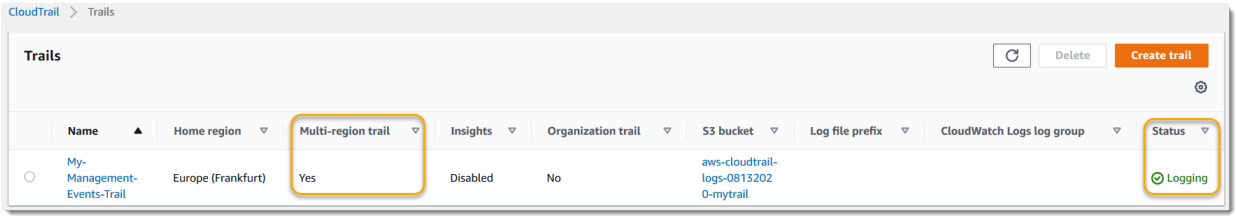
    > **Note**
    >
    > Meskipun Anda dapat menambahkan tag ke jejak saat Anda membuatnya di CloudTrail konsol, dan Anda dapat membuat bucket Amazon S3 untuk menyimpan file log Anda di CloudTrail konsol, Anda tidak dapat menambahkan tag ke bucket Amazon S3 dari CloudTrail konsol. Untuk informasi selengkapnya tentang melihat dan mengubah properti bucket Amazon S3, termasuk menambahkan tag ke bucket, lihat Panduan Pengguna Amazon S3 .

    Setelah Anda selesai membuat tag, pilih Ber ikutnya.

11. Pada halaman Pilih peristiwa log, pilih jenis peristiwa yang akan dicatat. Untuk jejak ini, pertahankan default, A cara manajemen. Di area Acara manajemen, pilih untuk mencatat peristiwa Baca dan Tulis, jika belum dipilih. Biarkan kotak centang untuk K ecualikan AWS KMS peristiwa dan Kecualikan peristiwa API Data Amazon RDS kosong, untuk mencatat semua peristiwa manajemen.



12. Tinggalkan setelan default untuk peristiwa Data, peristiwa Wawasan, dan peristiwa aktivitas Jaringan. Jejak ini tidak akan mencatat peristiwa data, peristiwa Wawasan, atau peristiwa aktivitas jaringan apa pun. Pilih Berikutnya.
13. Pada halaman T injau dan buat, tinjau pengaturan yang telah Anda pilih untuk jejak Anda. Pilih Edit untuk bagian untuk kembali dan membuat perubahan. Saat Anda siap untuk membuat jejak Anda, pilih Buat jejak.
14. Halaman Jalur menunjukkan jejak baru Anda di tabel. Perhatikan bahwa jejak diatur ke Multi-region jejak secara default, dan pencatatan diaktifkan untuk jejak secara default.



Untuk informasi lebih lanjut tentang jalur, lihatBekerja dengan jalan CloudTrail setapak.

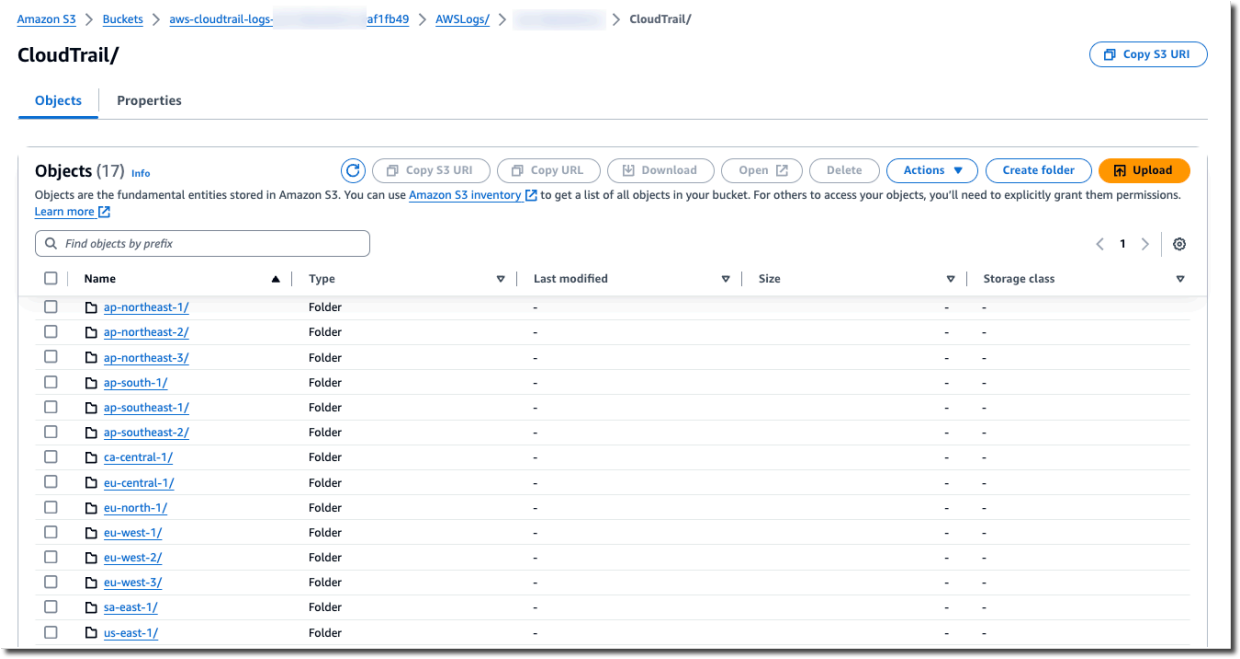
Melihat file log Anda

Dalam waktu rata-rata sekitar 5 menit setelah membuat jejak pertama Anda, CloudTrail kirimkan set file log pertama ke bucket Amazon S3 untuk jejak Anda. Anda dapat melihat file-file ini dan mempelajari tentang informasi yang dikandungnya.

> **Note**
>
> CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian AWS CloudTrail Tingkat Layanan untuk informasi selengkapnya.
> Jika Anda salah mengkonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan kembali file log ke bucket S3 Anda selama 30 hari, dan peristiwa yang dicoba untuk mengirimkan ini akan dikenakan biaya standar. CloudTrail Untuk menghindari biaya pada jejak yang salah dikonfigurasi, Anda perlu menghapus jejak.

Untuk melihat file log Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Jejak. Pada halaman Trails, temukan nama jejak yang baru saja Anda buat (dalam contoh,*`management-events`*).
3. Di baris untuk jejak, pilih nilai untuk bucket S3.
4. Konsol Amazon S3 terbuka dan menampilkan dua folder untuk bucket: `CloudTrail-Digest` dan`CloudTrail`. Pilih CloudTrail folder untuk melihat file log.
5. Jika Anda membuat jejak Multi-wilayah, ada folder untuk masing-masing Wilayah AWS. Pilih folder Wilayah AWS tempat Anda ingin meninjau file log. Misalnya, jika Anda ingin meninjau file log untuk Wilayah AS Timur (Ohio), pilih us-east-2.



6. Arahkan struktur folder bucket ke tahun, bulan, dan hari di mana Anda ingin meninjau log aktivitas di Wilayah tersebut. Pada hari itu, ada sejumlah file. Nama file dimulai dengan Akun AWS ID Anda, dan diakhiri dengan ekstensi `.gz`. Misalnya, jika ID akun Anda adalah*123456789012*, Anda akan melihat file dengan nama yang mirip dengan ini: *123456789012* _ _ CloudTrail *us-east-2* _ *20240512T0000Z_EXAMPLE* .json.gz.

   Untuk melihat file-file ini, Anda dapat mengunduhnya, unzip, dan kemudian melihatnya di editor teks biasa atau penampil file JSON. Beberapa browser juga mendukung tampilan file.gz dan JSON secara langsung. Sebaiknya gunakan penampil JSON, karena membuatnya lebih mudah untuk mengurai informasi dalam file CloudTrail log.

Membuat penyimpanan data peristiwa untuk peristiwa data S3

Anda dapat membuat penyimpanan data peristiwa untuk mencatat CloudTrail peristiwa (peristiwa manajemen, peristiwa data), peristiwa CloudTrail Wawasan, AWS Audit Manager bukti, item AWS Config konfigurasi, atau non-AWS peristiwa.

Saat Anda membuat penyimpanan data peristiwa untuk peristiwa data, Anda memilih jenis sumber daya Layanan AWS dan yang ingin Anda catat peristiwa datanya. Untuk informasi tentang Layanan AWS peristiwa data log tersebut, lihatPeristiwa data.

Panduan ini menunjukkan cara membuat penyimpanan data peristiwa untuk acara data Amazon S3. Dalam tutorial ini, alih-alih mencatat semua peristiwa data Amazon S3, kita akan memilih template pemilih log khusus untuk mencatat peristiwa hanya ketika objek dihapus dari bucket S3 tertentu.

Untuk membuat penyimpanan data peristiwa untuk peristiwa data S3

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, berikan nama penyimpanan data acara Anda, seperti`s3-data-events-eds`. Sebagai praktik terbaik, gunakan nama yang dengan cepat mengidentifikasi tujuan penyimpanan data peristiwa. Untuk informasi tentang CloudTrail persyaratan penamaan, lihatPersyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
     - Periode retensi default: 366 hari
     - Periode retensi maksimum: 3.653 hari
   - Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
     - Periode retensi default: 2.557 hari
     - Periode retensi maksimum: 2.557 hari

6. Tentukan periode retensi untuk penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

   CloudTrail Lake menentukan apakah acara akan dipertahankan dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode penyimpanan 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

7. (Opsional) Dalam En kripsi. pilih apakah Anda ingin mengenkripsi penyimpanan data peristiwa menggunakan kunci KMS Anda sendiri. Secara default, semua peristiwa di penyimpanan data peristiwa dienkripsi dengan CloudTrail menggunakan kunci KMS yang dimiliki dan AWS dikelola untuk Anda.

   Untuk mengaktifkan enkripsi menggunakan kunci KMS Anda sendiri, pilih Gunakan milik saya sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/`*`MyAliasName`*. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar CloudTrail log dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

   Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

   > **Note**
   >
   > Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses

data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

   Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

   Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`

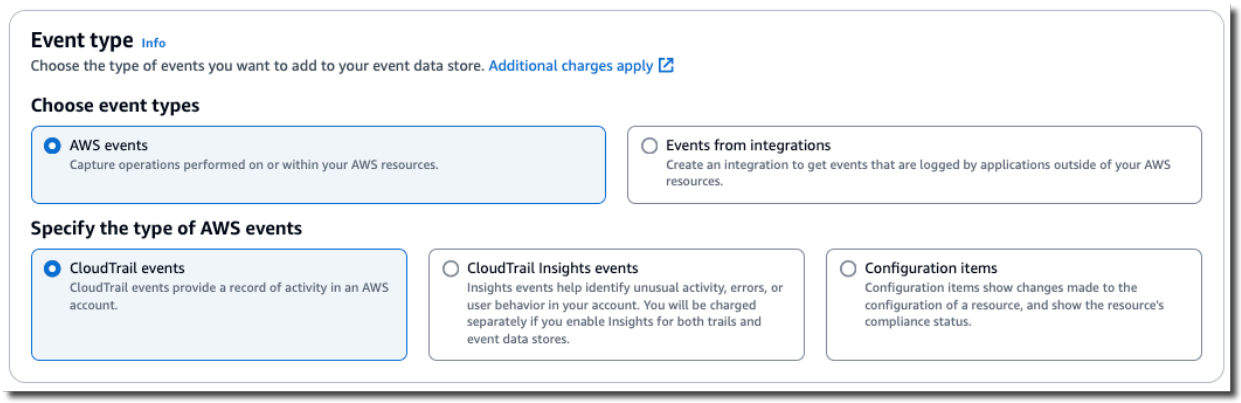
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

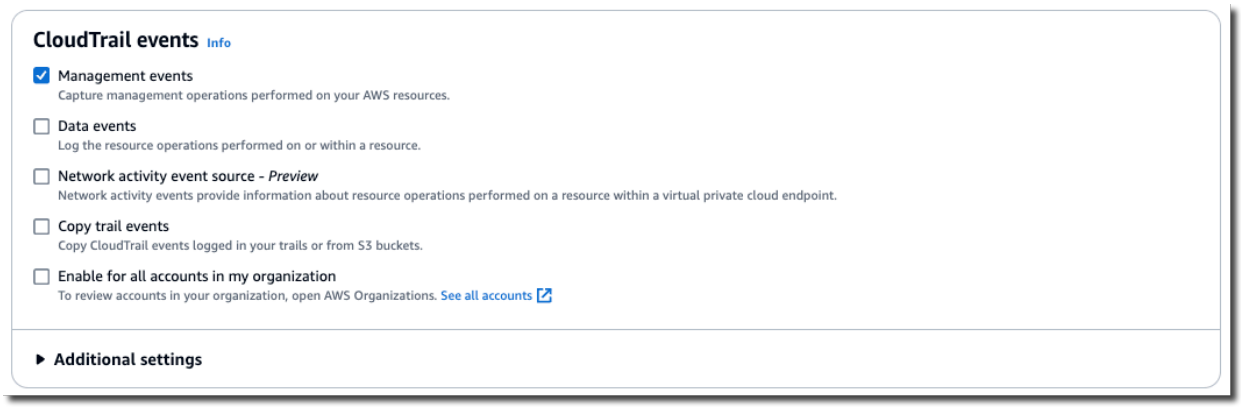
10. (Opsional) Di Tag, tambahkan satu atau beberapa tag kustom (pasangan kunci-nilai) ke penyimpanan data acara Anda. Tag dapat membantu Anda mengidentifikasi penyimpanan data CloudTrail acara Anda. Misalnya, Anda dapat melampirkan tag dengan nama **`stage`** dan nilainya**`prod`**. Anda dapat menggunakan tag untuk membatasi akses ke penyimpanan data acara Anda. Anda juga dapat menggunakan tag untuk melacak kueri dan biaya penyerapan untuk penyimpanan data acara Anda.

    Untuk informasi tentang cara menggunakan tag untuk melacak biaya, lihatMembuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake. Untuk informasi tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi tentang cara menggunakan tag di AWS, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Men andai Sumber AWS Daya.

11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
12. Pada halaman Pilih acara, tinggalkan pilihan default untuk jenis acara.



13. Untuk CloudTrail acara, pilih A cara data dan hapus pilihan Acara manajemen. Untuk informasi selengkapnya tentang peristiwa data, lihatMencatat log peristiwa data.

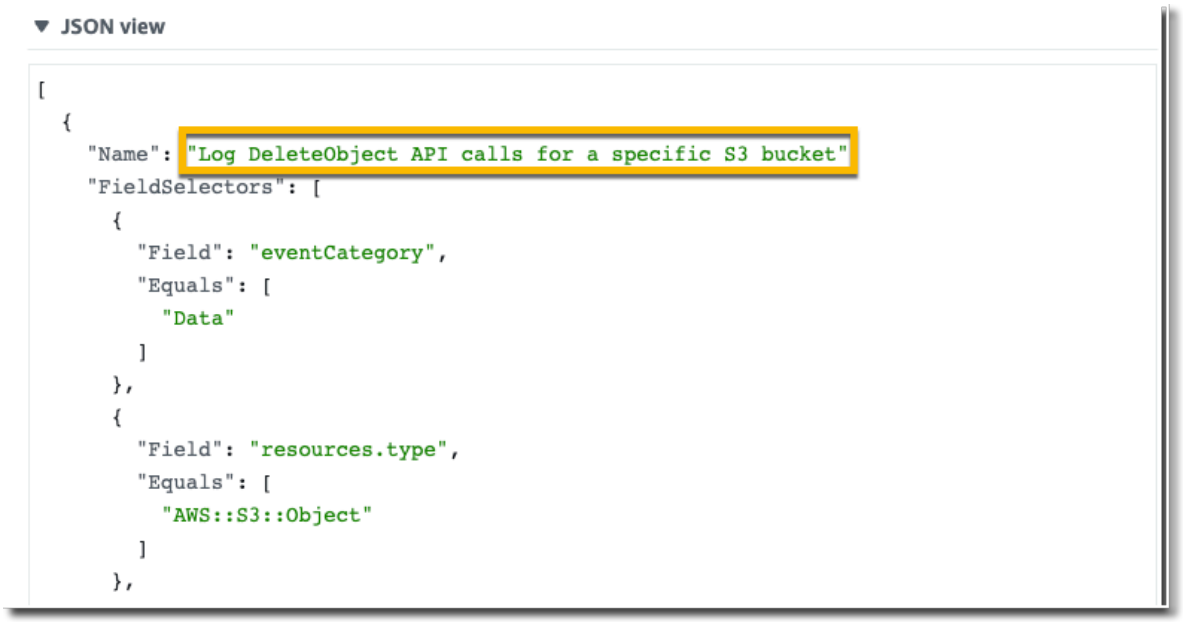


14. Tinggalkan pengaturan default untuk Sal in peristiwa jejak. Anda akan menggunakan opsi ini untuk menyalin peristiwa jejak yang ada ke penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat Salin peristiwa jejak ke penyimpanan data peristiwa.
15. Pilih Aktifkan untuk semua akun di organisasi saya jika ini adalah penyimpanan data acara organisasi. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi AWS Organizations.
16. Untuk pengaturan tambahan tinggalkan pilihan default. Secara default, penyimpanan data peristiwa mengumpulkan peristiwa untuk semua Wilayah AWS dan mulai menyerap peristiwa saat dibuat.
17. Untuk acara Data, buat pilihan berikut:

    a. Di Jenis sumber daya, pilih S3. Jenis sumber daya mengidentifikasi Layanan AWS dan sumber daya tempat peristiwa data dicatat.

    b. Di Template pemilih log, pilih K ustom. Memilih K ustom memungkinkan Anda menentukan pemilih acara khusus untuk memfilter pada `readOnly` bidang`eventName`,`resources.`ARN, dan. Untuk informasi tentang bidang ini, lihat AdvancedFieldSelector di Refer AWS CloudTrail ensi API.

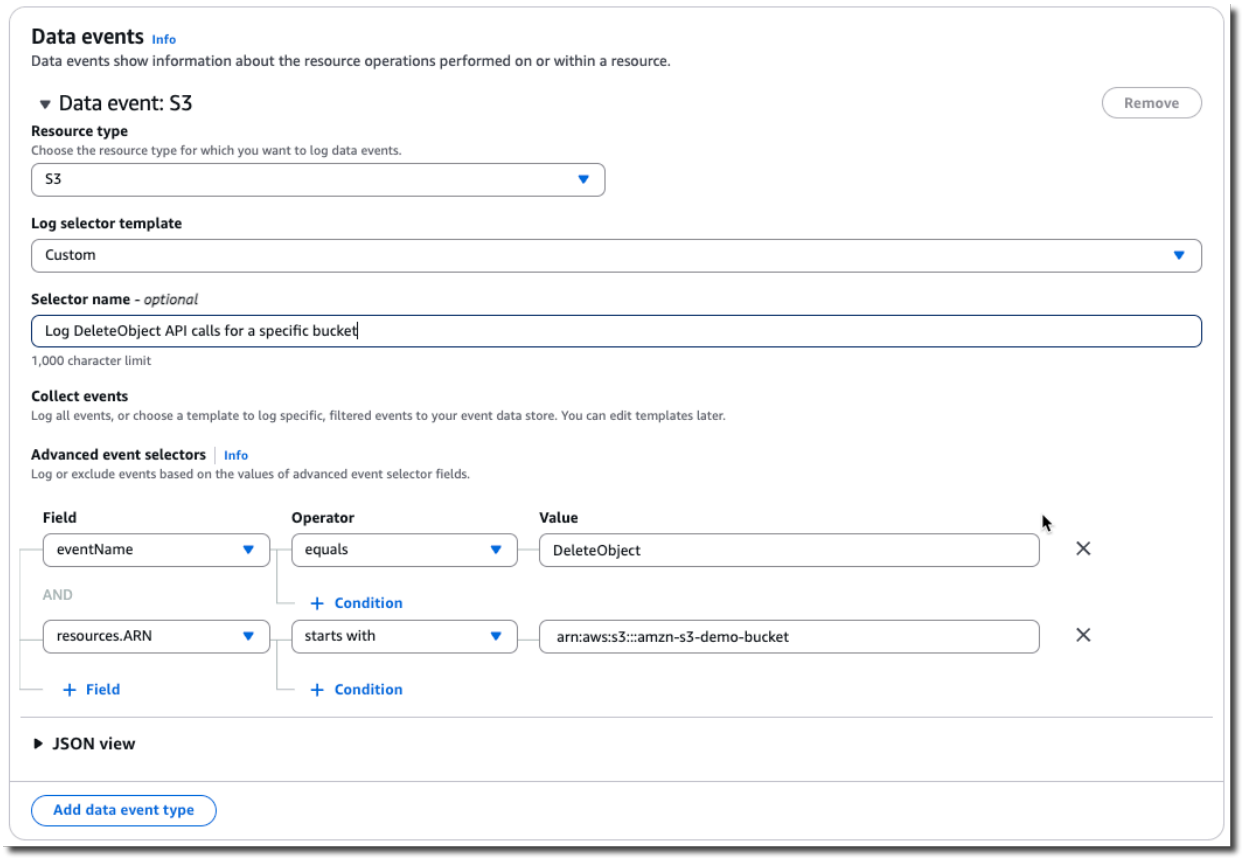
    c. (Opsional) Di Nama pemilih, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Panggilan DeleteObject API log untuk bucket S3 tertentu”. Nama pemilih terdaftar seperti `Name` pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.



d. Dalam pemilih acara lanj utan, kita akan membangun pemilih acara khusus untuk memfilter bidang `eventName` dan`resources.ARN`. Pemilih acara lanjutan untuk penyimpanan data peristiwa bekerja sama dengan pemilih peristiwa lanjutan yang Anda terapkan ke jejak. Untuk informasi selengkapnya tentang cara membuat pemilih acara lanjutan, lihat Mencatat peristiwa data dengan pemilih peristiwa lanjutan.

   i. Untuk Field pilih EventName. Untuk Operator, pilih sama. Untuk Nilai, masukkan **`DeleteObject`**. Pilih + Bid ang untuk memfilter bidang lain.

   ii. Untuk Field, pilih Resources.arn. Untuk Operator, pilih StartsWith. Untuk Nilai, masukkan ARN untuk bucket Anda (misalnya, arn:aws:s3:::). *`amzn-s3-demo-bucket`* Untuk informasi tentang cara mendapatkan ARN, lihat sumber daya Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.



18. Pilih Berikutnya untuk meninjau pilihan Anda.
19. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
20. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.

    Dari titik ini ke depan, penyimpanan data peristiwa menangkap peristiwa yang cocok dengan pemilih acara lanjutnya. Peristiwa yang terjadi sebelum Anda membuat penyimpanan data peristiwa tidak ada di penyimpanan data peristiwa, kecuali Anda memilih untuk menyalin peristiwa jejak yang ada.

Anda sekarang siap untuk menjalankan kueri di penyimpanan data acara Anda. Untuk informasi tentang cara melihat dan menjalankan kueri sampel, lihatLihat contoh kueri dengan konsol CloudTrail.

Untuk informasi lebih lanjut tentang CloudTrail Danau, lihatBekerja dengan AWS CloudTrail Danau.

Melihat CloudTrail biaya dan penggunaan Anda dengan AWS Cost Explorer

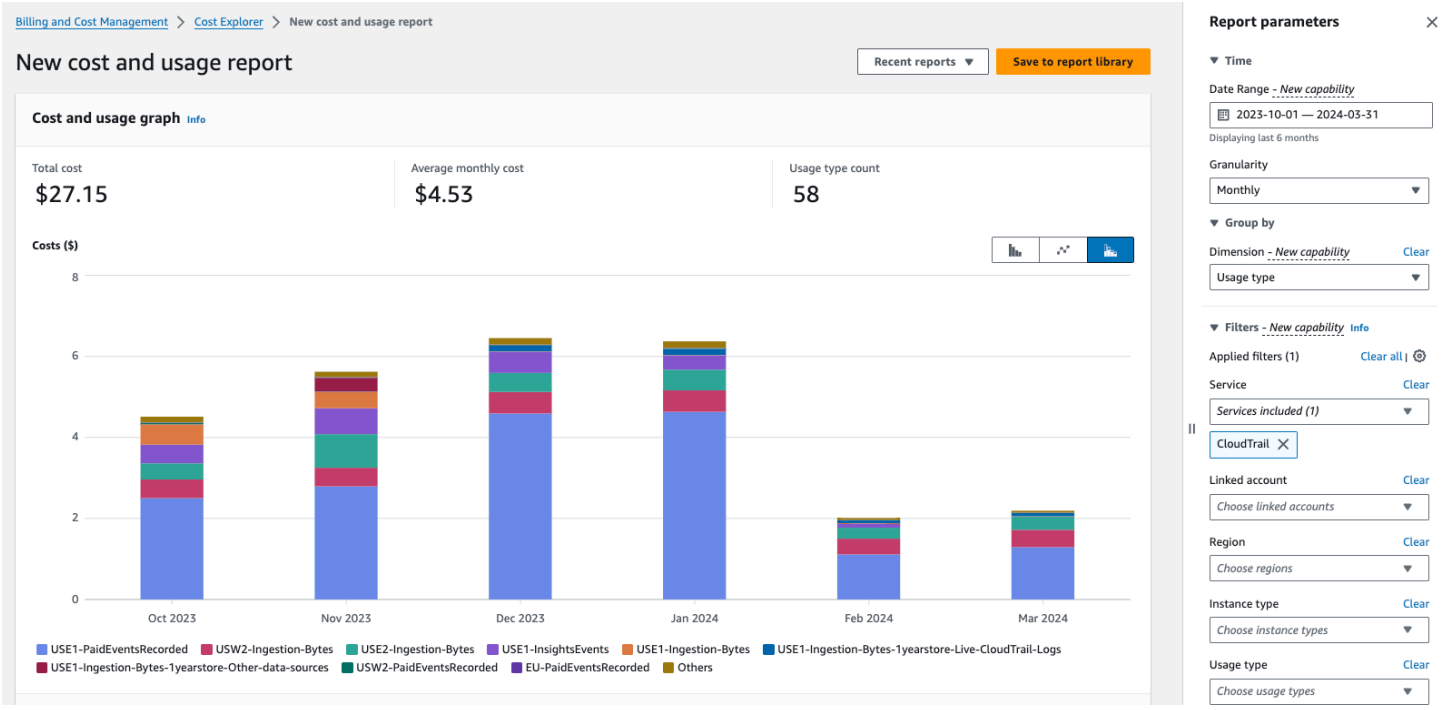
Bagian ini menjelaskan bagaimana Anda dapat melihat CloudTrail biaya dan penggunaan Anda AWS Cost Explorer. Cost Explorer memberi Anda kemampuan untuk memvisualisasikan, memahami, dan mengelola AWS biaya dan penggunaan Anda dari waktu ke waktu.

Untuk detail tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Untuk melihat CloudTrail biaya dan penggunaan dengan Cost Explorer

1. Masuk ke Konsol Manajemen AWS dan buka konsol Cost Explorer di https://console.aws.amazon.com/cost-management/home#/custom.
2. Di bawah Waktu, pilih rentang tanggal yang ingin Anda analisis.
3. Di bawah Kelompokkan menurut, untuk Dimensi, pilih Jenis penggunaan.
4. Di bawah Filter, untuk Layanan, pilih CloudTrail.

Gambar berikut menunjukkan contoh laporan biaya yang difilter CloudTrail dan dikelompokkan berdasarkan jenis Penggunaan.



Tinjau jenis Penggunaan untuk melihat CloudTrail fitur mana yang menghasilkan biaya paling banyak. Setiap jenis Penggunaan dimulai dengan kode Wilayah AWS tempat biaya dikeluarkan.

Tabel berikut menjelaskan jenis CloudTrail penggunaan untuk setiap CloudTrail fitur.

CloudTrail fitur	Jenis penggunaan	Deskripsi
CloudTrail jalan setapak	*region*-FreeEventsRecorded	Salinan pertama acara manajemen dikirimkan secara gratis ke file Wilayah AWS.
CloudTrail jalan setapak	*region*-PaidEventsRecorded	Biaya untuk salinan tambahan acara manajemen yang dikirimkan ke file Wilayah AWS.
CloudTrail jalan setapak	*region*-DataEventsRecorded	Biaya untuk pengiriman peristiwa data ke file Wilayah AWS. Peristiwa data selalu dikenakan biaya.
CloudTrail jalan setapak	*region*-NetworkEventsRecorded	Biaya untuk pengiriman acara aktivitas jaringan ke file Wilayah AWS. Acara aktivitas jaringan selalu dikenakan biaya.

CloudTrail fitur	Jenis penggunaan	Deskripsi
CloudTrail Danau	*region*-Ingestion-Bytes	Biaya untuk memasukkan acara ke dalam penyimpan an data acara CloudTrail Lake menggunakan opsi harga Seven-year retensi. Harga konsumsi didasarkan pada volume data yang dicerna dan sama untuk semua jenis acara.
CloudTrail Danau	*region*-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	Biaya untuk memasukka n peristiwa CloudTrail data, peristiwa aktivitas jaringan, dan peristiwa manajemen ke dalam penyimpan an data acara CloudTrail Lake menggunakan opsi harga retensi yang One-year dapat diperpanj ang.

CloudTrail fitur	Jenis penggunaan	Deskripsi
CloudTrail Danau	*region*-Ingestion-Bytes-1yearstore-Other-data-sources	Biaya untuk memasukkan sumber acara lain ke dalam penyimpanan data acara CloudTrail Lake menggunakan opsi harga retensi yang One-year dapat diperpanjang. Ini termasuk peristiwa CloudTrail Wawasan, item konfigurasi dari, bukti dari AWS Config AWS Audit Manager, CloudTrail log historis (tidak terkompresi) yang diimpor dari S3, dan peristiwa di luar. AWS

CloudTrail fitur	Jenis penggunaan	Deskripsi
CloudTrail Danau	*region*-QueryScanned-Bytes	Biaya untuk menjalankan kueri CloudTrail Danau. Saat menjalankan kueri di CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data yang dioptimalkan dan dikompresi yang dipindai.
CloudTrail Wawasan	*region*-InsightsEvents	Biaya untuk acara CloudTrail Insights. Untuk acara Insights, Anda dikenakan biaya berdasarkan jumlah peristiwa manajemen yang dianalisis per jenis Insight. Untuk informasi selengkapnya, lihat Biaya untuk acara Insights.

Penggunaan AWS Budgets untuk mengelola biaya

AWS Budgets fitur AWS Manajemen Penagihan dan Biaya, memungkinkan Anda untuk mengatur anggaran khusus yang mengingatkan Anda ketika biaya atau penggunaan Anda melebihi (atau diperkirakan melebihi) jumlah yang dianggarkan Anda.

Membuat anggaran untuk CloudTrail menggunakan AWS Budgets adalah praktik terbaik yang direkomendasikan, dan dapat membantu Anda melacak CloudTrail pengeluaran Anda. Cost-based anggaran membantu meningkatkan kesadaran tentang berapa banyak Anda mungkin ditagih untuk penggunaan Anda CloudTrail . Peringatan anggaran memberi tahu Anda ketika tagihan Anda mencapai ambang batas yang Anda tentukan. Ketika Anda menerima peringatan anggaran, Anda dapat membuat perubahan sebelum akhir siklus penagihan untuk mengelola biaya Anda.

> **Note**
>
> Meskipun Anda dapat menerapkan tag ke CloudTrail jejak, saat ini AWS Billing tidak dapat menggunakan tag yang diterapkan ke jalur untuk alokasi biaya. Cost Explorer dapat menunjukkan biaya untuk penyimpanan data acara CloudTrail Lake dan untuk CloudTrail layanan secara keseluruhan.

Untuk memulai dengan AWS Anggaran, buka AWS Manajemen Penagihan dan Biaya, lalu pilih Anggaran di bilah navigasi kiri. Sebaiknya konfigurasi lansiran anggaran saat Anda membuat anggaran untuk melacak CloudTrail pengeluaran. Untuk informasi selengkapnya tentang cara menggunakan AWS Anggaran, lihat Mengelola biaya Anda dengan AWS Budgets dan Praktik terbaik untuk AWS Budgets.

Membuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake

Anda dapat membuat tag alokasi biaya yang ditentukan pengguna untuk melacak kueri dan biaya konsumsi untuk penyimpanan data acara Lake Anda CloudTrail. Tag alokasi biaya yang ditentukan pengguna adalah pasangan nilai kunci yang dapat Anda kaitkan dengan penyimpanan data peristiwa. Setelah Anda mengaktifkan tag alokasi biaya, AWS gunakan tag untuk mengatur biaya sumber daya Anda pada laporan alokasi biaya Anda.

- Untuk membuat tag di konsol, lihat langkah 9 dari Untuk membuat penyimpanan data acara untuk CloudTrail acara prosedur.
- Untuk membuat tag menggunakan CloudTrail API, lihat CreateEventDataStoredan AddTagsdi Referensi AWS CloudTrail API.
- Untuk membuat tag menggunakan AWS CLI, lihat create-event-data-store dan add-tag di Command Reference.AWS CLI

Untuk informasi selengkapnya tentang mengaktifkan tag, lihat Mengaktifkan tag alokasi biaya yang ditentukan pengguna.

Mengelola biaya CloudTrail jejak

Anda dapat mengonfigurasi dan mengelola CloudTrail jejak dengan cara yang menangkap data yang Anda butuhkan sambil tetap hemat biaya. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Konfigurasi jejak

CloudTrail menawarkan fleksibilitas dalam cara Anda mengonfigurasi jejak di akun Anda. Beberapa keputusan yang Anda buat selama proses penyiapan mengharuskan Anda memahami dampaknya terhadap CloudTrail tagihan Anda. Berikut ini adalah contoh bagaimana konfigurasi jejak dapat memengaruhi CloudTrail tagihan Anda.

Penciptaan beberapa jejak

Salinan pertama acara manajemen di setiap wilayah dikirimkan secara gratis. Misalnya, jika akun Anda memiliki 2 jalur wilayah tunggal, jalur masuk, `us-east-1` dan jalur lain`us-west-2`, tidak ada CloudTrail biaya karena hanya ada satu peristiwa pencatatan jejak di setiap Wilayah masing-masing. Namun, jika akun Anda memiliki jejak Multi-wilayah dan jalur Single-region tambahan, jalur Single-region akan dikenakan biaya karena jalur Multi-wilayah sudah mencatat peristiwa di setiap Wilayah.

Jika Anda membuat lebih banyak jalur yang mengirimkan acara manajemen yang sama ke tujuan lain, pengiriman berikutnya akan dikenakan CloudTrail biaya. Anda dapat melakukan ini untuk memungkinkan grup pengguna yang berbeda (seperti pengembang, personel keamanan, dan auditor TI) menerima salinan file log mereka sendiri. Untuk kejadian data, semua pengiriman dikenakan CloudTrail biaya, termasuk yang pertama.

Saat Anda membuat lebih banyak jejak, sangat penting untuk mengetahui log Anda, dan memahami jenis dan volume peristiwa yang dihasilkan oleh sumber daya di akun Anda. Ini membantu Anda mengantisipasi volume peristiwa yang terkait dengan akun, dan merencanakan biaya jejak. Misalnya, menggunakan enkripsi sisi server yang AWS KMS dikelola (SSE-KMS) pada bucket S3 Anda dapat menghasilkan sejumlah besar peristiwa manajemen. AWS KMS CloudTrail Volume peristiwa yang lebih besar di beberapa jalur juga dapat memengaruhi biaya.

Untuk membantu membatasi jumlah peristiwa yang dicatat ke jejak Anda, Anda dapat memfilter AWS KMS atau peristiwa Amazon RDS Data API dengan memilih Kecualikan peristiwa atau Kecualikan AWS KMS peristiwa Amazon RDS Data API di halaman jejak Buat jejak atau Perbarui. Saat menggunakan pemilih acara dasar, Anda hanya dapat memfilter acara manajemen. Namun, Anda dapat menggunakan pemilih acara lanjutan untuk memfilter peristiwa manajemen dan data.

Anda dapat menggunakan pemilih acara lanjutan untuk menyertakan atau mengecualikan peristiwa data, memberi Anda kemampuan untuk mencatat hanya peristiwa data yang menarik. Untuk informasi selengkapnya, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut.

Anda dapat menggunakan pemilih acara lanjutan untuk menyertakan atau mengecualikan peristiwa aktivitas jaringan berdasarkan`eventName`,,`resources.type`,`resources.ARN`,`errorCode`, dan `vpcEndpointId` bidang, sehingga Anda dapat mencatat hanya peristiwa data yang menarik. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.

Untuk informasi selengkapnya tentang membuat dan memperbarui jejak, lihat Membuat jejak dengan CloudTrail konsol atau Memperbarui jejak dengan CloudTrail konsol di panduan ini.

AWS Organizations

Saat Anda menyiapkan jejak Organizations dengan CloudTrail, CloudTrail mereplikasi jejak ke setiap akun anggota dalam organisasi Anda. Jejak baru dibuat selain jalur yang ada di akun anggota. Pastikan bahwa konfigurasi jejak organisasi Anda cocok dengan cara Anda ingin jejak yang dikonfigurasi untuk semua akun dalam organisasi, karena konfigurasi jejak organisasi menyebar ke semua akun.

Karena Organizations membuat jejak di setiap akun anggota, akun anggota individu yang membuat jejak tambahan untuk mengumpulkan acara manajemen yang sama dengan jejak Organizations mengumpulkan salinan acara kedua. Akun dibebankan untuk salinan kedua. Demikian pula, jika akun memiliki jejak Multi-wilayah, dan membuat jejak kedua di satu Wilayah untuk mengumpulkan acara manajemen yang sama dengan jejak Multi-wilayah, jejak di Wilayah tunggal mengirimkan salinan peristiwa kedua. Salinan kedua menimbulkan biaya.

Lihat juga

- Harga AWS CloudTrail
- Mengelola biaya Anda dengan AWS Budgets

- Memulai Cost Explorer
- Bersiaplah untuk membuat jejak untuk organisasi Anda

Mengelola biaya CloudTrail Danau

AWS CloudTrail Penyimpanan data acara danau dan kueri dikenakan biaya. Anda dapat mengonfigurasi penyimpanan data peristiwa dengan cara yang menangkap data yang Anda butuhkan sambil tetap hemat biaya. Untuk informasi selengkapnya tentang harga CloudTrail , lihat Harga AWS CloudTrail.

Topik

- Opsi harga toko data acara
- Memahami biaya CloudTrail Danau
- Rekomendasi tentang bagaimana Anda dapat mengurangi biaya
- Lihat juga

Opsi harga toko data acara

Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data acara.

Tabel berikut menjelaskan opsi harga yang tersedia. Tabel menunjukkan opsi Harga di konsol dan `BillingMode` nilai yang sesuai untuk API, dan mencantumkan periode retensi default dan maksimum untuk setiap opsi.

Opsi harga (konsol)	BillingMode (API)	Deskripsi
Harga retensi yang dapat diperpanjang satu tahun	`EXTENDABLE_RETENTION_PRICING`	Direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data peristiwa per bulan dan menginginkan periode retensi yang fleksibel hingga 10 tahun. Opsi ini juga disarankan jika penyimpanan data acara Anda mengumpulkan item AWS Config

Opsi harga (konsol)	BillingMode (API)	Deskripsi
		konfigurasi, bukti Audit Manager, dan peristiwa dari luar. AWS Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga konsumsi. Setelah 366 hari, retensi diperpanjang tersedia dengan pay-as-you-go harga. Ini adalah pilihan default. Periode retensi default: 366 hari Periode retensi maksimum: 3,653 hari
Harga retensi tujuh tahun	`FIXED_RETENTION_PRICING`	Direkomendasikan jika mengharapkan untuk menelan lebih dari 25 TB data peristiwa per bulan dan membutuhkan periode retensi hingga 7 tahun. Retensi disertakan dengan harga konsumsi tanpa biaya tambahan. Periode retensi default: 2,557 hari Periode retensi maksimum: 2.557 hari

Memahami biaya CloudTrail Danau

Tabel berikut memberikan informasi tentang bagaimana penyimpanan data acara CloudTrail Lake dan kueri dikenakan biaya. Untuk informasi selengkapnya tentang harga CloudTrail , lihat Harga AWS CloudTrail.

Jenis biaya	Bagaimana Anda dikenakan biaya
Konsumsi data (data tidak terkompresi)	Untuk CloudTrail Lake, Anda membayar berdasarkan data yang tidak terkompresi yang dicerna. Opsi harga untuk penyimpanan data acara menentukan biaya menelan acara: • Harga retensi yang dapat diperpanjang satu tahun: Menawarkan harga konsumsi berdasarkan jenis acara. • Harga retensi tujuh tahun: Menawarkan harga konsumsi berdasarkan volume data yang dicerna. Penghematan terbesar dicapai ketika volume data yang dicerna setiap bulan melebihi 25 TB. Menyalin acara jejak Saat Anda menyalin peristiwa jejak ke CloudTrail Lake, CloudTrail buka ritsleting log yang disimpan dalam format gzip (terkompresi). Kemudian CloudTrail salin peristiwa yang terkandung dalam log ke penyimpanan data acara Anda. Ukuran data yang tidak terkompresi bisa lebih besar dari ukuran penyimpanan Amazon S3 yang sebenarnya. Untuk mendapatk an perkiraan umum ukuran data yang tidak terkompresi, kalikan ukuran log di bucket S3 dengan 10. **Note** CloudTrail tidak akan menyalin peristiwa jika waktu acaranya lebih lama dari periode retensi yang ditentuka n. Untuk menentukan periode retensi yang sesuai, ambil jumlah peristiwa tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara seperti yang ditunjukkan dalam persamaan ini: Periode retensi = *oldest-event-in-days* + *number-days-to-retain* Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan

Jenis biaya	Bagaimana Anda dikenakan biaya
	data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.
Retensi data (data yang dioptimalkan dan dikompresi)	CloudTrail Lake mengubah peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan cepat data terkompresi. Periode retensi penyimpanan data peristiwa menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail Lake menentukan apakah akan mempertah ankan suatu peristiwa dengan memeriksa apakah waktu acara berada dalam periode retensi yang ditentukan. Misalnya, jika Anda menentukan periode retensi 90 hari, CloudTrail akan menghapus peristiwa ketika waktu acara mereka lebih dari 90 hari. Untuk penyimpanan data acara menggunakan opsi harga retensi tujuh tahun, penyimpanan disertakan dengan harga konsumsi tanpa biaya tambahan. Untuk penyimpanan data acara menggunakan opsi harga retensi yang dapat diperpanjang satu tahun, penyimpanan disertakan tanpa biaya dengan harga konsumsi untuk 366 hari pertama (periode retensi default). Setelah 366 hari, penyimpan an ditawarkan di pay-as-you-pricing dan dibebankan berdasark an data yang dioptimalkan dan dikompresi di penyimpanan data acara.
Menjalankan kueri di CloudTrail Lake (data yang dioptimalkan dan dikompresi)	Saat menjalankan kueri di CloudTrail Lake, Anda membayar berdasarkan jumlah data yang dioptimalkan dan dikompresi yang dipindai.

Rekomendasi tentang bagaimana Anda dapat mengurangi biaya

Bagian ini memberikan rekomendasi tentang bagaimana Anda dapat mengurangi biaya saat bekerja dengan CloudTrail Lake.

Pilih opsi harga berdasarkan jenis acara yang akan dikumpulkan oleh toko data acara Anda dan konsumsi bulanan yang Anda harapkan

- Saat membuat penyimpanan data acara, pilih opsi harga berdasarkan jenis acara yang akan dikumpulkan oleh toko data acara Anda dan konsumsi bulanan yang Anda harapkan.

- Jika Anda berharap untuk menelan kurang dari 25 TB data acara setiap bulan dan menginginkan periode retensi yang fleksibel hingga 10 tahun, pilih opsi harga retensi yang dapat diperpanjang satu tahun. Kami juga umumnya merekomendasikan opsi ini untuk penyimpanan data peristiwa yang mengumpulkan item AWS Config konfigurasi, bukti Audit Manager, dan peristiwa dari luar AWS.

- Jika Anda berharap untuk menelan lebih dari 25 TB data acara setiap bulan dan membutuhkan periode retensi 7 tahun, pilih opsi harga retensi tujuh tahun.

Evaluasi konsumsi bulanan toko data acara Anda dari waktu ke waktu

- Evaluasi konsumsi bulanan historis penyimpanan data acara Anda untuk melihat apakah ada opsi harga yang lebih sesuai dengan kebutuhan Anda.

- Jika Anda memiliki penyimpanan data acara yang ada yang menggunakan opsi penetapan harga retensi tujuh tahun dan Anda mengonsumsi data kurang dari 25 TB setiap bulan, pertimbangkan untuk memperbarui penyimpanan data acara untuk menggunakan harga retensi yang dapat diperpanjang satu tahun. Untuk penyimpanan data peristiwa menggunakan opsi penetapan harga retensi tujuh tahun, Anda dapat mengubah opsi harga menggunakan CloudTrail konsol AWS CLI, atau UpdateEventDataStoreoperasi API.

- Jika Anda memiliki penyimpanan data acara yang ada yang menggunakan opsi harga retensi yang dapat diperpanjang satu tahun dan Anda menelan lebih dari 25 TB data acara setiap bulan, pertimbangkan apakah harga retensi tujuh tahun akan lebih sesuai dengan kebutuhan Anda. Untuk menggunakan opsi harga baru, hentikan konsumsi pada penyimpanan data acara Anda dan buat penyimpanan data acara baru dengan opsi harga retensi tujuh tahun.

Gunakan penyeleksi acara lanjutan untuk menyaring acara yang tidak menarik

Saat mengonfigurasi penyimpanan data peristiwa untuk acara CloudTrail manajemen, peristiwa data, atau peristiwa aktivitas jaringan, Anda dapat memfilter peristiwa yang tidak menarik dengan menggunakan pemilih acara lanjutan.

Anda dapat memfilter peristiwa manajemen pada bidang pemilih acara lanjutan berikut:`eventName`,,`eventSource`,`eventType`, `readOnlysessionCredentialFromConsole`, dan`userIdentity.arn`.

Anda dapat memfilter peristiwa data pada bidang pemilih acara lanjutan berikut:`eventName`,,`eventSource`,`eventType`,`resources.type`,`resources.`ARN, `readOnlysessionCredentialFromConsole`, dan`userIdentity.arn`. Untuk informasi selengkapnya, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut.

Anda dapat memfilter peristiwa aktivitas jaringan pada bidang pemilih peristiwa lanjutan berikut:`eventName`,`errorCode`, dan`vpcEndpointId`. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.

Pilih rentang waktu yang lebih sempit saat menyalin peristiwa jejak

Saat menyalin peristiwa jejak ke CloudTrail Danau, tentukan waktu acara mulai yang lebih sempit dan waktu acara akhir untuk mengurangi jumlah data yang tertelan.

Jika Anda menyalin peristiwa jejak ke CloudTrail Danau untuk analisis historis dan tidak ingin menelan peristiwa masa depan, batalkan pilihan untuk menelan peristiwa sehingga Anda tidak dikenakan biaya untuk menelan peristiwa tambahan apa pun.

Memformat kueri untuk menggunakan awal dan akhir **`eventTime`**

Ketika Anda menjalankan kueri di Lake, Anda membayar berdasarkan jumlah data yang dipindai. Anda dapat membatasi biaya dengan menentukan awal dan akhir `eventTime` untuk kueri.

Lihat juga

- Harga AWS CloudTrail
- CloudWatch Metrik yang didukung
- Mengelola biaya Anda dengan AWS Budgets
- Memulai dengan Cost Explorer

Bekerja dengan riwayat CloudTrail acara

CloudTrail diaktifkan secara default untuk AWS akun Anda dan Anda secara otomatis memiliki akses ke riwayat CloudTrail acara. Riwayat acara menyediakan catatan yang dapat dilihat, dapat dicari, dapat diunduh, dan tidak dapat diubah dari 90 hari terakhir peristiwa manajemen dalam file. Wilayah AWS Peristiwa ini menangkap aktivitas yang dilakukan melalui Konsol Manajemen AWS AWS Command Line Interface,, AWS SDKs dan APIs. Sejarah peristiwa mencatat peristiwa di Wilayah AWS mana peristiwa itu terjadi. Tidak ada CloudTrail biaya untuk melihat riwayat acara.

Anda dapat mencari peristiwa yang terkait dengan pembuatan, modifikasi, atau penghapusan sumber daya (seperti pengguna IAM atau EC2 instans Amazon) di basis menurut Wilayah Anda Akun AWS di CloudTrail konsol dengan melihat halaman Riwayat peristiwa. Anda juga dapat mencari peristiwa ini dengan menjalankan `aws cloudtrail lookup-events`perintah atau dengan menggunakan `LookupEvents`API.

Anda dapat menggunakan halaman Riwayat peristiwa di CloudTrail konsol untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi aktivitas akun di seluruh AWS infrastruktur Anda. Anda dapat menyesuaikan tampilan halaman Riwayat acara di konsol dengan memilih berapa banyak acara yang akan ditampilkan di setiap halaman dan kolom mana yang akan ditampilkan atau disembunyikan. Anda juga dapat membandingkan detail peristiwa dalam sejarah acara side-by-side. Anda dapat secara terprogram mencari acara dengan menggunakan atau. AWS SDKs AWS Command Line Interface

> **Note**
>
> Seiring waktu, Layanan AWS mungkin menambahkan acara tambahan. CloudTrail mencatat peristiwa ini dalam riwayat peristiwa, tetapi catatan aktivitas 90 hari penuh yang mencakup acara tambahan tidak akan tersedia hingga 90 hari setelah acara tersebut ditambahkan. Riwayat acara terpisah dari jejak atau penyimpanan data acara yang Anda buat untuk akun Anda. Perubahan yang Anda buat pada penyimpanan atau jejak data acara Anda tidak memengaruhi riwayat acara.

Bagian berikut menjelaskan cara mencari peristiwa manajemen terbaru dengan menggunakan CloudTrail konsol dan AWS CLI, dan menjelaskan cara mengunduh file acara. Untuk informasi tentang penggunaan `LookupEvents` API untuk mengambil informasi dari CloudTrail peristiwa, lihat LookupEventsdi Referensi AWS CloudTrail API.

Topik

- Keterbatasan sejarah acara
- Melihat acara manajemen terbaru dengan konsol
- Melihat acara manajemen terbaru dengan AWS CLI

Keterbatasan sejarah acara

Batasan berikut berlaku untuk riwayat acara.

- Halaman Riwayat peristiwa di CloudTrail konsol hanya menampilkan peristiwa manajemen. Ini tidak menampilkan peristiwa data, peristiwa Wawasan, atau peristiwa aktivitas jaringan.
- Riwayat acara terbatas pada 90 hari terakhir peristiwa. Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, buat penyimpanan data acara atau jejak.
- Saat mengunduh acara dari halaman Riwayat acara di CloudTrail konsol, Anda dapat mengunduh hingga 200.000 acara dalam satu file. Jika Anda mencapai batas acara 200.000, CloudTrail konsol akan memberikan opsi untuk mengunduh file tambahan.
- Riwayat acara tidak menyediakan agregasi acara tingkat organisasi. Untuk merekam peristiwa di seluruh organisasi Anda, buat penyimpanan atau jejak data acara organisasi.
- Pencarian riwayat peristiwa terbatas pada satu Akun AWS, hanya menampilkan peristiwa dari satu Wilayah AWS, dan tidak dapat menanyakan beberapa atribut. Anda hanya dapat menerapkan satu filter atribut dan filter rentang waktu.

  Anda dapat membuat penyimpanan data acara CloudTrail Lake untuk kueri di beberapa atribut dan Wilayah AWS. Anda juga dapat melakukan kueri di beberapa Akun AWS dalam suatu AWS Organizations organisasi. Di CloudTrail Lake, Anda dapat menanyakan beberapa jenis peristiwa, termasuk peristiwa manajemen, peristiwa data, peristiwa Wawasan, item AWS Config konfigurasi, bukti Audit Manager, dan AWS non-peristiwa. CloudTrail Kueri danau menawarkan tampilan acara yang lebih dalam dan lebih dapat disesuaikan daripada pencarian kunci dan nilai sederhana di halaman riwayat Acara, atau dengan menjalankan. `LookupEvents` Untuk informasi selengkapnya, lihat Bekerja dengan AWS CloudTrail Danau dan Membuat penyimpanan data acara untuk CloudTrail acara dengan konsol.
- Anda tidak dapat mengecualikan AWS KMS atau peristiwa Amazon RDS Data API dari riwayat peristiwa; pengaturan yang Anda terapkan ke penyimpanan data jejak atau peristiwa tidak berlaku untuk riwayat peristiwa.

Melihat acara manajemen terbaru dengan konsol

Anda dapat menggunakan halaman Riwayat acara di CloudTrail konsol untuk melihat 90 hari terakhir acara manajemen dalam file Wilayah AWS. Anda juga dapat mengunduh file dengan informasi tersebut, atau subset informasi berdasarkan filter dan rentang waktu yang Anda pilih. Anda dapat menyesuaikan tampilan riwayat Acara dengan memilih berapa banyak acara yang akan ditampilkan di setiap halaman dan memilih kolom mana yang akan ditampilkan di konsol. Anda juga dapat mencari dan memfilter peristiwa berdasarkan jenis sumber daya yang tersedia untuk layanan tertentu. Anda dapat memilih hingga lima acara dalam riwayat Acara dan membandingkan detailnya secara berdampingan.

Riwayat peristiwa tidak menampilkan peristiwa data. Untuk melihat peristiwa data, buat penyimpanan data acara atau jejak.

Setelah 90 hari, peristiwa tidak lagi ditampilkan dalam sejarah peristiwa. Anda tidak dapat menghapus peristiwa secara manual dari riwayat acara.

Anda dapat mempelajari lebih lanjut tentang cara CloudTrail mencatat peristiwa untuk layanan tertentu dengan berkonsultasi dengan dokumentasi untuk layanan tersebut. Untuk informasi selengkapnya, lihat AWS topik layanan untuk CloudTrail.

> **Note**
>
> Untuk catatan aktivitas dan acara yang sedang berlangsung selama 90 hari, buat penyimpanan data acara atau jejak.

Untuk melihat Riwayat acara

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa. Anda melihat daftar acara yang difilter, dengan acara terbaru ditampilkan terlebih dahulu. Filter default untuk acara adalah Read only, disetel ke false. Anda dapat menghapus filter itu dengan memilih X di sebelah kanan filter.
3. Anda dapat memfilter peristiwa pada satu atribut, yang dapat Anda pilih dari daftar drop-down. Untuk memfilter atribut, pilih atribut dari daftar drop-down dan masukkan nilai penuh untuk atribut tersebut. Misalnya, untuk melihat semua peristiwa login konsol, pilih Filter nama acara, dan

tentukan ConsoleLogin. Atau, untuk melihat peristiwa manajemen S3 terbaru, pilih filter sumber acara, dan tentukan`s3.amazonaws.com`.

4. Untuk melihat acara manajemen tertentu, pilih nama acara. Pada halaman detail acara, Anda dapat melihat detail tentang acara, melihat sumber daya yang direferensikan, dan melihat catatan acara.
5. Untuk membandingkan peristiwa, pilih hingga lima peristiwa dengan mengisi kotak centang di margin kiri tabel Riwayat acara. Anda dapat melihat detail untuk acara yang dipilih secara berdampingan di tabel Bandingkan detail acara.
6. Anda dapat menyimpan riwayat acara dengan mengunduhnya sebagai file dalam format CSV atau JSON. Mengunduh riwayat acara Anda dapat memakan waktu beberapa menit.

Daftar Isi

- Menavigasi antar halaman
- Menyesuaikan tampilan
- Acara penyaringan CloudTrail
- Melihat detail untuk suatu acara
- Mengunduh acara
- Melihat sumber daya yang direferensikan dengan AWS Config

Menavigasi antar halaman

Anda dapat menavigasi antar halaman dalam riwayat Acara dengan memilih halaman yang ingin Anda lihat. Anda juga dapat melihat halaman berikutnya dan sebelumnya dalam riwayat Acara.

Pilih **<** untuk melihat halaman sebelumnya dari riwayat Acara.

Pilih **>** untuk melihat halaman berikutnya dari riwayat Acara.

Menyesuaikan tampilan

Anda dapat menyesuaikan tampilan Riwayat acara di CloudTrail konsol dengan memilih dari preferensi berikut.

- Ukuran halaman - Pilih apakah Anda ingin menampilkan 10, 25, atau 50 acara di setiap halaman.

- Bungkus garis - Bungkus teks sehingga Anda dapat melihat semua teks untuk setiap acara.
- Baris bergaris - Bayangkan setiap baris lainnya di tabel.
- Tampilan waktu acara - Pilih apakah akan menampilkan waktu acara di UTC atau zona waktu lokal.
- Pilih kolom yang terlihat - Pilih kolom mana yang akan ditampilkan. Secara default, kolom berikut ditampilkan:
  - Nama acara
  - Waktu acara
  - Nama pengguna
  - Sumber acara
  - Tipe sumber daya
  - Nama sumber daya

> **Note**
>
> Anda tidak dapat mengubah urutan kolom, atau menghapus peristiwa secara manual dari riwayat Acara.

Untuk menyesuaikan tampilan

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa.
3. Pilih ikon roda gigi.
4. Untuk ukuran Halaman, pilih jumlah acara yang akan ditampilkan di halaman.
5. Pilih Bungkus baris untuk melihat semua teks untuk setiap acara.
6. Pilih baris bergaris untuk menaungi setiap baris lainnya di tabel.
7. Untuk tampilan waktu Acara, pilih apakah akan menampilkan waktu acara di UTC atau zona waktu setempat. Secara default, UTC dipilih.
8. Di Pilih kolom yang terlihat, pilih kolom yang ingin Anda tampilkan. Matikan kolom yang tidak ingin Anda tampilkan.
9. Setelah selesai melakukan perubahan, pilih Konfirmasi.

Acara penyaringan CloudTrail

Tampilan default peristiwa dalam riwayat Acara menggunakan filter atribut untuk mengecualikan peristiwa hanya-baca dari daftar peristiwa yang ditampilkan. Filter atribut ini dinamai Read-only, dan disetel ke false. Anda dapat menghapus filter ini untuk menampilkan acara baca dan tulis. Untuk hanya melihat peristiwa Baca, Anda dapat mengubah nilai filter menjadi true. Anda juga dapat memfilter peristiwa berdasarkan atribut lain. Anda juga dapat memfilter berdasarkan rentang waktu.

> **Note**
>
> Anda hanya dapat menerapkan satu filter atribut dan filter rentang waktu. Anda tidak dapat menerapkan beberapa filter atribut.

AWS kunci akses

ID kunci AWS akses yang digunakan untuk menandatangani permintaan. Jika permintaan dibuat dengan kredenal keamanan sementara, ini adalah ID kunci akses dari kredenal sementara.

ID peristiwa

CloudTrail ID acara. Setiap acara memiliki ID unik.

Nama peristiwa

Nama peristiwa. Misalnya, Anda dapat memfilter pada peristiwa IAM, seperti`CreatePolicy`, atau peristiwa Amazon EC2, seperti. `RunInstances`

Sumber peristiwa

AWS Layanan tempat permintaan dibuat, seperti `iam.amazonaws.com` atau`s3.amazonaws.com`. Anda dapat menggulir daftar sumber acara setelah Anda memilih filter sumber acara.

Baca saja

Jenis acara yang dibaca. Acara dikategorikan sebagai acara baca atau acara tulis. Jika disetel ke false, acara baca tidak termasuk dalam daftar acara yang ditampilkan. Secara default, filter atribut ini diterapkan dan nilainya disetel ke false.

Nama sumber daya

Nama atau ID sumber daya yang direferensikan oleh acara. Misalnya, nama sumber daya mungkin “auto-scaling-test-group” untuk grup Auto Scaling atau “i-12345678910" untuk instans EC2.

Tipe sumber daya

Jenis sumber daya yang direferensikan oleh acara tersebut. Misalnya, jenis sumber daya dapat `Instance` untuk EC2 atau `DBInstance` untuk RDS. Jenis sumber daya bervariasi untuk setiap AWS layanan.

Rentang waktu

Rentang waktu di mana Anda ingin memfilter acara. Anda dapat memilih rentang Relatif atau rentang Absolut. Anda dapat memfilter acara selama 90 hari terakhir.

Nama pengguna

Identitas yang direferensikan oleh acara tersebut. Misalnya, ini bisa berupa pengguna, nama peran, atau peran layanan.

Jika tidak ada peristiwa yang dicatat untuk atribut atau waktu yang Anda pilih, daftar hasil kosong. Anda hanya dapat menerapkan satu filter atribut selain rentang waktu. Jika Anda memilih filter atribut yang berbeda, rentang waktu yang ditentukan akan dipertahankan.

Langkah-langkah berikut menjelaskan cara memfilter berdasarkan atribut.

Untuk memfilter berdasarkan atribut

1. Untuk memfilter hasil berdasarkan atribut, pilih atribut dari daftar drop-down atribut Pencarian, lalu ketik atau pilih nilai untuk atribut di kotak teks.
2. Untuk menghapus filter atribut, pilih X di sebelah kanan kotak filter atribut.

Langkah-langkah berikut menjelaskan cara memfilter berdasarkan tanggal dan waktu mulai dan berakhir.

Untuk memfilter berdasarkan tanggal dan waktu mulai dan berakhir

1. Untuk mempersempit rentang waktu acara yang ingin Anda lihat, pilih rentang waktu di bilah rentang waktu. Anda dapat memilih rentang Relatif atau rentang Absolut.

Pilih Rentang relatif untuk memilih dari nilai preset atau memilih rentang kustom. Nilai preset adalah 30 menit, 1 jam, 12 jam, atau 1 hari. Untuk menentukan rentang waktu kustom, pilih Kustom.

Pilih Rentang absolut untuk menentukan waktu mulai dan akhir tertentu. Anda juga dapat memilih antara zona waktu lokal atau UTC.

2. Untuk menghapus filter rentang waktu, pilih Hapus dan tutup di bilah rentang waktu.

Melihat detail untuk suatu acara

1. Pilih acara dalam daftar hasil untuk menampilkan detailnya.
2. Sumber daya yang direferensikan dalam acara ditampilkan di tabel referensi Sumber daya pada halaman detail acara.
3. Beberapa sumber daya yang direferensikan memiliki tautan. Pilih tautan untuk membuka konsol untuk sumber daya itu.
4. Gulir ke catatan acara di halaman detail untuk melihat catatan peristiwa JSON, juga disebut payload acara.
5. Pilih Riwayat acara di halaman breadcrumb untuk menutup halaman detail acara dan kembali ke Riwayat acara.

Mengunduh acara

Anda dapat mengunduh riwayat peristiwa yang direkam sebagai file dalam format CSV atau JSON. Anda dapat mengunduh hingga 200.000 acara dalam satu file. Jika Anda mencapai batas acara 200.000, CloudTrail konsol akan memberikan opsi untuk mengunduh file tambahan. Gunakan filter dan rentang waktu untuk mengurangi ukuran file yang Anda unduh.

> **Note**
>
> CloudTrail file riwayat peristiwa adalah file data yang berisi informasi (seperti nama sumber daya) yang dapat dikonfigurasi oleh pengguna individu. Beberapa data berpotensi ditafsirkan sebagai perintah dalam program yang digunakan untuk membaca dan menganalisis data ini (injeksi CSV). Misalnya, ketika CloudTrail peristiwa diekspor ke CSV dan diimpor ke program spreadsheet, program tersebut mungkin memperingatkan Anda tentang masalah keamanan.

Anda harus memilih untuk menonaktifkan konten ini untuk menjaga keamanan sistem Anda. Selalu nonaktifkan tautan atau makro dari file riwayat acara yang diunduh.

1. Tambahkan filter dan rentang waktu untuk acara dalam riwayat Acara yang ingin Anda unduh. Misalnya, Anda dapat menentukan nama acara`StartInstances`, dan menentukan rentang waktu untuk tiga hari terakhir aktivitas.
2. Pilih Unduh acara, lalu pilih Unduh sebagai CSV atau Unduh sebagai JSON. Pengunduhan segera dimulai.

   Note

   Unduhan Anda mungkin membutuhkan waktu untuk menyelesaikannya. Untuk hasil yang lebih cepat, sebelum Anda memulai proses pengunduhan, gunakan filter yang lebih spesifik atau rentang waktu yang lebih pendek untuk mempersempit hasil. Anda dapat membatalkan unduhan. Jika Anda membatalkan unduhan, unduhan sebagian termasuk hanya beberapa data peristiwa mungkin ada di komputer lokal Anda. Untuk mengunduh riwayat acara lengkap, mulai ulang unduhan.
3. Setelah unduhan Anda selesai, buka file untuk melihat peristiwa yang Anda tentukan.
4. Untuk membatalkan unduhan, pilih Batalkan, lalu konfirmasikan dengan memilih Batalkan unduhan. Jika Anda perlu memulai ulang unduhan, tunggu hingga unduhan sebelumnya selesai dibatalkan.

Melihat sumber daya yang direferensikan dengan AWS Config

AWS Config mencatat detail konfigurasi, hubungan, dan perubahan pada AWS sumber daya Anda.

Pada panel Resources direferensikan, pilih kolom timeline AWS Config sumber daya untuk melihat sumber daya di konsol.



AWS Config

Jika



ikon berwarna abu-abu, AWS Config tidak dihidupkan, atau tidak merekam jenis sumber daya.

Pilih ikon untuk pergi ke AWS Config konsol untuk mengaktifkan layanan atau mulai merekam jenis sumber daya itu. Untuk informasi selengkapnya, lihat Mengatur AWS Config Menggunakan Konsol di Panduan AWS Config Pengembang.

Jika Tautan tidak tersedia muncul di kolom, sumber daya tidak dapat dilihat karena salah satu alasan berikut:

- AWS Config tidak mendukung jenis sumber daya. Untuk informasi selengkapnya, lihat Sumber Daya yang Didukung, Item Konfigurasi, dan Hubungan di Panduan AWS Config Pengembang.
- AWS Config baru-baru ini menambahkan dukungan untuk jenis sumber daya, tetapi belum tersedia dari CloudTrail konsol. Anda dapat mencari sumber daya di AWS Config konsol untuk melihat garis waktu sumber daya.
- Sumber daya dimiliki oleh orang lain Akun AWS.
- Sumber daya dimiliki oleh yang lain Layanan AWS, seperti kebijakan IAM yang dikelola.
- Sumber daya dibuat dan kemudian dihapus segera.
- Sumber daya baru-baru ini dibuat atau diperbarui.

Untuk memberi pengguna izin hanya-baca untuk melihat sumber daya di AWS Config konsol, lihat. Memberikan izin untuk melihat AWS Config informasi tentang CloudTrail konsol

Untuk informasi selengkapnya AWS Config, lihat Panduan AWS Config Pengembang.

Melihat acara manajemen terbaru dengan AWS CLI

Anda dapat mencari acara CloudTrail manajemen selama 90 hari terakhir untuk saat ini Wilayah AWS menggunakan aws cloudtrail lookup-events perintah. aws cloudtrail lookup-eventsPerintah menunjukkan peristiwa di Wilayah AWS mana mereka terjadi.

Lookup mendukung atribut berikut untuk acara manajemen:

- AWS kunci akses
- ID peristiwa
- Nama peristiwa
- Sumber peristiwa
- Baca saja

- Nama sumber daya
- Tipe sumber daya
- Nama pengguna

Semua atribut adalah opsional.

`lookup-events`Perintah ini mencakup opsi berikut:

- `--max-items`*`<integer>`*— Jumlah total item yang akan dikembalikan dalam output perintah. Jika jumlah total item yang tersedia lebih dari nilai yang ditentukan, a `NextToken` disediakan dalam output perintah. Untuk melanjutkan pagination, berikan `NextToken` nilai dalam argumen starting-token dari perintah sub- sequent. Jangan gunakan elemen `NextToken` respons langsung di luar AWS CLI.
- `--start-time`*`<timestamp>`*- Menentukan bahwa hanya peristiwa yang terjadi setelah atau pada waktu yang ditentukan dikembalikan. Jika waktu mulai yang ditentukan adalah setelah waktu akhir yang ditentukan, kesalahan dikembalikan.
- `--lookup-attributes`*`<integer>`*— Berisi daftar atribut pencarian. Saat ini daftar hanya dapat berisi satu item.
- `--generate-cli-skeleton`*`<string>`*— Mencetak kerangka JSON ke output standar tanpa mengirim permintaan API. Jika diberikan tanpa nilai atau input nilai, mencetak input sampel JSON yang dapat digunakan sebagai argumen untuk`--cli-input-json`. Demikian pula, jika diberikan yaml-input itu akan mencetak input sampel YAMAL yang dapat digunakan dengan. `--cli-input-yaml` Jika dilengkapi dengan output nilai, itu memvalidasi input perintah dan mengembalikan sampel output JSON untuk perintah itu. Kerangka JSON yang dihasilkan tidak stabil antara versi AWS CLI dan tidak ada jaminan kompatibilitas mundur dalam kerangka JSON yang dihasilkan.
- `--cli-input-json`*`<string>`*— Membaca argumen dari string JSON yang disediakan. String JSON mengikuti format yang disediakan oleh `--generate-cli-skeleton` parameter. Jika argumen lain disediakan pada baris perintah, nilai-nilai tersebut akan menggantikan nilai yang disediakan JSON. Tidak mungkin untuk meneruskan nilai biner arbitrer menggunakan nilai yang disediakan JSON karena string akan diambil secara harfiah. Ini mungkin tidak ditentukan bersama dengan `--cli-input-yaml` parameter.

Untuk informasi umum tentang penggunaan Antarmuka Baris AWS Perintah, lihat Panduan AWS Command Line Interface Pengguna.

Daftar Isi

- Prasyarat
- Mendapatkan bantuan baris perintah
- Mencari acara
- Menentukan jumlah acara untuk kembali
- Mencari acara berdasarkan rentang waktu
- Mencari acara berdasarkan atribut
  - Contoh pencarian atribut
- Menentukan halaman hasil berikutnya
- Mendapatkan masukan JSON dari sebuah file
- Bidang keluaran pencarian

Prasyarat

- Untuk menjalankan AWS CLI perintah, Anda harus menginstal AWS CLI. Untuk informasi, lihat Memulai dengan AWS CLI.
- Pastikan AWS CLI versi Anda lebih besar dari 1.6.6. Untuk memverifikasi versi CLI, jalankan aws --version pada baris perintah.
- Untuk mengatur akun, Wilayah AWS, dan format output default untuk AWS CLI sesi, gunakan aws configure perintah. Untuk informasi selengkapnya, lihat Mengonfigurasi Antarmuka Baris AWS Perintah.

> **Note**
>
> CloudTrail AWS CLI Perintahnya peka huruf besar/kecil.

Mendapatkan bantuan baris perintah

Untuk melihat bantuan baris perintah`lookup-events`, ketik perintah berikut:

```
aws cloudtrail lookup-events help
```

Mencari acara

> **Important**
>
> Tingkat permintaan pencarian dibatasi hingga dua per detik, per akun, per Wilayah. Jika batas ini terlampaui, kesalahan pelambatan terjadi.

Untuk melihat sepuluh peristiwa terbaru, ketik perintah berikut:

```
aws cloudtrail lookup-events --max-items 10
```

Peristiwa yang dikembalikan terlihat mirip dengan contoh fiktif berikut, yang telah diformat agar mudah dibaca:

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
```

```
                \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                \"eventType\":\"AwsApiCall\",
                \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```

Untuk penjelasan tentang bidang terkait pencarian di output, lihat bagian Bidang keluaran pencarian nanti dalam dokumen ini. Untuk penjelasan tentang bidang dalam CloudTrail acara tersebut, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

Menentukan jumlah acara untuk kembali

Untuk menentukan jumlah acara yang akan dikembalikan, ketik perintah berikut:

```
aws cloudtrail lookup-events --max-items <integer>
```

Nilai yang mungkin adalah 1 hingga 50. Contoh berikut mengembalikan satu peristiwa.

```
aws cloudtrail lookup-events --max-items 1
```

Mencari acara berdasarkan rentang waktu

Acara dari 90 hari terakhir tersedia untuk pencarian. Untuk menentukan rentang waktu, ketik perintah berikut:

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *`<timestamp>`*menentukan, dalam UTC, bahwa hanya peristiwa yang terjadi setelah atau pada waktu yang ditentukan dikembalikan. Jika waktu mulai yang ditentukan adalah setelah waktu akhir yang ditentukan, kesalahan dikembalikan.

`--end-time` *`<timestamp>`*menentukan, dalam UTC, bahwa hanya peristiwa yang terjadi sebelum atau pada waktu yang ditentukan dikembalikan. Jika waktu akhir yang ditentukan sebelum waktu mulai yang ditentukan, kesalahan dikembalikan.

Waktu mulai default adalah tanggal paling awal bahwa data tersedia dalam 90 hari terakhir. Waktu akhir default adalah waktu peristiwa yang terjadi paling dekat dengan waktu saat ini.

Semua stempel waktu ditampilkan di UTC.

Mencari acara berdasarkan atribut

Untuk memfilter berdasarkan atribut, ketik perintah berikut:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Anda dapat menentukan hanya satu key/value pasangan atribut untuk setiap lookup-events perintah. Berikut ini adalah nilai yang valid untuk`AttributeKey`. Nama nilai peka huruf besar/kecil.

- `AccessKeyId`
- `EventId`
- `EventName`
- `EventSource`
- `ReadOnly`
- `ResourceName`
- `ResourceType`
- `Username`

Panjang maksimum untuk `AttributeValue` adalah 2000 karakter. Karakter berikut (_", ", , ',\ \n') dihitung sebagai dua karakter menuju batas 2000 karakter.

Contoh pencarian atribut

Contoh perintah berikut mengembalikan peristiwa di mana nilai `AccessKeyId` adalah`AKIAIOSFODNN7EXAMPLE`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

Contoh perintah berikut mengembalikan acara untuk yang ditentukan CloudTrail`EventId`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Contoh perintah berikut mengembalikan peristiwa di mana nilai `EventName` adalah`RunInstances`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

Contoh perintah berikut mengembalikan peristiwa di mana nilai `EventSource` adalah`iam.amazonaws.com`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

Contoh perintah berikut mengembalikan acara tulis. Ini tidak termasuk acara baca seperti `GetBucketLocation` dan`DescribeStream`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

Contoh perintah berikut mengembalikan peristiwa di mana nilai `ResourceName` adalah`CloudTrail_CloudWatchLogs_Role`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

Contoh perintah berikut mengembalikan peristiwa di mana nilai `ResourceType` adalah`AWS::S3::Bucket`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

Contoh perintah berikut mengembalikan peristiwa di mana nilai `Username` adalah`root`.

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Menentukan halaman hasil berikutnya

Untuk mendapatkan halaman hasil berikutnya dari `lookup-events` perintah, ketik perintah berikut:

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

dimana nilai untuk *<token>* diambil dari bidang pertama dari output dari perintah sebelumnya.

Saat Anda menggunakan `--next-token` perintah, Anda harus menggunakan parameter yang sama seperti pada perintah sebelumnya. Misalnya, Anda menjalankan perintah berikut:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

Untuk mendapatkan halaman hasil berikutnya, perintah Anda berikutnya akan terlihat seperti ini:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

Mendapatkan masukan JSON dari sebuah file

AWS CLI Untuk beberapa AWS layanan memiliki dua parameter, `--generate-cli-skeleton` dan`--cli-input-json`, yang dapat Anda gunakan untuk menghasilkan template JSON yang dapat Anda modifikasi dan gunakan sebagai input ke `--cli-input-json` parameter. Bagian ini menjelaskan cara menggunakan parameter ini dengan`aws cloudtrail lookup-events`. Untuk informasi lebih umum, lihat AWS CLI kerangka dan file input.

Untuk mencari CloudTrail acara dengan mendapatkan input JSON dari file

1. Buat template input untuk digunakan `lookup-events` dengan mengarahkan `--generate-cli-skeleton` output ke file, seperti pada contoh berikut.

   ```
   aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
   ```

   File template yang dihasilkan (dalam hal ini, LookupEvents .txt) terlihat seperti ini:

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
       ],
       "StartTime": null,
   ```

```
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Gunakan editor teks untuk memodifikasi JSON sesuai kebutuhan. Masukan JSON harus berisi hanya nilai-nilai yang ditentukan.

> **Important**
>
> Semua nilai kosong atau nol harus dihapus dari template sebelum Anda dapat menggunakannya.

Contoh berikut menentukan rentang waktu dan jumlah maksimum hasil untuk kembali.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Untuk menggunakan file yang diedit sebagai input, gunakan sintaks `--cli-input-json file://<filename>`, seperti pada contoh berikut:

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> Anda dapat menggunakan argumen lain pada baris perintah yang sama dengan`--cli-input-json`.

Bidang keluaran pencarian

Peristiwa

Daftar peristiwa pencarian berdasarkan atribut lookup dan rentang waktu yang ditentukan. Daftar acara diurutkan berdasarkan waktu, dengan acara terbaru terdaftar terlebih dahulu. Setiap

entri berisi informasi tentang permintaan pencarian dan menyertakan representasi string dari CloudTrail peristiwa yang diambil.

Entri berikut menjelaskan bidang di setiap acara pencarian.

CloudTrailEvent

Sebuah string JSON yang berisi representasi objek dari acara dikembalikan. Untuk informasi tentang masing-masing elemen yang dikembalikan, lihat Rekam Isi Tubuh.

EventId

String yang berisi GUID acara dikembalikan.

EventName

Sebuah string yang berisi nama acara dikembalikan.

EventSource

AWS Layanan yang diminta untuk dibuat.

EventTime

Tanggal dan waktu, dalam format waktu UNIX, acara.

Sumber Daya

Daftar sumber daya yang direferensikan oleh acara yang dikembalikan. Setiap entri sumber daya menentukan jenis sumber daya dan nama sumber daya.

ResourceName

String yang berisi nama sumber daya yang direferensikan oleh acara tersebut.

ResourceType

String yang berisi jenis sumber daya yang direferensikan oleh acara tersebut. Ketika jenis sumber daya tidak dapat ditentukan, null dikembalikan.

Nama Pengguna

String yang berisi nama pengguna akun untuk acara yang dikembalikan.

NextToken

Sebuah string untuk mendapatkan halaman berikutnya dari hasil dari `lookup-events` perintah sebelumnya. Untuk menggunakan token, parameternya harus sama dengan yang ada di

perintah asli. Jika tidak ada `NextToken` entri yang muncul di output, tidak ada lagi hasil untuk dikembalikan.

Bekerja dengan CloudTrail Wawasan

AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan menanggapi aktivitas tidak biasa yang terkait dengan tingkat panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen dan data. CloudTrail Insights menganalisis peristiwa manajemen dan data Anda sebelumnya untuk menetapkan pola normal tingkat panggilan API dan tingkat kesalahan API, juga disebut baseline. CloudTrail kemudian menghasilkan peristiwa Wawasan ketika tingkat panggilan API saat ini atau tingkat kesalahan menyimpang dari baseline.

Anda dapat mengumpulkan dua jenis Wawasan, masing-masing untuk manajemen dan peristiwa data.

Wawasan acara manajemen

- Tingkat panggilan API — Pengukuran panggilan API manajemen khusus tulis yang terjadi per menit terhadap volume panggilan API dasar. Untuk mencatat peristiwa Insights pada tingkat panggilan API untuk peristiwa manajemen, penyimpanan data jejak atau peristiwa harus mengaktifkan Wawasan dan peristiwa `write` manajemen log.
- Tingkat kesalahan API — Pengukuran panggilan API manajemen yang menghasilkan kode kesalahan. Kesalahan ditampilkan jika panggilan API tidak berhasil. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, penyimpanan data jejak atau peristiwa harus mengaktifkan Wawasan dan log `read` atau peristiwa `write` manajemen, atau keduanya `read` dan peristiwa `write` manajemen.

Data peristiwa Wawasan

- Tingkat panggilan API — Pengukuran panggilan API data yang terjadi per menit terhadap volume panggilan API dasar. Untuk mencatat peristiwa Insights pada tingkat panggilan API, jejak harus mengaktifkan Insights dan mencatat peristiwa data.
- Tingkat kesalahan API — Pengukuran panggilan API data yang menghasilkan kode kesalahan. Kesalahan ditampilkan jika panggilan API tidak berhasil. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mengaktifkan Wawasan dan log `read` atau peristiwa `write` data, atau keduanya `read` dan peristiwa `write` data.

> **Note**
>
> Peristiwa wawasan tentang peristiwa data hanya didukung di jalur dan bukan di penyimpanan data peristiwa.

CloudTrail Wawasan menganalisis peristiwa manajemen dan data yang terjadi di setiap Wilayah dan menghasilkan peristiwa Wawasan ketika aktivitas tidak biasa terdeteksi yang menyimpang dari baseline. Peristiwa CloudTrail Wawasan dihasilkan di Wilayah yang sama dengan manajemen pendukungnya atau peristiwa data yang dihasilkan.

Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika mengaktifkan Wawasan peristiwa manajemen untuk penyimpanan data jalur dan peristiwa, serta Wawasan peristiwa data. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Topik

- Biaya untuk acara Insights
- Penyampaian acara Insights
- Pencatatan peristiwa Wawasan dengan CloudTrail konsol
- Pencatatan peristiwa Wawasan dengan AWS CLI
- Melihat acara Wawasan untuk jalur
- Melihat peristiwa Wawasan untuk penyimpanan data acara

Biaya untuk acara Insights

> **Note**
>
> Peristiwa wawasan tentang peristiwa data hanya didukung di jalur.

Saat Anda mengaktifkan peristiwa Wawasan di trek atau penyimpanan data peristiwa yang ada, CloudTrail analisis 28 hari terakhir dari manajemen dan peristiwa data yang dikumpulkan oleh jejak atau penyimpanan data peristiwa untuk menetapkan dasar aktivitas normal. Setelah garis dasar awal dibuat, garis dasar dihitung ulang setiap hari pada data 28 hari terakhir. Tidak ada CloudTrail biaya untuk analisis baseline.

Setelah analisis dasar, Anda dikenakan CloudTrail biaya untuk setiap peristiwa manajemen dan data masa depan yang dianalisis oleh CloudTrail. Anda dikenakan biaya berdasarkan jumlah peristiwa manajemen dan data yang dianalisis untuk jenis Wawasan yang diaktifkan.

Jika Anda memilih untuk mencatat tingkat panggilan API dan jenis Insights tingkat kesalahan API untuk peristiwa manajemen untuk penyimpanan data jejak atau peristiwa yang mencatat `read` dan peristiwa `write` manajemen, jumlah total peristiwa yang dianalisis akan lebih besar daripada jumlah total peristiwa manajemen yang direkam. Ini karena CloudTrail akan menganalisis peristiwa manajemen khusus tulis dua kali, sekali untuk menghitung tingkat panggilan API dan sekali lagi untuk menentukan tingkat kesalahan API. Peristiwa manajemen read-only akan dianalisis sekali untuk menghitung tingkat kesalahan API.

Demikian pula, jika Anda memilih untuk mencatat tingkat panggilan API dan jenis Insights tingkat kesalahan API untuk peristiwa data untuk jejak yang mencatat `read` dan peristiwa `write` data, jumlah total peristiwa yang dianalisis akan lebih besar daripada jumlah total peristiwa data yang direkam. Ini karena CloudTrail akan menganalisis semua peristiwa data dua kali, sekali untuk menghitung tingkat panggilan API dan sekali lagi untuk menentukan tingkat kesalahan API.

Anda dapat mengidentifikasi biaya untuk Wawasan untuk peristiwa manajemen dan data pada tagihan Anda dengan mencari masing-masing jenis `InsightsEvents` dan jenis `DataInsightsEvents` penggunaan. Untuk informasi selengkapnya, lihat Melihat CloudTrail biaya dan penggunaan Anda dengan AWS Cost Explorer.

Anda akan dikenakan biaya Insights terpisah untuk trek dan penyimpanan data acara, dan acara data terpisah Wawasan untuk jalur. Untuk informasi lebih lanjut tentang harga, lihat AWS CloudTrail Harga.

Contoh 1 — Aktifkan Wawasan tentang peristiwa manajemen untuk tingkat panggilan API dan tingkat kesalahan API pada jejak

Dalam contoh pertama ini, Anda mengaktifkan Wawasan pada peristiwa manajemen pencatatan jejak dan memilih untuk mengumpulkan kedua jenis Wawasan. Jejak dalam contoh ini mencatat keduanya `read` dan peristiwa `write` manajemen.

- CloudTrail menganalisis peristiwa manajemen yang dicatat dalam 28 hari terakhir untuk membentuk baseline. Tidak ada CloudTrail biaya untuk analisis.
- Setelah garis dasar dibuat, jejak mencatat 300.000 peristiwa manajemen, 270.000 di antaranya adalah acara `read` manajemen dan 30.000 adalah peristiwa `write` manajemen.

- Per `write` istiwa manajemen dianalisis dua kali, sekali untuk tingkat panggilan API dan sekali untuk tingkat kesalahan API (30.000 * 2 = 60.000).
- Per `read` istiwa manajemen dianalisis sekali untuk tingkat kesalahan API (270.000*1=270.000).
- Total peristiwa manajemen yang dianalisis adalah 330.000 (60.000 + 270.000). Anda akan dikenakan biaya untuk menganalisis 330.000 acara manajemen untuk jalur ini. Anda akan dikenakan biaya terpisah jika mengaktifkan Insights untuk jejak lain atau penyimpanan data acara.

Contoh 2 — Aktifkan Wawasan tentang peristiwa manajemen untuk dua jalur

Dalam contoh berikutnya, Anda mengaktifkan Wawasan pada dua peristiwa manajemen pencatatan jalur, jejak A dan jejak B. Anda memilih untuk mengaktifkan tingkat panggilan API Wawasan hanya pada jejak A dan Wawasan tingkat kesalahan API hanya pada jejak B. Baik log jalur `read` maupun peristiwa `write` manajemen.

- CloudTrail menganalisis peristiwa `write` manajemen yang dicatat dalam 28 hari terakhir untuk membentuk baseline. Tidak ada CloudTrail biaya untuk analisis.
- Setelah garis dasar dibuat, jejak mencatat 800.000 peristiwa manajemen, di mana 710.000 adalah `read` peristiwa dan 90.000 adalah peristiwa. `write`

  Untuk jejak A, analisis berikut terjadi:

  - Per `write` istiwa manajemen dianalisis sekali untuk tingkat panggilan API (90.000 * 1 = 90.000).
  - Per `read` istiwa manajemen tidak dianalisis, karena CloudTrail hanya menganalisis peristiwa `write` manajemen untuk Wawasan tingkat panggilan API.
  - Total peristiwa manajemen yang dianalisis adalah 90.000. Anda akan dikenakan biaya untuk menganalisis 90.000 acara manajemen untuk jalur A.

  Untuk jejak B, analisis berikut terjadi:

  - Per `write` istiwa manajemen dianalisis sekali untuk tingkat kesalahan API (90.000 * 1 = 90.000).
  - Per `read` istiwa manajemen dianalisis sekali untuk tingkat kesalahan API (710.000 *1=710.000).
  - Total peristiwa manajemen yang dianalisis adalah 800.000 (90.000 + 710.000). Anda akan dikenakan biaya untuk menganalisis 800.000 acara manajemen untuk jalur B.

Contoh 3 — Aktifkan Wawasan tentang peristiwa manajemen untuk tingkat panggilan API dan tingkat kesalahan API pada jejak dan penyimpanan data peristiwa

Dalam contoh ini, Anda mengaktifkan Insights untuk tingkat panggilan API dan tingkat kesalahan API pada peristiwa manajemen logging penyimpanan data jejak dan peristiwa. Penyimpanan data jejak dan peristiwa adalah pencatatan `read` dan pengel `write` olaan peristiwa. Anda akan dikenakan biaya untuk CloudTrail Wawasan untuk penyimpanan data jejak dan peristiwa secara terpisah saat Anda mengaktifkan Wawasan pada keduanya.

- CloudTrail menganalisis peristiwa manajemen yang dicatat dalam 28 hari terakhir untuk membentuk baseline. Tidak ada CloudTrail biaya untuk analisis.
- Setelah baseline dibuat, data jejak dan peristiwa menyimpan catatan 500.000 peristiwa manajemen, di mana 380.000 adalah peristiwa `read` manajemen dan 120.000 adalah peristiwa `write` manajemen.

  Untuk jejak, analisis berikut terjadi:

  - Per `write` istiwa manajemen dianalisis dua kali untuk jejak, sekali untuk tingkat panggilan API dan sekali untuk tingkat kesalahan API (120.000 * 2 = 240.000).
  - Per `read` istiwa manajemen dianalisis sekali untuk jejak tingkat kesalahan API (380,000 *1 = 380.000).
  - Total peristiwa manajemen yang dianalisis untuk jejak adalah 620.000 (240.000 + 380.000). Anda akan dikenakan biaya untuk menganalisis 620.000 acara manajemen untuk jalur tersebut.

  Untuk penyimpanan data peristiwa, analisis berikut terjadi:

  - Per `write` istiwa manajemen dianalisis dua kali untuk penyimpanan data peristiwa, sekali untuk tingkat panggilan API dan sekali untuk tingkat kesalahan API (120.000 * 2=240.000).
  - Per `read` istiwa manajemen dianalisis sekali untuk penyimpanan data peristiwa untuk tingkat kesalahan API (380,000 *1=380.000).
  - Total peristiwa manajemen yang dianalisis untuk penyimpanan data peristiwa adalah 620.000 (240.000 + 380.000). Anda akan dikenakan biaya untuk menganalisis 620.000 peristiwa manajemen untuk penyimpanan data acara.

Contoh 4 — Aktifkan peristiwa manajemen Wawasan dan peristiwa data Wawasan untuk tingkat panggilan API dan tingkat kesalahan API pada jejak

Dalam contoh terakhir ini, Anda mengaktifkan Wawasan tentang manajemen dan peristiwa data. Jejak dalam contoh ini adalah logging `read` dan `write` manajemen dan peristiwa data.

- CloudTrail menganalisis peristiwa manajemen dan data yang dicatat dalam 28 hari terakhir untuk membentuk baseline. Tidak ada CloudTrail biaya untuk analisis.
- Setelah garis dasar dibuat, jejak mencatat 300.000 peristiwa manajemen, 270.000 di antaranya adalah acara manajemen yang dibaca dan 30.000 adalah peristiwa manajemen tulis. Jejak juga mencatat 400.000 peristiwa data, 340.000 di antaranya adalah peristiwa data baca dan 60.000 adalah peristiwa data tulis.
  - Per `write` istiwa manajemen dianalisis dua kali, sekali untuk tingkat panggilan API dan sekali untuk tingkat kesalahan API (30.000 * 2 = 60.000). Per `read` istiwa manajemen dianalisis sekali untuk tingkat kesalahan API (270.000*1=270.000). Total peristiwa manajemen yang dianalisis adalah 330.000 (60.000 + 270.000).
  - Per `read` istiwa dan `write` data dianalisis dua kali, sekali untuk tingkat panggilan API dan sekali untuk tingkat kesalahan API (400.000* 2). Total peristiwa data yang dianalisis adalah 800.000.
  - Anda akan dikenakan biaya untuk menganalisis 1.130.000 peristiwa manajemen dan data untuk jejak ini.

Penyampaian acara Insights

Tidak seperti jenis peristiwa lain yang CloudTrail menangkap, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda yang berbeda secara signifikan dari pola penggunaan tipikal akun.

Tempat CloudTrail pengiriman acara dan berapa lama waktu yang dibutuhkan untuk menerima peristiwa Insights berbeda antara jalur dan penyimpanan data acara.

> **Note**
>
> Peristiwa wawasan tentang peristiwa data hanya didukung di jalur.

Pengiriman acara wawasan untuk jalur

Jika Anda telah mengaktifkan peristiwa Insights di trek dan CloudTrail mendeteksi aktivitas yang tidak biasa CloudTrail , kirimkan peristiwa Insights ke `/CloudTrail-Insight` folder di bucket S3 tujuan yang dipilih untuk jejak Anda. Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya pada jejak, CloudTrail mungkin diperlukan waktu hingga 36 jam untuk mulai mengirimkan peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Jika Anda menonaktifkan pencatatan peristiwa Insights pada jejak dan kemudian mengaktifkan kembali peristiwa Insights, atau menghentikan dan memulai ulang pencatatan pada jejak, mungkin diperlukan waktu hingga 36 jam CloudTrail untuk memulai ulang pengiriman peristiwa Insights, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Pengiriman peristiwa wawasan untuk penyimpanan data acara

Jika Anda telah mengaktifkan peristiwa Wawasan di penyimpanan data peristiwa sumber, CloudTrail mengirimkan peristiwa Wawasan ke penyimpanan data peristiwa tujuan. Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya di penyimpanan data peristiwa sumber, CloudTrail mungkin diperlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Wawasan ke penyimpanan data peristiwa tujuan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Jika Anda menonaktifkan pencatatan peristiwa Insights di penyimpanan data peristiwa sumber dan kemudian mengaktifkan kembali peristiwa Insights, atau menghentikan dan memulai ulang penyerapan peristiwa di penyimpanan data peristiwa sumber, mungkin diperlukan waktu hingga 7 hari CloudTrail untuk memulai ulang pengiriman peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut. Biaya tambahan berlaku untuk menelan acara Insights di CloudTrail Lake. Anda akan dikenakan biaya terpisah jika mengaktifkan Insights untuk trek dan penyimpanan data acara. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Pencatatan peristiwa Wawasan dengan CloudTrail konsol

Bagian ini menjelaskan cara mengaktifkan peristiwa Wawasan di trek atau penyimpanan data peristiwa yang ada menggunakan CloudTrail konsol.

Untuk informasi selengkapnya tentang cara membuat jejak baru untuk mencatat peristiwa Wawasan, lihatMembuat jejak dengan konsol.

Untuk informasi selengkapnya tentang cara membuat penyimpanan data peristiwa baru untuk mengumpulkan peristiwa Wawasan, lihatMembuat penyimpanan data acara untuk acara Insights dengan konsol.

Topik

- Mengaktifkan CloudTrail Wawasan pada jejak yang ada dengan konsol
- Mengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang ada dengan konsol

Mengaktifkan CloudTrail Wawasan pada jejak yang ada dengan konsol

Gunakan prosedur berikut untuk mengaktifkan CloudTrail Wawasan pada jejak yang ada.

1. Di panel navigasi kiri CloudTrail konsol, buka halaman Trails, dan pilih nama jejak.
2. Di acara Wawasan, pilih Edit.

> **Note**
>
> Biaya tambahan berlaku untuk mencatat peristiwa Insights. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

3. Di Jenis acara, pilih peristiwa Wawasan.
4. Dalam peristiwa Insights pilih peristiwa manajemen atau peristiwa data
5. Di bawah Jenis wawasan, pilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Jejak Anda harus mencatat manajemen Tulis atau peristiwa data untuk mencatat peristiwa Insights untuk tingkat panggilan API. Jejak Anda harus mencatat manajemen Baca atau Tulis atau data untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.
6. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

CloudTrail mungkin memerlukan waktu hingga 36 jam untuk mulai menyampaikan peristiwa Wawasan setelah Anda mengaktifkan peristiwa Wawasan di jejak, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Mengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang ada dengan konsol

Gunakan prosedur berikut untuk mengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang ada.

Biaya tambahan berlaku untuk menelan acara Insights di CloudTrail Lake. Anda akan dikenakan biaya terpisah jika mengaktifkan Insights untuk trek dan penyimpanan data acara. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

> **Note**
>
> Anda hanya dapat mengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang berisi peristiwa CloudTrail manajemen. Anda tidak dapat mengaktifkan CloudTrail Wawasan pada jenis penyimpanan data peristiwa lainnya.

1. Di panel navigasi kiri CloudTrail konsol, di bawah Lake, pilih Peny impanan data acara.
2. Pilih nama penyimpanan data acara.
3. Di Acara manajemen, pilih Edit.
4. Pilih Aktifkan penangkapan peristiwa Wawasan.
5. Pilih toko acara tujuan yang akan mengumpulkan acara Insights. Penyimpanan data acara tujuan akan mengumpulkan peristiwa Wawasan berdasarkan aktivitas acara manajemen di penyimpanan data acara ini. Untuk informasi tentang cara membuat penyimpanan data acara tujuan, lihatUntuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.
6. Pilih jenis Wawasan. Anda dapat memilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Anda harus mencatat peristiwa manajemen T ulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau T ulis untuk mencatat peristiwa Insights untuk tingkat kesalahan API.
7. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

CloudTrail dapat memakan waktu hingga 7 hari untuk mulai mengirimkan acara Insights, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Pencatatan peristiwa Wawasan dengan AWS CLI

Anda dapat mengonfigurasi trek dan penyimpanan data peristiwa untuk mencatat peristiwa Wawasan menggunakan AWS CLI.

> **Note**
>
> Untuk Wawasan peristiwa Manajemen: Untuk mencatat peristiwa Insights pada tingkat panggilan API, penyimpanan data jejak atau peristiwa harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak atau penyimpanan data peristiwa harus mencatat `read` atau `write` mengelola.

Untuk Wawasan peristiwa Data: Untuk mencatat peristiwa Insights pada tingkat panggilan API atau tingkat kesalahan API, jejak harus mencatat `read` atau peristiwa `write` data.

Topik

- Pencatatan peristiwa Wawasan untuk jejak menggunakan AWS CLI
- Pencatatan peristiwa Wawasan untuk penyimpanan data peristiwa menggunakan AWS CLI

Pencatatan peristiwa Wawasan untuk jejak menggunakan AWS CLI

Untuk mengembalikan pemilih Insights saat ini untuk jejak, jalankan `get-insight-selectors` perintah.

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

Contoh respons berikut menunjukkan pemilih Wawasan untuk jejak bernama`insights-trail`.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/insights-trail",
    "InsightSelectors": [
        {
            "InsightType": "ApiCallRateInsight",
            "EventCategories": [
                "Management",
                "Data"
            ]
        },
        {
            "InsightType": "ApiErrorRateInsight",
            "EventCategories": [
                "Management",
                "Data"
            ]
        }
    ]
}
```

Jika jejak tidak mengaktifkan Insights, get-insight-selectors perintah mengembalikan pesan kesalahan berikut: “Terjadi kesalahan (InsightNotEnabledException) saat memanggil GetInsightSelectors

operasi: Trail arn:aws:cloudtrail:us-east- 1:123456789012: tidak mengaktifkan Insights. trail/trailName Edit pengaturan jejak untuk mengaktifkan Wawasan, lalu coba operasi lagi."

Untuk mengonfigurasi jejak Anda untuk mencatat peristiwa Insights, jalankan `put-insight-selectors` perintah. Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan peristiwa Wawasan. Nilai pemilih wawasan dapat berupa`ApiCallRateInsight`,`ApiErrorRateInsight`, atau keduanya. Masing-masing InsightType dapat diaktifkan untuk manajemen EventCategory atau data EventCategory atau keduanya.

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight", "EventCategories": ["Data"]},{"InsightType":
 "ApiErrorRateInsight", "EventCategories": ["Data", "Management"]}]'
```

Hasil berikut menunjukkan pemilih peristiwa Insights yang dikonfigurasi untuk jejak.

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight",
            "EventCategories": [
                "Data"
            ]
         },
         {
            "InsightType": "ApiCallRateInsight",
            "EventCategories": [
                "Data",
                "Management"
            ]
         }
      ]
 }
```

Pencatatan peristiwa Wawasan untuk penyimpanan data peristiwa menggunakan AWS CLI

Untuk mengaktifkan Wawasan pada penyimpanan data peristiwa, Anda harus memiliki penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen dan penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.

Untuk melihat apakah peristiwa Insights diaktifkan pada penyimpanan data peristiwa, jalankan get-insight-selectors perintah.

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Untuk melihat apakah penyimpanan data peristiwa dikonfigurasi untuk menerima peristiwa Insights atau peristiwa manajemen, jalankan get-event-data-store perintah.

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

Jika penyimpanan data peristiwa dikonfigurasi untuk menerima peristiwa Insights, itu `eventCategory` akan disetel ke`Insight`.

Prosedur berikut menunjukkan cara membuat penyimpanan data peristiwa tujuan dan sumber, lalu mengaktifkan peristiwa Wawasan.

1. Jalan aws cloudtrail create-event-data-store kan perintah untuk membuat penyimpanan data peristiwa tujuan yang mengumpulkan peristiwa Wawasan. Nilai untuk `eventCategory` harus `Insight`. Ganti *`retention-period-days`* dengan jumlah hari Anda ingin menyimpan acara di penyimpanan data acara Anda.

   Jika Anda masuk dengan akun manajemen untuk AWS Organizations organisasi, sertakan `--organization-enabled` parameter jika Anda ingin memberikan akses administrator yang didelegasikan ke penyimpanan data peristiwa.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
   ```

```
      "Name": "Select Insights events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["Insight"] }
        ]
    }
  ]'
```

Berikut ini adalah contoh respons.

```
{
    "Name": "insights-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

Anda akan menggunakan ARN (atau akhiran ID ARN) dari respons sebagai nilai untuk `--insights-destination` parameter pada langkah 3.

2. Jalan aws cloudtrail create-event-data-store kan perintah untuk membuat penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen. Secara default, data peristiwa menyimpan log semua peristiwa manajemen. Anda tidak perlu menentukan pemilih acara

lanjutan jika Anda ingin mencatat semua peristiwa manajemen. Ganti *retention-period-days* dengan jumlah hari Anda ingin menyimpan acara di penyimpanan data acara Anda. Jika Anda membuat penyimpanan data acara organisasi, sertakan `--organization-enabled` parameter.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Anda akan menggunakan ARN (atau akhiran ID ARN) dari respons sebagai nilai untuk `--event-data-store` parameter pada langkah 3.

3. Jalankan put-insight-selectors perintah untuk mengaktifkan peristiwa Insights. Nilai pemilih wawasan dapat berupa`ApiCallRateInsight`,`ApiErrorRateInsight`, atau keduanya.

Untuk `--event-data-store` parameter, tentukan ARN (atau akhiran ID ARN) dari penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen dan akan mengaktifkan Wawasan. Untuk `--insights-destination` parameter, tentukan ARN (atau akhiran ID ARN) dari penyimpanan data peristiwa tujuan yang akan mencatat peristiwa Insights.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Hasil berikut menunjukkan pemilih peristiwa Insights yang dikonfigurasi untuk penyimpanan data peristiwa.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya di penyimpanan data peristiwa, CloudTrail mungkin diperlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Melihat acara Wawasan untuk jalur

Bagian ini menjelaskan cara mencari jejak acara Insights selama 90 hari terakhir dengan CloudTrail Insights diaktifkan. Untuk informasi tentang cara melihat CloudTrail Wawasan untuk penyimpanan data acara, lihatMelihat dasbor Wawasan untuk penyimpanan data peristiwa.

Anda dapat melihat, memfilter, dan mengunduh 90 hari terakhir acara Insights untuk mendapatkan jejak dari halaman Wawasan di konsol.

Anda dapat mengambil 90 hari terakhir acara Insights secara terprogram:

- Untuk Trails mencatat peristiwa manajemen dengan menjalankan AWS CLI lookup-eventsperintah, atau operasi LookupEventsAPI.
- Untuk Trails mencatat peristiwa data dengan menjalankan AWS CLI list-insights-dataperintah, atau operasi ListInsightsDataAPI.

Untuk deskripsi bidang rekaman peristiwa Wawasan untuk jejak, lihat. CloudTrail merekam konten untuk acara Insights untuk jalur

> **Note**
>
> Halaman Insights dan AWS CLI `lookup-events` atau `list-insights-data` perintah hanya mencantumkan peristiwa Wawasan jika Anda telah mengaktifkan Wawasan pada jejak yang merupakan manajemen pencatatan atau peristiwa data. Untuk informasi tentang mengaktifkan Wawasan tentang jejak, lihat Mengaktifkan CloudTrail Wawasan pada jejak yang ada dengan konsol dan. Pencatatan peristiwa Wawasan untuk jejak menggunakan AWS CLI
>
> Untuk mencatat peristiwa Insights pada rasio panggilan API, jejak harus mencatat `write` manajemen atau peristiwa data. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mencatat `read` atau `write` mengelola atau peristiwa data.

Topik

- Melihat peristiwa Wawasan untuk jalur dengan konsol
- Melihat acara Wawasan untuk jalur dengan AWS CLI

Melihat peristiwa Wawasan untuk jalur dengan konsol

Bagian ini menjelaskan cara melihat, mencari, dan mengunduh acara Insights selama 90 hari terakhir untuk jejak dari halaman Wawasan di CloudTrail konsol. Untuk informasi tentang cara melihat CloudTrail Wawasan untuk penyimpanan data peristiwa, lihatMelihat dasbor Wawasan untuk penyimpanan data peristiwa.

Setelah peristiwa Insights dicatat untuk jejak, peristiwa tersebut ditampilkan di halaman Wawasan selama 90 hari. Anda tidak dapat menghapus peristiwa secara manual dari halaman Wawasan. Karena peristiwa Insights yang diaktifkan untuk jejak disimpan di bucket Amazon S3 yang dikonfigurasi untuk jejak tersebut, menghapus peristiwa Insights dari bucket akan menghapus peristiwa tersebut.

Anda dapat memantau log jejak Anda dan diberi tahu ketika peristiwa Wawasan tertentu terjadi dengan mengaktifkan CloudWatch Log. Untuk informasi selengkapnya, lihat Memantau File CloudTrail Log dengan CloudWatch Log Amazon.

> **Note**
>
> - CloudTrail Peristiwa wawasan harus diaktifkan di jejak Anda untuk melihat peristiwa Wawasan di konsol. Berikan waktu hingga 36 jam CloudTrail untuk menyampaikan peristiwa Insights pertama, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.
> - Untuk Wawasan peristiwa Manajemen: Untuk mencatat peristiwa Wawasan pada tingkat panggilan API, jejak harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mencatat `read` atau peristiwa `write` manajemen.
> - Untuk Wawasan peristiwa Data: Untuk mencatat peristiwa Insights pada tingkat panggilan API atau tingkat kesalahan API, jejak harus mencatat `read` atau peristiwa `write` data.

Untuk melihat acara Insights

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/home/.
2. Di panel navigasi, pilih Wawasan untuk melihat semua peristiwa Wawasan yang masuk ke akun Anda dalam 90 hari terakhir. Anda juga dapat melihat lima peristiwa Wawasan terbaru dari halaman Dasbor.
3. Pada halaman Wawasan, Anda dapat memilih tab Wawasan peristiwa manajemen atau Wawasan peristiwa data
4. Anda dapat memfilter peristiwa Wawasan berdasarkan sumber peristiwa, nama acara, atau ID peristiwa. Untuk informasi selengkapnya tentang memfilter peristiwa Wawasan, lihatMemfilter peristiwa Wawasan.

5. Anda dapat membatasi daftar lebih lanjut ke rentang Relatif atau Rentang Absolut.

Daftar Isi

- Memfilter peristiwa Wawasan
- Melihat detail acara Insights
- Memperbesar, menggeser, dan mengunduh grafik
- Ubah pengaturan rentang waktu grafik
- Mengunduh acara Insights

Memfilter peristiwa Wawasan

Secara default, peristiwa di halaman Wawasan ditampilkan dalam urutan kronologis terbalik berdasarkan waktu mulai acara.

Anda dapat memfilter daftar dengan memilih salah satu dari tiga atribut berikut:

Nama peristiwa

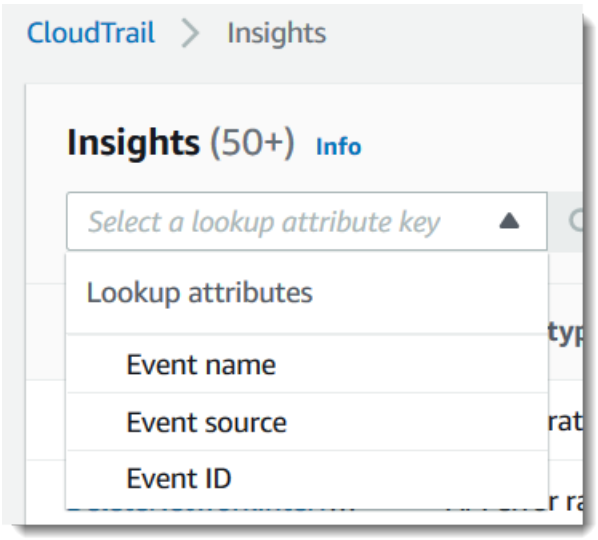
Nama acara, biasanya AWS API tempat tingkat aktivitas yang tidak biasa dicatat.

Sumber peristiwa

AWS Layanan tempat permintaan dibuat, seperti `iam.amazonaws.com` atau`s3.amazonaws.com`. Jika Anda memilih untuk memfilter berdasarkan sumber peristiwa, Anda dapat menggulir daftar sumber peristiwa.

ID peristiwa

ID acara Insights. ID peristiwa tidak ditampilkan di tabel halaman Wawasan, tetapi merupakan atribut yang dapat digunakan untuk memfilter peristiwa Wawasan. ID peristiwa manajemen atau peristiwa data yang dianalisis untuk menghasilkan peristiwa Wawasan berbeda dari ID peristiwa Insights.



Daftar berikut menjelaskan atribut acara, yang tidak dapat disaring:

Jenis wawasan

Jenis peristiwa CloudTrail Insights, yaitu tingkat panggilan API atau tingkat kesalahan API. Jenis wawasan tingkat panggilan API menganalisis pengelolaan khusus tulis atau panggilan API data yang digabungkan per menit terhadap volume panggilan API dasar. Jenis wawasan tingkat kesalahan API menganalisis manajemen atau panggilan API data yang menghasilkan kode kesalahan. Kesalahan ditampilkan jika panggilan API tidak berhasil.

Waktu mulai acara

Waktu mulai acara Insights, diukur sebagai menit pertama di mana aktivitas yang tidak biasa dicatat. Atribut ini ditampilkan dalam tabel Wawasan, tetapi Anda tidak dapat memfilter waktu mulai acara di konsol.

Rata-rata dasar

Baseline mewakili pola normal tingkat panggilan API atau aktivitas tingkat kesalahan, dihitung setiap hari. Rata-rata dasar adalah rata-rata garis dasar harian ini selama tujuh hari sebelum dimulainya acara Insights. Sementara periode ini umumnya tujuh hari, CloudTrail bulatkan periode perhitungan menjadi sejumlah hari, sehingga durasi dasar yang tepat mungkin sedikit berbeda.

Rata-rata wawasan

Jumlah rata-rata panggilan ke API, atau jumlah rata-rata kesalahan tertentu yang dikembalikan pada panggilan ke API, yang memicu peristiwa Insights. Rat CloudTrail a-rata Wawasan untuk acara awal adalah tingkat kejadian yang memicu peristiwa Wawasan. Biasanya, ini adalah menit pertama dari aktivitas yang tidak biasa. Rata-rata Wawasan untuk acara akhir adalah tingkat

kejadian selama durasi aktivitas yang tidak biasa, antara acara Insights awal dan acara Wawasan akhir.

Perubahan tarif

Perbedaan antara nilai rata-rata Baseline dan rata-rata Insight, diukur sebagai persentase. Misalnya, jika rata-rata dasar dari `AccessDenied` kesalahan yang terjadi adalah 1,0, dan rata-rata Insight adalah 3,0, perubahan tingkat adalah 300%. Perubahan tarif untuk rata-rata Insight yang melebihi rata-rata dasar menunjukkan panah atas di sebelah nilai. Jika peristiwa Wawasan dicatat karena aktivitas berada di bawah rata-rata dasar, perubahan Rate menampilkan panah bawah di sebelah persentase.

Jika tidak ada peristiwa yang dicatat untuk atribut atau waktu yang Anda pilih, daftar hasil akan kosong. Anda hanya dapat menerapkan satu filter atribut selain rentang waktu. Jika Anda memilih filter atribut yang berbeda, rentang waktu yang ditentukan akan dipertahankan.

Langkah-langkah berikut menjelaskan cara memfilter berdasarkan atribut.

Untuk memfilter berdasarkan atribut

1. Untuk memfilter hasil berdasarkan atribut, pilih atribut pencarian dari menu tarik-turun, lalu ketik atau pilih nilai di kotak Masukkan nilai pencarian.
2. Untuk menghapus filter atribut, pilih X di sebelah kanan kotak filter atribut.

Langkah-langkah berikut menjelaskan cara memfilter berdasarkan tanggal dan waktu mulai dan akhir.

Untuk memfilter berdasarkan tanggal dan waktu mulai dan akhir

1. Dari Filter berdasarkan tanggal dan waktu, pilih salah satu dari berikut ini:
   - Rentang absolut - Memungkinkan Anda memilih waktu tertentu. Lanjutkan ke langkah berikutnya.
   - Rentang relatif - Dipilih secara default. Memungkinkan Anda memilih periode waktu relatif terhadap waktu mulai acara Insights. Lanjutkan ke langkah 3.
2. Untuk mengatur rentang Absolute, lakukan hal berikut.
   a. Pilih hari yang Anda inginkan rentang waktu dimulai. Masukkan waktu mulai pada hari yang dipilih. Untuk memasukkan tanggal secara manual, ketik tanggal dalam format`yyyy/mm/dd`.

Waktu mulai dan akhir menggunakan jam 24 jam, dan nilai harus dalam format`hh:mm:ss`. Misalnya, untuk menunjukkan waktu mulai pukul 18:30, masukkan. **`18:30:00`**

b. Pilih tanggal akhir untuk rentang di kalender, atau tentukan tanggal dan waktu akhir di bawah kalender. Pilih Terapkan.

3. Untuk mengatur rentang Relatif, lakukan hal berikut.

a. Pilih periode waktu yang telah ditetapkan relatif terhadap waktu mulai acara Insights. Rentang waktu yang telah ditetapkan termasuk 30 menit, 1 jam, 12 jam, atau 1 hari. Untuk menentukan rentang waktu khusus, pilih K ustom.

b. Ketika Anda telah mengatur waktu relatif yang Anda inginkan, pilih Ter apkan.

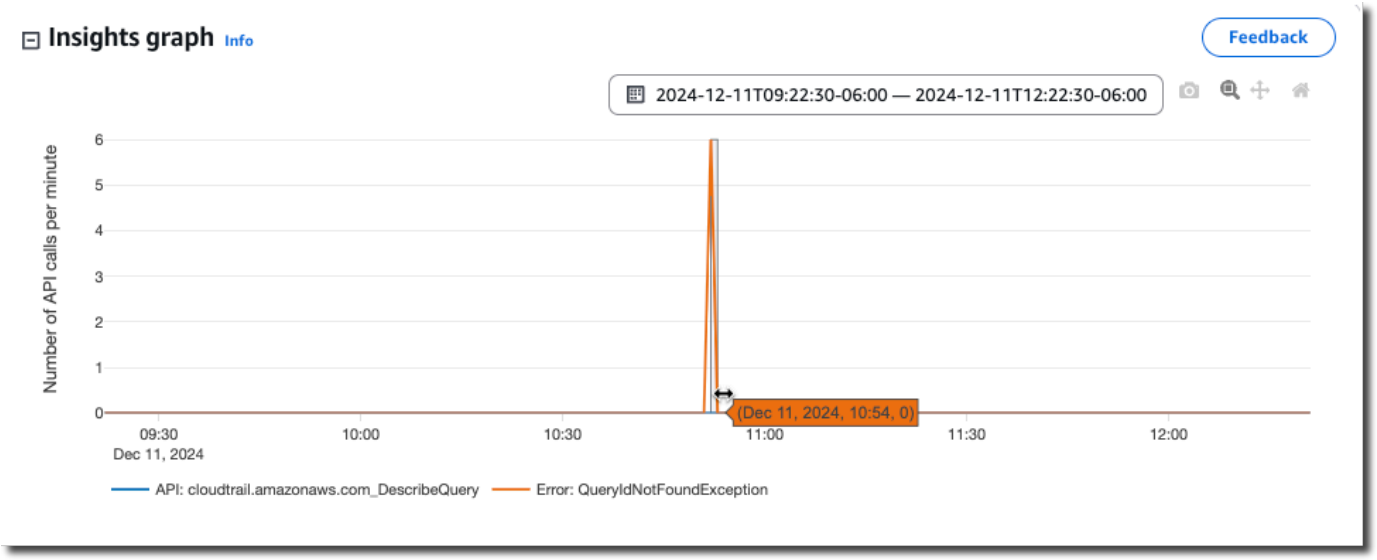
4. Untuk menghapus filter rentang waktu, pilih ikon kalender di sebelah kanan kotak Filter berdasarkan tanggal dan waktu, lalu pilih H apus dan tutup.

Melihat detail acara Insights

1. Pilih acara Wawasan dalam daftar hasil untuk menampilkan detailnya. Halaman detail untuk acara Wawasan menampilkan grafik garis waktu aktivitas yang tidak biasa.



2. Arahkan kursor ke pita yang disorot untuk menunjukkan waktu mulai dan durasi setiap peristiwa Insights dalam grafik.



Informasi berikut ditampilkan di area Informasi tambahan grafik:

- Jenis wawasan. Ini bisa berupa tingkat panggilan API atau tingkat kesalahan API.
- Pemicu. Ini adalah tautan ke tab peristiwa Cloudtrail, yang mencantumkan manajemen atau peristiwa data yang dianalisis untuk menentukan bahwa aktivitas tidak biasa terjadi.
- Panggilan API per menit atau Kesalahan per menit
  - Rata-rata dasar - Tingkat kejadian tipikal per menit pada API tempat peristiwa Insights dicatat, sebagaimana diukur dalam kurang-lebih tujuh hari sebelumnya, di Wilayah tertentu di akun Anda.
  - Rata-rata wawasan - Tingkat kejadian per menit di API ini yang memicu peristiwa Insights. Rat CloudTrail a-rata Wawasan untuk acara awal adalah tingkat panggilan atau kesalahan per menit pada API yang memicu peristiwa Insights. Biasanya, ini adalah menit pertama dari aktivitas yang tidak biasa. Rata-rata Wawasan untuk acara akhir adalah tingkat panggilan API atau kesalahan per menit selama durasi aktivitas yang tidak biasa, antara acara Insights awal dan acara Insights akhir.
- Sumber acara. T AWS itik akhir layanan tempat jumlah panggilan atau kesalahan API yang tidak biasa dicatat. Pada gambar sebelumnya, sumbernya adalah`ec2.amazonaws.com`, yang merupakan titik akhir layanan untuk Amazon EC2.
- Start event ID - ID peristiwa Insights yang dicatat pada awal aktivitas yang tidak biasa.
- ID peristiwa akhir - ID peristiwa Insights yang dicatat pada akhir aktivitas yang tidak biasa.

- ID peristiwa bersama - Dalam peristiwa Wawasan, ID peristiwa Ber sama adalah GUID yang dihasilkan oleh CloudTrail Insights untuk mengidentifikasi secara unik pasangan awal dan akhir peristiwa Wawasan. ID peristiwa bersama adalah umum antara acara Insights awal dan akhir, dan membantu menciptakan korelasi antara kedua peristiwa untuk mengidentifikasi aktivitas yang tidak biasa secara unik.

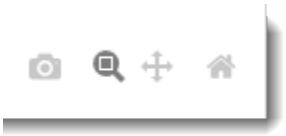
3. Pilih tab Atribusi untuk melihat informasi tentang identitas pengguna, agen pengguna, ARN sumber daya, dan peristiwa Wawasan tingkat panggilan API, kode kesalahan yang berkorelasi dengan aktivitas yang tidak biasa dan aktivitas dasar. Maksimal lima identitas pengguna, lima agen pengguna, lima ARN sumber daya, dan lima kode kesalahan ditampilkan dalam tabel pada tab Atribusi, diurutkan berdasarkan rata-rata jumlah aktivitas, dalam urutan menurun dari tertinggi ke terendah. Atribusi ARN sumber daya hanya tersedia untuk peristiwa Wawasan pada peristiwa data.
4. Pada tab CloudTrail peristiwa, lihat peristiwa terkait yang CloudTrail dianalisis untuk menentukan bahwa aktivitas tidak biasa terjadi. Secara default, filter sudah diterapkan untuk nama acara Insights, yang juga merupakan nama API terkait. Tab CloudTrail peristiwa menampilkan peristiwa CloudTrail manajemen atau data yang terkait dengan API subjek yang terjadi antara waktu mulai (dikurangi satu menit) dan waktu akhir (ditambah satu menit) dari acara Insights.

   Saat Anda memilih peristiwa Wawasan lainnya dalam grafik, peristiwa yang ditampilkan dalam tabel CloudTrail peristiwa berubah. Peristiwa ini membantu Anda melakukan analisis yang lebih mendalam untuk menentukan kemungkinan penyebab peristiwa Insights tertentu dan alasan terjadinya aktivitas API yang tidak biasa.

   Untuk menampilkan semua CloudTrail peristiwa yang dicatat selama durasi peristiwa Insights, dan tidak hanya untuk API terkait, matikan filter.
5. Pilih tab Catatan peristiwa Insights untuk melihat acara awal dan akhir Wawasan dalam format JSON.
6. Memilih sumber Event yang dit autkan akan mengembalikan Anda ke halaman Wawasan, yang difilter oleh sumber peristiwa tersebut.

Memperbesar, menggeser, dan mengunduh grafik

Anda dapat memperbesar, menggeser, dan mengatur ulang sumbu grafik pada halaman detail peristiwa Wawasan dengan menggunakan bilah alat di sudut kanan atas.

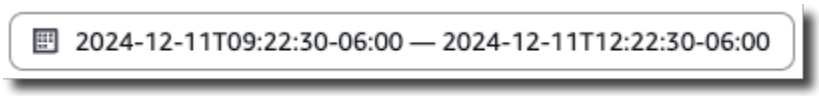


Dari kiri ke kanan, tombol perintah pada toolbar grafik melakukan hal berikut:

- Unduh plot sebagai PNG - Unduh gambar grafik yang ditampilkan pada halaman detail, dan simpan dalam format PNG.
- Zoom - Seret untuk memilih area pada grafik yang ingin Anda perbesar dan lihat secara lebih rinci.
- Pan - Geser grafik untuk melihat tanggal atau waktu yang berdekatan.
- Setel ulang sumbu - Ubah sumbu grafik kembali ke aslinya, hapus pengaturan zoom dan pan.

Ubah pengaturan rentang waktu grafik

Anda dapat mengubah rentang waktu—durasi yang dipilih dari peristiwa yang ditampilkan pada sumbu x—yang ditampilkan dalam grafik dengan memilih pengaturan di sudut kanan atas grafik.



Mengunduh acara Insights

Anda dapat mengunduh riwayat peristiwa Insights yang direkam sebagai file dalam format CSV atau JSON. Gunakan filter dan rentang waktu untuk mengurangi ukuran file yang Anda unduh.

> **Note**
>
> CloudTrail file riwayat peristiwa adalah file data yang berisi informasi (seperti nama sumber daya) yang dapat dikonfigurasi oleh pengguna individu. Beberapa data berpotensi dapat ditafsirkan sebagai perintah dalam program yang digunakan untuk membaca dan menganalisis data ini (injeksi CSV). Misalnya, ketika CloudTrail acara diekspor ke CSV dan diimpor ke program spreadsheet, program tersebut mungkin memperingatkan Anda tentang masalah keamanan. Sebagai praktik terbaik keamanan, nonaktifkan tautan atau makro dari file riwayat acara yang diunduh.

1. Tentukan filter dan rentang waktu untuk acara yang ingin Anda unduh. Misalnya, Anda dapat menentukan nama acara,`StartInstances`, dan menentukan rentang waktu untuk 12 jam terakhir aktivitas.
2. Pilih Unduh acara, lalu pilih Unduh sebagai CSV atau Unduh sebagai JSON. Anda diminta untuk memilih lokasi untuk menyimpan file.

   > **Note**
   >
   > Unduhan Anda mungkin membutuhkan waktu untuk selesai. Untuk hasil yang lebih cepat, sebelum Anda memulai proses pengunduhan, gunakan filter yang lebih spesifik atau rentang waktu yang lebih pendek untuk mempersempit hasil.

3. Setelah unduhan selesai, buka file untuk melihat peristiwa yang Anda tentukan.
4. Untuk membatalkan unduhan Anda, pilih Batal. Jika Anda membatalkan unduhan sebelum selesai, file CSV atau JSON di komputer lokal Anda mungkin hanya berisi sebagian dari acara Anda.

Melihat acara Wawasan untuk jalur dengan AWS CLI

Bagian ini menjelaskan cara menggunakan `list-insights-data` perintah AWS CLI `lookup-events` and untuk mencari jejak peristiwa Insights selama 90 hari terakhir dengan peristiwa Insights diaktifkan. Untuk informasi tentang cara mengaktifkan CloudTrail Wawasan di jalur, lihatPencatatan peristiwa Wawasan untuk jejak menggunakan AWS CLI.

> **Note**
>
> Anda tidak dapat menggunakan `list-insights-data` perintah `lookup-events` atau untuk mencari peristiwa Insights untuk penyimpanan data peristiwa, namun, CloudTrail Lake menawarkan sejumlah contoh kueri untuk penyimpanan data peristiwa Insights. Untuk informasi selengkapnya, lihat Melihat contoh kueri untuk acara Insights.

`lookup-events`Perintah ini memiliki opsi berikut:

- `--end-time`
- `--event-category`
- `--max-results`

- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

`list-insights-data`Perintah ini memiliki opsi berikut:

- `--end-time`
- `--data-type`
- `--max-results`
- `--start-time`
- `--dimensions`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

Untuk informasi umum tentang penggunaan AWS Command Line Interface, lihat Panduan AWS Command Line Interface Pengguna.

Daftar Isi

- Prasyarat
- Mendapatkan bantuan baris perintah
- Mencari acara Wawasan untuk acara manajemen
- Mencari acara Wawasan untuk peristiwa data
- Menentukan jumlah peristiwa Wawasan untuk acara manajemen yang akan dikembalikan
- Menentukan jumlah peristiwa Wawasan untuk peristiwa data yang akan ditampilkan
- Mencari acara Wawasan untuk acara manajemen berdasarkan rentang waktu
- Mencari acara Wawasan untuk peristiwa data berdasarkan rentang waktu
- Mencari acara Wawasan untuk acara manajemen berdasarkan atribut
  - Contoh pencarian atribut
- Mencari peristiwa Wawasan untuk peristiwa data berdasarkan dimensi

  - Contoh pencarian dimensi
- Menentukan halaman hasil berikutnya untuk acara Wawasan untuk acara manajemen
- Menentukan halaman hasil berikutnya untuk acara Wawasan untuk acara manajemen
- Mendapatkan masukan JSON dari file untuk acara Insights untuk acara manajemen
- Mendapatkan masukan JSON dari file untuk peristiwa Insights untuk peristiwa data
- Bidang keluaran pencarian

Prasyarat

- Untuk menjalankan AWS CLI perintah, Anda harus menginstal file AWS CLI. Untuk informasi selengkapnya, lihat Memulai dengan AWS CLI.
- Pastikan AWS CLI versi Anda lebih besar dari 1.6.6. Untuk memverifikasi versi CLI, jalankan aws --version pada baris perintah.
- Untuk mengatur akun, Wilayah, dan format output default untuk AWS CLI sesi, gunakan aws configure perintah. Untuk informasi selengkapnya, lihat Mengkonfigurasi Antarmuka Baris AWS Perintah.
- Untuk mencatat peristiwa Insights pada rasio panggilan API, jejak harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mencatat `read` atau `write` mengelola peristiwa.

> **Note**
>
> CloudTrail AWS CLI Perintahnya peka huruf besar/kecil.

Mendapatkan bantuan baris perintah

Untuk melihat bantuan baris perintah`lookup-events`, ketik perintah berikut.

```
aws cloudtrail lookup-events help
```

Mencari acara Wawasan untuk acara manajemen

Untuk melihat 50 peristiwa Insights terbaru, ketik perintah berikut.

```
aws cloudtrail lookup-events --event-category insight
```

Peristiwa yang dikembalikan terlihat mirip dengan contoh berikut,

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:52:00Z",
            "awsRegion": "us-east-1",
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "sourceEventCategory": "Management",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 1.2
                                }
```

```
                        ],
                        "baseline": []
                    },
                    {
                        "attribute": "userAgent",
                        "insight": [
                            {
                                "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                "average": 1.2
                            }
                        ],
                        "baseline": []
                    }
                ]
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.09",
        "eventTime": "2024-12-11T16:53:00Z",
        "awsRegion": "us-east-1",
        "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "888888888888",
        "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
        "insightDetails": {
            "state": "End",
            "eventSource": "cloudtrail.amazonaws.com",
            "eventName": "DescribeQuery",
            "insightType": "ApiErrorRateInsight",
            "errorCode": "QueryIdNotFoundException",
            "sourceEventCategory": "Management",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 0
                    },
                    "insight": {
                        "average": 6
                    },
                    "insightDuration": 1,
                    "baselineDuration": 11092
```

```
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        }
    ]
}
```

Untuk penjelasan tentang bidang terkait pencarian di output, lihat Bidang keluaran pencarian di topik ini. Untuk penjelasan bidang dalam acara Wawasan, lihatCloudTrail merekam konten untuk acara Insights untuk jalur.

Mencari acara Wawasan untuk peristiwa data

Untuk melihat 50 peristiwa Insights terbaru, ketik perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
```

Peristiwa yang dikembalikan terlihat mirip dengan contoh berikut,


```
    {
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP

    "Events": [
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:52:00Z",
            "awsRegion": "us-east-2",
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "s3.amazonaws.com",
                "eventName": "PutObject",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "InvalidRequest",
                "sourceEventCategory": "Data",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::123456789012:assumed-role/
Admin",
                                    "average": 1.2
                                }
                            ],
```

```
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        }
                    ]
                },

                "insightSource": "arn:aws:cloudtrail:us-
east-2:123456789012:trail/TrailName"
            },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:53:00Z",
            "awsRegion": "us-east-1",
            "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "End",
                "eventSource": "s3.amazonaws.com",
                "eventName": "PutObject",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "InvalidRequest",
                "sourceEventCategory": "Data",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 6
                        },
```

```
                        "insightDuration": 1,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::123456789012:assumed-role/
Admin",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                },

                "insightSource": "arn:aws:cloudtrail:us-
east-2:123456789012:trail/TrailName"
            },
            "eventCategory": "Insight"
        }
    ]
}
```

Menentukan jumlah peristiwa Wawasan untuk acara manajemen yang akan dikembalikan

Untuk menentukan jumlah peristiwa Wawasan untuk peristiwa manajemen yang akan ditampilkan, ketik perintah berikut.

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

Nilai default untuk*<integer>*, jika tidak ditentukan, adalah 50. Nilai yang mungkin adalah 1 hingga 50. Contoh berikut mengembalikan satu hasil.

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

Menentukan jumlah peristiwa Wawasan untuk peristiwa data yang akan ditampilkan

Untuk menentukan jumlah peristiwa Wawasan untuk peristiwa data yang akan ditampilkan, ketik perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --max-results <integer>
```

Nilai default untuk*<integer>*, jika tidak ditentukan, adalah 50. Nilai yang mungkin adalah 1 hingga 50. Contoh berikut mengembalikan satu hasil.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --max-results 1
```

Mencari acara Wawasan untuk acara manajemen berdasarkan rentang waktu

Wawasan acara untuk acara manajemen dari 90 hari terakhir tersedia untuk pencarian. Untuk menentukan rentang waktu, ketik perintah berikut.

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>*menetapkan, di UTC, bahwa hanya peristiwa Wawasan yang terjadi setelah atau pada waktu yang ditentukan yang dikembalikan. Jika waktu mulai yang ditentukan adalah setelah waktu akhir yang ditentukan, kesalahan dikembalikan.

`--end-time` *<timestamp>*menetapkan, di UTC, bahwa hanya peristiwa Wawasan yang terjadi sebelum atau pada waktu yang ditentukan yang dikembalikan. Jika waktu akhir yang ditentukan sebelum waktu mulai yang ditentukan, kesalahan dikembalikan.

Waktu mulai default adalah tanggal paling awal bahwa data tersedia dalam 90 hari terakhir. Waktu akhir default adalah waktu peristiwa yang terjadi paling dekat dengan waktu saat ini.

Semua stempel waktu ditampilkan di UTC.

Mencari acara Wawasan untuk peristiwa data berdasarkan rentang waktu

Insights event untuk peristiwa data dari 90 hari terakhir tersedia untuk pencarian. Untuk menentukan rentang waktu, ketik perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --start-time <timestamp> --
end-time <timestamp>
```

`--start-time` *<timestamp>*menetapkan, di UTC, bahwa hanya peristiwa Wawasan yang terjadi setelah atau pada waktu yang ditentukan yang dikembalikan. Jika waktu mulai yang ditentukan adalah setelah waktu akhir yang ditentukan, kesalahan dikembalikan.

`--end-time` *<timestamp>*menetapkan, di UTC, bahwa hanya peristiwa Wawasan yang terjadi sebelum atau pada waktu yang ditentukan yang dikembalikan. Jika waktu akhir yang ditentukan sebelum waktu mulai yang ditentukan, kesalahan dikembalikan.

Waktu mulai default adalah tanggal paling awal bahwa data tersedia dalam 90 hari terakhir. Waktu akhir default adalah waktu peristiwa yang terjadi paling dekat dengan waktu saat ini.

Semua stempel waktu ditampilkan di UTC.

Mencari acara Wawasan untuk acara manajemen berdasarkan atribut

Untuk memfilter berdasarkan atribut, ketik perintah berikut.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

Anda hanya dapat menentukan satu pasangan nilai kunci atribut untuk setiap lookup-events perintah. Berikut ini adalah nilai acara Insights yang valid untuk`AttributeKey`. Nama nilai peka huruf besar/kecil.

- `EventId`
- `EventName`
- `EventSource`

Panjang maksimum untuk `AttributeValue` adalah 2000 karakter. Karakter berikut (_", ", , ',\ \n') dihitung sebagai dua karakter menuju batas 2000 karakter.

Contoh pencarian atribut

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventName` adalah`PutRule`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventId` adalah`b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventSource` adalah`iam.amazonaws.com`.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

Mencari peristiwa Wawasan untuk peristiwa data berdasarkan dimensi

Untuk memfilter berdasarkan dimensi, ketik perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
       --dimensions <DimensionKey>=<DimensionValue>
```

Anda hanya dapat menentukan satu pasangan nilai kunci dimensi untuk setiap list-insights-events perintah. Berikut ini adalah nilai acara Insights yang valid untuk`DimensionKey`. Nama nilai peka huruf besar/kecil.

- `EventId`
- `EventName`
- `EventSource`

Panjang maksimum untuk `DimensionValue` adalah 2000 karakter. Karakter berikut (_", ", , ',\ \n') dihitung sebagai dua karakter menuju batas 2000 karakter.

Contoh pencarian dimensi

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventName` adalah`PutObject`.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventName=PutObject
```

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventId` adalah`b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002`.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventId=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

Perintah contoh berikut mengembalikan peristiwa Wawasan di mana nilai `EventSource` adalah`s3.amazonaws.com`.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventSource=s3.amazonaws.com
```

Menentukan halaman hasil berikutnya untuk acara Wawasan untuk acara manajemen

Untuk mendapatkan halaman hasil berikutnya dari `lookup-events` perintah, ketik perintah berikut.

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

Dalam perintah ini, nilai untuk *<token>* diambil dari bidang pertama dari output dari perintah sebelumnya.

Saat Anda menggunakan `--next-token` perintah, Anda harus menggunakan parameter yang sama seperti pada perintah sebelumnya. Misalnya, Anda menjalankan perintah berikut.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

Untuk mendapatkan halaman hasil berikutnya, perintah Anda berikutnya akan terlihat seperti berikut.

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Menentukan halaman hasil berikutnya untuk acara Wawasan untuk acara manajemen

Untuk mendapatkan halaman hasil berikutnya dari `list-insights-data` perintah, ketik perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName<same parameters as previous
 command> --next-token=<token>
```

Dalam perintah ini, nilai untuk *<token>* diambil dari bidang pertama dari output dari perintah sebelumnya.

Saat Anda menggunakan `--next-token` perintah, Anda harus menggunakan parameter yang sama seperti pada perintah sebelumnya. Misalnya, Anda menjalankan perintah berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventName=PutObject
```

Untuk mendapatkan halaman hasil berikutnya, perintah Anda berikutnya akan terlihat seperti berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-
source arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
 --dimensions EventName=PutObject --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

Mendapatkan masukan JSON dari file untuk acara Insights untuk acara manajemen

AWS CLI Untuk beberapa AWS layanan memiliki dua parameter, `--generate-cli-skeleton` dan`--cli-input-json`, yang dapat Anda gunakan untuk menghasilkan template JSON, yang dapat Anda modifikasi dan gunakan sebagai input ke `--cli-input-json` parameter. Bagian ini menjelaskan cara menggunakan parameter ini dengan`aws cloudtrail lookup-events`. Untuk informasi selengkapnya, lihat AWS CLI kerangka dan file input.

Untuk mencari acara Insights dengan mendapatkan masukan JSON dari file

1. Buat template input untuk digunakan `lookup-events` dengan mengarahkan `--generate-cli-skeleton` output ke file, seperti pada contoh berikut.

   ```
   aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
    LookupEvents.txt
   ```

   File template yang dihasilkan (dalam hal ini, LookupEvents .txt) terlihat seperti berikut.

   ```
   {
       "LookupAttributes": [
           {
               "AttributeKey": "",
               "AttributeValue": ""
           }
       ],
       "StartTime": null,
       "EndTime": null,
       "MaxResults": 0,
       "NextToken": ""
   }
   ```

2. Gunakan editor teks untuk memodifikasi JSON sesuai kebutuhan. Masukan JSON harus berisi hanya nilai-nilai yang ditentukan.

   > **Important**
   >
   > Semua nilai kosong atau nol harus dihapus dari template sebelum Anda dapat menggunakannya.

Contoh berikut menentukan rentang waktu dan jumlah maksimum hasil untuk kembali.

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. Untuk menggunakan file yang diedit sebagai input, gunakan sintaks `--cli-input-json file://<filename>`, seperti pada contoh berikut.

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> Anda dapat menggunakan argumen lain pada baris perintah yang sama dengan`--cli-input-json`.

Mendapatkan masukan JSON dari file untuk peristiwa Insights untuk peristiwa data

AWS CLI Untuk beberapa AWS layanan memiliki dua parameter, `--generate-cli-skeleton` dan`--cli-input-json`, yang dapat Anda gunakan untuk menghasilkan template JSON, yang dapat Anda modifikasi dan gunakan sebagai input ke `--cli-input-json` parameter. Bagian ini menjelaskan cara menggunakan parameter ini dengan`aws cloudtrail list-insights-data`. Untuk informasi selengkapnya, lihat AWS CLI kerangka dan file input.

Untuk mencari acara Insights dengan mendapatkan masukan JSON dari file

1. Buat template input untuk digunakan `list-insights-data` dengan mengarahkan `--generate-cli-skeleton` output ke file, seperti pada contoh berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --generate-cli-
skeleton > ListInsightsData.txt
```

File template yang dihasilkan (dalam hal ini, ListInsightsData .txt) terlihat seperti berikut.

```
{
   "InsightSource": "",
    "DataType": "InsightsEvents",
    "Dimensions":
    {
        "KeyName": ""
    },
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Gunakan editor teks untuk memodifikasi JSON sesuai kebutuhan. Masukan JSON harus berisi hanya nilai-nilai yang ditentukan.

> **Important**
>
> Semua nilai kosong atau nol harus dihapus dari template sebelum Anda dapat menggunakannya.

Contoh berikut menentukan rentang waktu dan jumlah maksimum hasil untuk kembali.

```
{

   "InsightSource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "DataType": "InsightsEvents",
    "Dimensions":
    {
        "EventName": "PutObject"
    },
    "StartTime": "2025-11-01",
    "EndTime": "2025-11-05",
    "MaxResults": 1
}
```

3. Untuk menggunakan file yang diedit sebagai input, gunakan sintaks `--cli-input-json file://<filename>`, seperti pada contoh berikut.

```
aws cloudtrail list-insights-data --data-type InsightsEvents --cli-input-json
 file://ListInsightsData.txt
```

> **Note**
>
> Anda dapat menggunakan argumen lain pada baris perintah yang sama dengan`--cli-input-json`.

Bidang keluaran pencarian

Peristiwa

Daftar peristiwa pencarian berdasarkan atribut lookup dan rentang waktu yang ditentukan. Daftar acara diurutkan berdasarkan waktu, dengan acara terbaru terdaftar terlebih dahulu. Setiap entri berisi informasi tentang permintaan pencarian dan menyertakan representasi string dari CloudTrail peristiwa yang diambil.

Entri berikut menjelaskan bidang di setiap acara pencarian.

CloudTrailEvent

Sebuah string JSON yang berisi representasi objek dari acara dikembalikan. Untuk informasi tentang masing-masing elemen yang dikembalikan, lihat Rekam Isi Tubuh.

EventId

Sebuah string yang berisi GUID dari acara dikembalikan.

EventName

Sebuah string yang berisi nama acara dikembalikan.

EventSource

AWS Layanan yang diminta untuk dibuat.

EventTime

Tanggal dan waktu, dalam format waktu UNIX, acara.

Sumber Daya

Daftar sumber daya yang direferensikan oleh acara yang dikembalikan. Setiap entri sumber daya menentukan jenis sumber daya dan nama sumber daya.

ResourceName

String yang berisi nama sumber daya yang direferensikan oleh acara tersebut.

ResourceType

String yang berisi jenis sumber daya yang direferensikan oleh acara tersebut. Ketika jenis sumber daya tidak dapat ditentukan, null dikembalikan.

Nama Pengguna

String yang berisi nama pengguna akun untuk acara yang dikembalikan.

NextToken

Sebuah string untuk mendapatkan halaman berikutnya dari hasil dari `lookup-events` perintah sebelumnya. Untuk menggunakan token, parameternya harus sama dengan yang ada di perintah asli. Jika tidak ada `NextToken` entri yang muncul di output, tidak ada lagi hasil untuk dikembalikan.

Untuk informasi selengkapnya tentang acara CloudTrail Wawasan, lihat Bekerja dengan CloudTrail Wawasan di panduan ini.

Melihat peristiwa Wawasan untuk penyimpanan data acara

Bagian ini menjelaskan cara Anda dapat melihat peristiwa Wawasan untuk penyimpanan data peristiwa Insights dengan melihat dasbor peristiwa Wawasan dan menjalankan kueri sampel.

Untuk informasi tentang cara mengaktifkan CloudTrail Wawasan di penyimpanan data peristiwa, lihatMengaktifkan CloudTrail Wawasan pada penyimpanan data peristiwa yang ada dengan konsol.

CloudTrail permintaan dikenakan biaya berdasarkan jumlah data yang dipindai. Untuk membantu mengontrol biaya, sebaiknya batasi kueri dengan menambahkan stempel `eventTime` waktu awal dan akhir ke kueri. Untuk informasi lebih lanjut tentang harga CloudTrail, lihat Harga AWS CloudTrail.

Untuk deskripsi bidang catatan peristiwa Insights untuk penyimpanan data peristiwa, lihatCloudTrail merekam konten untuk acara Wawasan untuk penyimpanan data acara.

Topik

- Melihat dasbor Wawasan untuk penyimpanan data peristiwa
- Melihat contoh kueri untuk acara Insights

Melihat dasbor Wawasan untuk penyimpanan data peristiwa

Dasbor peristiwa Wawasan menunjukkan proporsi keseluruhan peristiwa Wawasan berdasarkan jenis Wawasan, proporsi peristiwa Wawasan menurut jenis Wawasan untuk pengguna dan layanan teratas, dan jumlah peristiwa Wawasan per hari. Dasbor juga menyertakan widget yang mencantumkan acara Insights hingga 30 hari.

> **Note**
>
> - Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya di penyimpanan data peristiwa sumber, CloudTrail mungkin diperlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut. Untuk informasi selengkapnya, lihat Penyampaian acara Insights.
> - Dasbor peristiwa Wawasan hanya menampilkan informasi tentang peristiwa Wawasan yang dikumpulkan oleh penyimpanan data peristiwa yang dipilih, yang ditentukan oleh konfigurasi penyimpanan data peristiwa sumber. Misalnya, jika Anda mengonfigurasi penyimpanan data peristiwa sumber untuk mengaktifkan acara Insights `ApiCallRateInsight` tetapi tidak`ApiErrorRateInsight`, Anda tidak akan melihat informasi tentang peristiwa Insights pada`ApiErrorRateInsight`.

Untuk melihat dasbor peristiwa Insights

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Lake, pilih Dasbor.
3. Pilih tab Das bor terkelola dan kustom.
4. Dari dasbor terkel AWS ola, pilih dasbor acara Insights.
5. Pilih penyimpanan data acara Insights Anda.
6. Pilih untuk memfilter data dasbor dengan rentang Absolut atau Rentang Relatif. Pilih Rentang absolut untuk memilih tanggal dan rentang waktu tertentu. Pilih Rentang relatif untuk memilih

rentang waktu yang telah ditentukan atau rentang khusus. Secara default, dasbor menampilkan data acara selama 24 jam terakhir.

> **Note**
>
> CloudTrail Kueri Lake dikenakan biaya berdasarkan jumlah data yang dipindai. Untuk membantu mengontrol biaya, Anda dapat memfilter pada rentang waktu yang lebih sempit. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

7. Pilih ikon refresh untuk mengisi grafik untuk widget dasbor. Setiap widget menunjukkan status penyegaran.

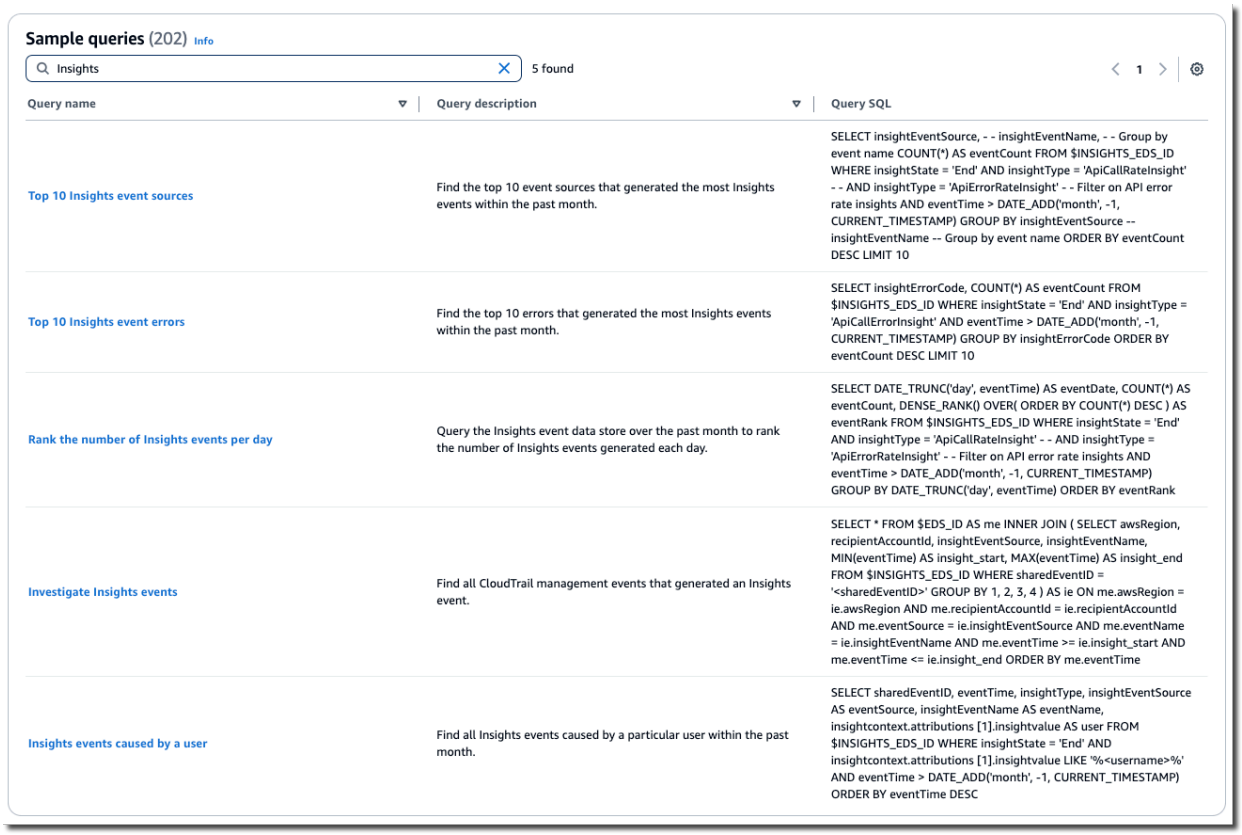
Untuk informasi lebih lanjut tentang dasbor Danau, lihatCloudTrail Dasbor danau.

Melihat contoh kueri untuk acara Insights

Kon CloudTrail sol menyediakan sejumlah kueri sampel untuk acara Insights yang dapat membantu Anda mulai menulis kueri Anda sendiri.

Untuk melihat contoh kueri untuk acara Insights

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Lake, pilih Query.
3. Pada halaman Kueri, pilih tab Kueri Sam pel.
4. Cari kueri untuk acara Wawasan. Pilih nama Kueri untuk membuka kueri di tab Editor.



5. Pada tab Editor, pilih penyimpanan data peristiwa Insights. Ketika Anda memilih penyimpanan data peristiwa dari daftar, CloudTrail secara otomatis mengisi ID penyimpanan data peristiwa di `FROM` baris editor kueri.
6. Pilih Jalan kan untuk menjalankan kueri. Setelah kueri selesai, Anda dapat melihat output perintah dan hasil kueri.

   Tab Output perintah menunjukkan metadata tentang kueri Anda, seperti apakah kueri berhasil, jumlah catatan yang cocok, dan waktu menjalankan kueri.

   Tab Hasil kueri menampilkan data peristiwa di penyimpanan data peristiwa terpilih yang cocok dengan kueri Anda.

Untuk informasi selengkapnya tentang mengedit kueri, lihatMembuat atau mengedit kueri dengan CloudTrail konsol. Untuk informasi selengkapnya tentang menjalankan kueri dan menyimpan hasil kueri, lihatJalankan kueri dan simpan hasil kueri dengan konsol.

Bekerja dengan AWS CloudTrail Danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

AWS CloudTrail Lake memungkinkan Anda menjalankan SQL-based kueri pada acara Anda. CloudTrail Lake mengonversi peristiwa yang ada dalam format JSON berbasis baris ke format Apache ORC. ORC adalah format penyimpanan kolumnar yang dioptimalkan untuk pengambilan data dengan cepat. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih peristiwa lanj utan. Anda dapat menyimpan data peristiwa di penyimpanan data peristiwa hingga 3.653 hari (sekitar 10 tahun) jika memilih opsi harga retensi One-year yang dapat diperpanjang, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi. Seven-year Pemilih yang Anda terapkan ke penyimpanan data peristiwa mengontrol peristiwa mana yang bertahan dan tersedia untuk Anda kueri. CloudTrail Lake adalah solusi audit yang dapat melengkapi tumpukan kepatuhan Anda, dan membantu Anda dengan pemecahan masalah hampir real-time.

CloudTrail Perubahan ketersediaan danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Untuk kemampuan yang mirip dengan CloudTrail Danau, jelajahi CloudWatch.

Setelah mempertimbangkan dengan cermat, kami memutuskan untuk menutup AWS CloudTrail Lake dengan pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa.

AWS CloudTrail Lake menyediakan solusi terkelola untuk menangkap, menyimpan, dan menganalisis log audit dari AWS dan AWS non-sumber. AWS CloudTrail terus tersedia untuk pelanggan yang

sudah ada, tetapi CloudTrail Lake hanya akan menerima perbaikan bug penting dan pembaruan keamanan.

Panduan ini memberikan informasi tentang opsi migrasi untuk pelanggan AWS CloudTrail Lake.

> **Note**
>
> AWS CloudTrail terus didukung sepenuhnya. Hanya AWS CloudTrail Danau yang tidak lagi terbuka untuk pelanggan baru. AWS CloudTrail Jejak, Wawasan, dan Peristiwa Gabungan Anda tidak terpengaruh.

Dukungan berkelanjutan untuk penyimpanan data acara yang ada

AWS CloudTrail Lake mendukung dua jenis penyimpanan data acara (EDS): penyimpanan data acara organisasi, dan penyimpanan data acara akun. Tingkat dukungan lanjutan tergantung pada jenis yang telah Anda konfigurasikan.

- Penyimpanan data acara organisasi — Jika AWS Organisasi Anda memiliki EDS tingkat organisasi, AWS CloudTrail Lake akan terus berfungsi seperti yang diharapkan. Ini termasuk dukungan untuk akun anggota baru yang ditambahkan ke organisasi Anda dan ekspansi ke tambahan Wilayah AWS. Untuk mempelajari cara membuat penyimpanan data acara organisasi, lihatMembuat penyimpanan data acara organisasi.
- Penyimpanan data acara akun — Jika AWS Organisasi Anda hanya memiliki penyimpanan data acara tingkat akun, AWS CloudTrail Lake akan terus mendukung akun yang ada, termasuk ekspansi ke akun baru. Wilayah AWS Namun, AWS CloudTrail Lake tidak akan mendukung konsumsi akun baru yang ditambahkan ke organisasi Anda. Untuk menangkap data AWS CloudTrail Lake untuk akun baru di organisasi Anda, Anda harus membuat penyimpanan data acara organisasi atau bermigrasi ke Amazon CloudWatch.

> **Note**
>
> Jika Anda mengantisipasi penambahan akun anggota baru ke AWS Organisasi Anda dan ingin AWS CloudTrail Lake menutup akun tersebut secara otomatis, pastikan Anda memiliki penyimpanan data acara organisasi yang dikonfigurasi. Penyimpanan data acara akun tidak akan memperluas cakupan ke akun anggota organisasi yang baru ditambahkan.

Opsi migrasi

Kami menyarankan Anda memigrasikan data log AWS CloudTrail Danau Anda ke Amazon CloudWatch.

Amazon CloudWatch

- Amazon CloudWatch menyatukan data keamanan, operasi, dan kepatuhan dalam satu solusi, serta menyediakan analitik yang fleksibel dan kemampuan integrasi yang mulus. Pelanggan dapat secara otomatis menormalkan dan memproses data untuk menawarkan konsistensi di seluruh sumber dengan dukungan bawaan untuk format Open Cybersecurity Schema Framework (OCSF) dan Open Telemetry (OTel), sehingga Anda dapat fokus pada analitik dan wawasan.
- Amazon CloudWatch menyediakan kemampuan CloudTrail Lake saat ini pada titik harga yang sebanding, dan memiliki kemampuan tambahan yang merupakan permintaan utama dari pelanggan CloudTrail Lake. Ini termasuk analitik asli yang didukung oleh OpenSearch, konektor pra-bangun untuk sumber pihak ketiga yang populer, dan akses terbuka melalui Apache Iceberg API.
- Untuk memulai Amazon CloudWatch, lihat CloudWatchsaluran pipa di Panduan CloudWatch Pengguna Amazon. Untuk detail tentang harga, lihat CloudWatch harga.

Membandingkan arsitektur

Arsitektur AWS CloudTrail Lake saat ini menyediakan solusi terkelola untuk menangkap, menyimpan, dan menganalisis log audit melalui penyimpanan data peristiwa, dan kueri. Sistem ini beroperasi sebagai fitur di dalamnya AWS CloudTrail. Alternatif yang direkomendasikan, Amazon CloudWatch, mempertahankan kemampuan inti untuk menangkap, menyimpan, dan menganalisis CloudTrail log. Ini menyatukan data keamanan, operasi, dan kepatuhan dalam satu solusi. Amazon CloudWatch menawarkan kemampuan tambahan seperti analitik asli yang didukung oleh OpenSearch, konektor pra-bangun untuk sumber pihak ketiga yang populer, akses terbuka melalui Apache Iceberg API, dan dukungan bawaan untuk format Open Cybersecurity Schema Framework (OCSF) dan Open Telemetry (OTel).

Kemampuan	CloudTrail Danau	CloudWatch	Detail
Sumber Data	3 AWS, 16 Third-Party	60+ AWS, 12 Third-Party	CloudWatch mendukung 30+ AWS sumber termasuk Aliran VPC, Lambda, EKS, ALB, NLB CloudTrai l & (kecuali Acara Jaringan & Wawasan).
Cross-account/ cross-region Pemberdayaan	Ya	Sebagian	CloudWatch Ingestion mendukung pemberdayaan di seluruh akun tetapi membutuhkan pemberdayaan terpisah di setiap Wilayah.
Cross-account/ cross-region Sentralisasi	Ya	Ya	Aktifkan agregasi log di seluruh akun & Wilayah dalam satu akun & Wilayah.
CloudTrail Fitur Keselamat an - Tertelan acara terlambat , perlindungan penghentian & kekekalan	Ya	Ya	CloudWatch hanya mendukung CloudTrail events/data melalui CW Ingestion (dan, bukan jalur).
Transformasi & Pengayaan Data	Terbatas	Ya	CloudWatch mendukung Transform asi OCSF Terkelola untuk sumber utama & transformasi khusus untuk sumber yang tersisa.
Analisis Asli	Ya	Ya	CloudTrail Lake mendukung In-place kueri SQL dengan Athena. CloudWatch mendukung Log QL, SQL & PPL query In-place dengan. OpenSearch

Kemampuan	CloudTrail Danau	CloudWatch	Detail
SQL bersarang	Ya	Tidak	CloudTrail Lake mendukung kueri SQL bersarang yang kompleks.
Analisis 3P	Ya	Ya	CloudWatch mendukung kueri di tempat dengan alat pilihan 3P melalui Amazon S3 Tables dan AI Unified Studio. SageMaker
Ekspor Data ke AWS tujuan lain atau alat 3P	Ya	Ya	Anda dapat mengirim data melalui filter CloudWatch berlangganan, dan konektor tabel S3.
Analitik Tambahan	Tidak	Ya	CloudWatch mendukung Alerts & Metrics untuk observabilitas & kasus penggunaan keamanan.
Penyeleksi Acara untuk CloudTrail	Ya	Terbatas	CloudWatch mendukung Selektor lanjutan untuk peristiwa CloudTrail Data.

Prosedur migrasi

AWS baru-baru ini memperkenalkan cara yang disederhanakan untuk menyatukan data operasional dan keamanan Anda dengan memungkinkan Anda mengimpor penyimpanan data peristiwa CloudTrail Danau (EDS) historis langsung ke Amazon CloudWatch. Integrasi ini menggunakan CloudWatch arsitektur manajemen data terpadu baru untuk menyediakan satu panel kaca untuk log Anda.

Praktik Terbaik: Pendekatan Percontohan

Sebelum melakukan migrasi skala penuh dari data historis Anda, sangat disarankan untuk melakukan migrasi pilot menggunakan sebagian kecil data. Hal ini memungkinkan Anda untuk:

- Verifikasi bahwa log yang diimpor muncul dengan benar di CloudWatch.
- Konfirmasikan bahwa kueri dan dasbor Anda berperilaku seperti yang diharapkan.

- Validasi bahwa izin dan peran IAM dikonfigurasi dengan benar.

Setelah Anda puas dengan hasilnya, Anda dapat melanjutkan dengan percaya diri untuk memigrasikan kumpulan data historis lengkap.

- Verifikasi Skema: Pastikan format log muncul seperti yang diharapkan di CloudWatch Log.
- Manajemen Biaya: Perkirakan biaya konsumsi dengan mengamati volume sampel 24 jam.
- Validasi Kueri: Uji kueri Wawasan CloudWatch Log Anda terhadap data sampel untuk memastikan logika pemantauan Anda tetap utuh.

Setelah berhasil memigrasikan kumpulan data historis, Anda dapat mengaktifkan log langsung CloudWatch untuk memastikan Anda terus menangkap CloudTrail log.

> **Note**
>
> Data sebelum 2023 tidak akan dimigrasikan dari CloudTrail Danau ke Amazon. CloudWatch Jika Anda memerlukan akses ke acara yang lebih lama dari 2023, Anda harus terus menanyakannya langsung di CloudTrail Lake, atau memindahkannya ke bucket Amazon S3.

Prasyarat

- Izin IAM: Pastikan identitas IAM Anda memiliki izin untuk mengakses CloudTrail Lake (`cloudtrail:GetEventDataStore`,`cloudtrail:ListEventDataStore`) dan CloudWatch Logs (`logs:CreateImportTask`), serta izin IAM (,,). `iam:ListRoles` `iam:CreateRole` `iam:PassRole`
- Service-Linked Peran: CloudTrail membutuhkan peran IAM untuk melakukan ekspor atas nama Anda. Anda dapat membuat ini selama proses pengaturan di konsol.

Metode 1: Menggunakan CloudTrail Konsol (Disarankan)

Ini adalah cara paling langsung untuk mendorong data dari Lake Event Data Store yang ada.

1. Buka CloudTrail konsol.
2. Di panel navigasi kiri, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih penyimpanan data peristiwa yang berisi data yang ingin Anda migrasi.

4. Pilih tombol Tindakan di kanan atas dan pilih Ekspor ke CloudWatch.
5. Konfigurasikan Pengaturan Ekspor:
   - Rentang Waktu: (disarankan untuk Pilot) Alih-alih memilih seluruh riwayat Anda, pilih jendela sempit (misalnya, 24 jam terakhir) untuk memverifikasi integrasi. Setelah diverifikasi, ulangi proses untuk data historis yang tersisa.
   - Tujuan: Tentukan Grup CloudWatch Log yang ada atau buat yang baru.
6. Peran IAM: Pilih peran IAM yang ada atau pilih Buat peran IAM baru CloudTrail untuk memungkinkan pengiriman log. CloudWatch
7. Tinjau konfigurasi dan pilih Ekspor.

Metode 2: Menggunakan AWS CLI (buat-tugas-impor)

Metode ini memungkinkan Anda untuk secara terprogram memicu konsumsi data peristiwa historis.

Langkah 1: Identifikasi Sumber ARN

Anda akan memerlukan Nama Sumber Daya Amazon (ARN) dari Toko Data Acara CloudTrail Danau Anda. Anda dapat menemukan ini di CloudTrail konsol atau dengan menjalankan`aws cloudtrail list-event-data-stores`.

Langkah 2: Buat Tugas Impor

Gunakan `logs` layanan untuk membuat tugas. Anda harus menentukan sumber ARN dari Event Data Store.

```
aws logs create-import-task \
    --import-source-arn "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id" \
    --import-role-arn "arn:aws:iam::account-id:role/role-name" \
    --import-filter '{"startEventTime": START_TIME, "endEventTime": END_TIME}'
```

Parameter:

- `--import-source-arn`: ARN dari CloudTrail Lake Event Data Store yang berisi log sejarah.
- `--import-role-arn`: ARN dari peran IAM dengan izin yang benar.
- `--import-filter`: Objek opsional yang menentukan waktu mulai dan akhir acara yang ingin Anda impor.

Langkah 3: Pantau Status Tugas

Karena impor asinkron, Anda dapat memeriksa kemajuan migrasi menggunakan perintah: `describe-import-tasks`

```
aws logs describe-import-tasks \
    --import-id "import-id"
```

Sumber daya tambahan

- AWS CloudTrail Referensi API
- AWS CloudTrail Panduan Pengguna
- Panduan CloudWatch Pengguna Amazon
- Bekerja dengan aturan CloudWatch pemberdayaan telemetri
- CloudWatch Cross-account Sentralisasi log lintas wilayah

CloudTrail Penyimpanan data acara danau

Saat Anda membuat penyimpanan data peristiwa, Anda memilih jenis peristiwa yang akan disertakan dalam penyimpanan data acara Anda. Anda dapat membuat penyimpanan data peristiwa untuk menyertakan CloudTrail peristiwa (peristiwa manajemen, peristiwa data, peristiwa aktivitas jaringan), peristiwa CloudTrail Wawasan, item AWS Config konfigurasi , AWS Audit Manager bukti, atau peristiwa dari luar AWS. Setiap penyimpanan data peristiwa hanya dapat berisi kategori peristiwa tertentu (misalnya, item AWS Config konfigurasi), karena skema ??? peristiwa unik untuk kategori acara. Anda dapat menyimpan acara dari organisasi di AWS Organizations dalam penyimpanan data acara organisasi, termasuk acara dari beberapa Wilayah dan akun. Anda juga dapat menjalankan kueri SQL di beberapa penyimpanan data peristiwa menggunakan kata kunci SQL JOIN yang didukung. Untuk informasi tentang menjalankan kueri di beberapa penyimpanan data peristiwa, lihatDukungan kueri multi-tabel tingkat lanjut.

Anda dapat menyalin peristiwa jejak ke penyimpanan data peristiwa baru atau yang sudah ada untuk membuat snapshot point-in-time dari peristiwa yang dicatat ke jejak. Untuk informasi selengkapnya, lihat Salin peristiwa jejak ke penyimpanan data peristiwa.

Anda dapat menggabungkan penyimpanan data peristiwa untuk melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL pada data acara menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses

data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

Anda dapat melampirkan kebijakan berbasis sumber daya ke penyimpanan data acara untuk menyediakan akses lintas akun ke prinsipal yang dipilih. Anda dapat menambahkan kebijakan berbasis sumber daya saat membuat atau memperbarui penyimpanan data peristiwa di CloudTrail konsol, atau dengan menjalankan perintah AWS CLI `put-resource-policy`. Untuk informasi selengkapnya, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

Secara default, semua peristiwa di penyimpanan data peristiwa dienkripsi oleh CloudTrail. Saat Anda mengonfigurasi penyimpanan data peristiwa, Anda dapat memilih untuk menggunakan AWS Key Management Service kunci Anda sendiri. Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

Anda dapat mengontrol akses ke tindakan pada penyimpanan data peristiwa dengan menggunakan otorisasi berdasarkan tag. Untuk informasi dan contoh lebih lanjut, lihat Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag dalam panduan ini.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat membuat penyimpanan data peristiwa, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data peristiwa. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data peristiwa. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

CloudTrail Lake mendukung CloudWatch metrik Amazon, yang menyediakan informasi tentang data yang dicerna dan byte penyimpanan. Untuk informasi selengkapnya tentang CloudWatch metrik yang didukung, lihat CloudWatch Metrik yang didukung.

> **Note**
>
> CloudTrail biasanya mengirimkan acara dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin.

CloudTrail Kueri danau

CloudTrail Kueri Lake menawarkan tampilan acara yang lebih dalam dan lebih dapat disesuaikan daripada pencarian kunci dan nilai sederhana di ri wayat acara, atau berjalan`LookupEvents`. Pencarian riwayat peristiwa terbatas pada satu Akun AWS, hanya mengembalikan peristiwa dari satu Wilayah AWS, dan tidak dapat menanyakan beberapa atribut. Sebaliknya, pengguna CloudTrail Lake dapat menjalankan kueri SQL yang kompleks di beberapa bidang peristiwa. CloudTrail Lake mendukung semua `SELECT` pernyataan dan fungsi Trino yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Trino.

Anda dapat membuat kueri pada tab CloudTrail Lake Editor dengan menulis kueri di SQL dari awal, dengan membuka kueri yang disimpan atau sampel dan mengeditnya, atau dengan menggunakan generator kueri untuk menghasilkan kueri dari prompt bahasa Inggris. Untuk informasi selengkapnya, lihat Membuat atau mengedit kueri dengan CloudTrail konsol dan Buat kueri CloudTrail Danau dari petunjuk bahasa alami.

Anda dapat menyimpan kueri CloudTrail Lake untuk penggunaan di masa mendatang, dan melihat hasil kueri hingga tujuh hari. Saat menjalankan kueri, Anda dapat menyimpan hasil kueri ke bucket Amazon S3.

Kon CloudTrail sol menyediakan sejumlah kueri sampel yang dapat membantu Anda mulai menulis kueri Anda sendiri. Untuk informasi selengkapnya, lihat Lihat contoh kueri dengan konsol CloudTrail.

CloudTrail Kueri danau dikenakan biaya. Ketika Anda menjalankan kueri di Lake, Anda membayar berdasarkan jumlah data yang dipindai. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

CloudTrail Dasbor danau

Anda dapat menggunakan CloudTrail dasbor Lake untuk melihat tren acara untuk penyimpanan data acara di akun Anda. CloudTrail Danau menawarkan jenis dasbor berikut:

- Dasbor terkelola — Anda dapat melihat dasbor terkelola untuk melihat tren peristiwa untuk penyimpanan data peristiwa yang mengumpulkan peristiwa manajemen, peristiwa data, atau peristiwa Wawasan. Dasbor ini secara otomatis tersedia untuk Anda dan dikelola oleh CloudTrail Lake. CloudTrail menawarkan 14 dasbor terkelola untuk dipilih. Anda dapat menyegarkan dasbor terkelola secara manual. Anda tidak dapat mengubah, menambah, atau menghapus widget untuk

dasbor ini, namun, Anda dapat menyimpan dasbor terkelola sebagai dasbor khusus jika Anda ingin memodifikasi widget atau mengatur jadwal penyegaran.

- Dasbor kustom - Dasbor kustom memungkinkan Anda untuk menanyakan peristiwa dalam jenis penyimpanan data acara apa pun. Anda dapat menambahkan hingga 10 widget ke dasbor kustom. Anda dapat menyegarkan dasbor khusus secara manual, atau Anda dapat mengatur jadwal penyegaran.
- Dasbor Sorotan — Aktifkan dasbor Sorotan untuk melihat ikhtisar sekilas AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Dasbor Sorotan dikelola oleh CloudTrail dan menyertakan widget yang relevan dengan akun Anda. Widget yang ditampilkan di dasbor Sorotan unik untuk setiap akun. Widget ini dapat mendeteksi aktivitas abnormal atau anomali di permukaan. Misalnya, dasbor Sorotan Anda dapat menyertakan widget Total akses lintas akun, yang menunjukkan jika ada peningkatan aktivitas lintas akun yang tidak normal. CloudTrail memperbarui dasbor Highlights setiap 6 jam. Dasbor menunjukkan data 24 jam terakhir dari pembaruan terakhir.

Setiap dashboard terdiri dari satu atau lebih widget dan setiap widget mewakili query SQL.

Untuk informasi selengkapnya, lihat CloudTrail Dasbor danau.

CloudTrail Integrasi danau

Anda dapat menggunakan integrasi CloudTrail Lake untuk mencatat dan menyimpan data aktivitas pengguna dari luar AWS; dari sumber apa pun di lingkungan hibrida Anda, seperti aplikasi in-house atau SaaS yang dihosting di lokasi atau di cloud, mesin virtual, atau wadah. Setelah membuat penyimpanan data peristiwa di CloudTrail Lake dan membuat saluran untuk mencatat peristiwa aktivitas, Anda memanggil `PutAuditEvents` API untuk memasukkan aktivitas aplikasi Anda ke CloudTrail dalamnya. Anda kemudian dapat menggunakan CloudTrail Lake untuk mencari, menanyakan, dan menganalisis data yang dicatat dari aplikasi Anda.

Integrasi juga dapat mencatat peristiwa ke penyimpanan data acara Anda dari lebih dari selusin CloudTrail mitra. Dalam integrasi mitra, Anda membuat penyimpanan data acara tujuan, saluran, dan kebijakan sumber daya. Setelah Anda membuat integrasi, Anda memberikan saluran ARN kepada mitra. Ada dua jenis integrasi: langsung dan solusi. Dengan integrasi langsung, mitra memanggil `PutAuditEvents` API untuk mengirimkan acara ke penyimpanan data acara untuk AWS akun Anda. Dengan integrasi solusi, aplikasi berjalan di AWS akun Anda dan aplikasi memanggil `PutAuditEvents` API untuk mengirimkan acara ke penyimpanan data acara untuk AWS akun Anda.

Untuk informasi selengkapnya tentang integrasi, lihat Membuat integrasi dengan sumber peristiwa di luar. AWS

Sumber daya tambahan

Sumber daya berikut dapat membantu Anda mendapatkan pemahaman yang lebih baik tentang apa itu CloudTrail Danau dan bagaimana Anda dapat menggunakannya.

- Modernisasi Manajemen Log Audit Anda Menggunakan CloudTrail Danau (YouTube video)
- Catatan Acara Aktivitas dari Non-AWS Sumber di AWS CloudTrail Danau (YouTube video)
- Analisis Log Aktivitas dengan AWS CloudTrail Danau dan Amazon Athena (YouTube video)
- Dapatkan visibilitas ke log aktivitas untuk identitas tenaga kerja dan pelanggan Anda (AWS blog)
- Menggunakan AWS CloudTrail Lake untuk mengidentifikasi koneksi TLS lama ke titik AWS akhir layanan (blog)AWS
- Bagaimana Arctic Wolf menggunakan AWS CloudTrail Danau untuk Menyederhanakan Keamanan dan Oper asi (AWS blog)
- CloudTrail Danau FAQ
- AWS CloudTrail Referensi API
- AWS CloudTrail Referensi API Data
- AWS CloudTrail Panduan Onboarding Mitra

CloudTrail Daerah yang didukung Danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Saat ini, CloudTrail Danau didukung sebagai berikut Wilayah AWS:

Nama Wilayah	Region
AS Timur (Virginia Utara)	us-east-1
US East (Ohio)	us-east-2
AS Barat (California Utara)	us-west-1
US West (Oregon)	as-barat-2
Afrika (Cape Town)	af-selatan-1
Asia Pasifik (Hong Kong)	ap-east-1
Asia Pasifik (Hyderabad)	ap-south-2
Asia Pasifik (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Asia Pasifik (Mumbai)	ap-south-1
Asia Pacific (Osaka)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-sentral-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-barat-2
Eropa (Milan)	eu-selatan-1

Nama Wilayah	Region
Eropa (Paris)	eu-west-3
Eropa (Spanyol)	eu-south-2
Eropa (Stockholm)	eu-north-1
Europe (Zurich)	eu-central-2
Israel (Tel Aviv)	il-central-1
Timur Tengah (Bahrain)	me-south-1
Timur Tengah (UAE)	me-central-1
Amerika Selatan (Sao Paulo)	sa-east-1
AWS GovCloud (AS-Timur)	us-gov-east-1
AWS GovCloud (AS-Barat)	us-gov-west-1

Untuk informasi tentang titik akhir CloudTrail layanan, lihat AWS CloudTrail titik akhir dan kuota.

Untuk informasi selengkapnya tentang penggunaan CloudTrail di AWS GovCloud (US) Regions, lihat Titik Akhir Layanan di Panduan AWS GovCloud (US) Pengguna.

CloudTrail Konsep dan terminologi danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Bagian ini menjelaskan konsep dan istilah kunci untuk membantu Anda menggunakan AWS CloudTrail Lake.

Konsep dan istilah

- Menyimpan data acara
- Integrasi
- Kueri
- Dasbor

Menyimpan data acara

Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut.

Anda dapat membuat penyimpanan data peristiwa untuk mencatat CloudTrail peristiwa (peristiwa manajemen, peristiwa data, peristiwa aktivitas jaringan), peristiwa CloudTrailWawasan, AWS Audit Manager bukti, item AWS Config konfigurasi, atau peristiwa di luar. AWS

Penyeleksi acara tingkat lanjut

Penyeleksi acara tingkat lanjut menentukan acara mana yang akan disertakan dalam penyimpanan data acara. Penyeleksi acara tingkat lanjut membantu Anda mengontrol biaya dengan mencatat hanya peristiwa yang penting bagi Anda.

Untuk acara manajemen, peristiwa data, dan peristiwa aktivitas jaringan, Anda dapat menggunakan pemilih acara lanjutan untuk memfilter peristiwa. Misalnya, jika Anda membuat penyimpanan data peristiwa untuk mengumpulkan peristiwa manajemen, Anda dapat memfilter peristiwa API Data AWS Key Management Service (AWS KMS) atau Amazon Relational Database Service (Amazon RDS). Biasanya, AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` menghasilkan lebih dari 99 persen peristiwa.

Untuk item AWS Config konfigurasi, bukti Audit Manager, atau peristiwa di luar AWS, penyeleksi peristiwa lanjutan hanya digunakan untuk menyertakan peristiwa jenis tersebut di penyimpanan data peristiwa.

Federation

Federation memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL pada data peristiwa menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data

memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri.

Saat Anda mengaktifkan federasi kueri Lake, CloudTrail buat sumber daya federasi atas nama Anda dan daftarkan sumber daya tersebut. AWS Lake Formation Setelah federasi Danau diaktifkan, Anda dapat langsung menanyakan data acara Anda di Athena tanpa perlu melakukan langkah tambahan apa pun. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

Opsi harga

Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi tentang harga, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

Periode retensi

Periode retensi penyimpanan data peristiwa menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail Lake menentukan apakah akan mempertahankan suatu peristiwa dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode retensi 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

Periode retensi default

Periode retensi default penyimpanan data peristiwa adalah jumlah hari default dimana data peristiwa disimpan di penyimpanan data acara. Selama periode penyimpanan default penyimpanan data acara, penyimpanan disertakan dengan harga konsumsi tanpa biaya tambahan. Setelah periode retensi default, harga untuk penyimpanan adalah pay-as-you-go.

Periode retensi maksimum

Periode retensi maksimum penyimpanan data peristiwa mewakili jumlah hari maksimum yang dapat Anda simpan data di penyimpanan data peristiwa.

Perlindungan pengakhiran

Secara default, penyimpanan data peristiwa mengaktifkan perlindungan penghentian, yang melindungi penyimpanan data peristiwa agar tidak terhapus secara tidak sengaja. Untuk menghapus penyimpanan data peristiwa dengan perlindungan penghentian diaktifkan, pilih

Ubah perlindungan penghentian dari menu Tindakan di halaman detail penyimpanan data acara. Kemudian Anda dapat melanjutkan dengan menghapus penyimpanan data acara. Untuk informasi selengkapnya, lihat Ubah perlindungan penghentian dengan konsol.

Integrasi

Anda dapat menggunakan integrasi CloudTrail Lake untuk mencatat dan menyimpan data aktivitas pengguna dari sumber berikut:

- Di luar AWS
- Sumber apa pun di lingkungan hybrid Anda, seperti aplikasi in-house atau perangkat lunak sebagai layanan (SaaS) yang dihosting di tempat atau di cloud, mesin virtual, atau wadah

Integrasi membutuhkan saluran untuk menyampaikan acara dan penyimpanan data acara untuk menerima acara. Setelah Anda menyiapkan integrasi, panggil operasi PutAuditEventsAPI untuk memasukkan aktivitas aplikasi Anda ke dalamnya CloudTrail. Kemudian, Anda dapat menggunakan CloudTrail Lake untuk mencari, menanyakan, dan menganalisis data yang dicatat dari aplikasi Anda. Untuk informasi selengkapnya, lihat Buat integrasi dengan sumber acara di luar AWS.

Tipe integrasi

Ada dua jenis integrasi: langsung dan solusi. Dengan integrasi langsung, mitra memanggil operasi `PutAuditEvents` API untuk mengirimkan peristiwa ke penyimpanan data acara untuk Anda Akun AWS. Dengan integrasi solusi, aplikasi berjalan di dalam Anda Akun AWS dan aplikasi memanggil operasi `PutAuditEvents` API untuk mengirimkan peristiwa ke penyimpanan data acara untuk Anda Akun AWS.

Saluran

Aktivitas acara dari sumber di luar AWS pekerjaan dengan menggunakan saluran untuk membawa acara ke CloudTrail Danau dari mitra eksternal yang bekerja dengan CloudTrail, atau dari sumber Anda sendiri. Saat membuat saluran, Anda memilih satu atau beberapa penyimpanan data acara untuk menyimpan peristiwa yang datang dari sumber saluran. Anda dapat mengubah penyimpanan data peristiwa tujuan untuk saluran sesuai kebutuhan, selama penyimpanan data peristiwa tujuan disetel ke `eventCategory="ActivityAuditLog"` peristiwa log. Saat Anda membuat saluran untuk acara dari mitra eksternal, Anda memberikan saluran Nama Sumber Daya Amazon (ARN) ke mitra atau aplikasi sumber.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Kebijakan berbasis sumber daya yang dilampirkan pada saluran memungkinkan sumber untuk mengirimkan peristiwa melalui saluran. Jika channel tidak memiliki kebijakan sumber daya, hanya pemilik channel yang dapat memanggil operasi `PutAuditEvents` API di channel tersebut. Untuk informasi selengkapnya, lihat AWS CloudTrail contoh kebijakan berbasis sumber daya.

Kueri

Pertanyaan di CloudTrail Lake ditulis dalam SQL. Anda dapat membuat kueri di tab CloudTrail Lake Editor dengan menulis kueri di SQL dari awal, dengan membuka kueri yang disimpan atau sampel dan mengeditnya, atau dengan menggunakan generator kueri untuk menghasilkan kueri dari prompt bahasa Inggris. Untuk informasi selengkapnya, lihat Membuat atau mengedit kueri dengan CloudTrail konsol dan Buat kueri CloudTrail Danau dari petunjuk bahasa alami.

CloudTrail Lake mendukung semua Trino `SELECT` pernyataan dan fungsi yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web Trino dokumentasi.

Dasbor

Dengan menggunakan dasbor CloudTrail Lake, Anda dapat memvisualisasikan peristiwa di penyimpanan data acara dan melihat tren peristiwa, seperti top, pengguna Layanan AWS, dan kesalahan. Untuk informasi selengkapnya, lihat CloudTrail Dasbor danau.

Jenis dasbor

CloudTrail Lake menawarkan jenis dasbor berikut:

- Dasbor terkelola — Anda dapat melihat dasbor terkelola untuk melihat tren acara untuk penyimpanan data acara yang mengumpulkan peristiwa manajemen, peristiwa data, atau peristiwa Wawasan. Dasbor ini secara otomatis tersedia untuk Anda dan dikelola oleh CloudTrail Lake. CloudTrail menawarkan 14 dasbor terkelola untuk dipilih. Anda dapat menyegarkan dasbor terkelola secara manual. Anda tidak dapat memodifikasi, menambah, atau menghapus widget untuk dasbor ini, namun, Anda dapat menyimpan dasbor terkelola sebagai dasbor khusus jika Anda ingin memodifikasi widget atau mengatur jadwal penyegaran.

- Dasbor khusus - Dasbor khusus memungkinkan Anda untuk menanyakan peristiwa dalam jenis penyimpanan data acara apa pun. Anda dapat menambahkan hingga 10 widget ke dasbor kustom. Anda dapat menyegarkan dasbor kustom secara manual, atau Anda dapat mengatur jadwal penyegaran.
- Dasbor Sorotan — Aktifkan dasbor Sorotan untuk melihat at-a-glance ikhtisar AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Dasbor Sorotan dikelola oleh CloudTrail dan menyertakan widget yang relevan dengan akun Anda. Widget yang ditampilkan di dasbor Sorotan unik untuk setiap akun. Widget ini dapat muncul aktivitas abnormal atau anomali yang terdeteksi. Misalnya, dasbor Sorotan Anda dapat menyertakan widget akses lintas akun Total, yang menunjukkan jika ada peningkatan aktivitas lintas akun yang tidak normal. CloudTrail memperbarui dasbor Sorotan setiap 6 jam. Dasbor menunjukkan 24 jam terakhir data dari pembaruan terakhir.

Widget

Widget adalah komponen yang membentuk dasbor dan memberikan visualisasi, seperti diagram garis atau diagram batang. Setiap widget sesuai dengan query SQL. Saat Anda menyegarkan dasbor, CloudTrail jalankan kueri untuk setiap widget di dasbor untuk mengisi data widget.

CloudTrail Penyimpanan data acara danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Saat Anda membuat penyimpanan data peristiwa di CloudTrail Lake, Anda memilih jenis acara yang akan disertakan dalam penyimpanan data acara Anda. Anda dapat membuat penyimpanan data peristiwa untuk menyertakan CloudTrail peristiwa (peristiwa manajemen, peristiwa data, atau peristiwa aktivitas jaringan), peristiwa CloudTrail Wawasan, item AWS Config konfigurasi, atau peristiwa di luar AWS. Setiap jenis penyimpanan data peristiwa hanya dapat berisi kategori peristiwa tertentu (misalnya, item AWS Config konfigurasi), karena skema peristiwa unik untuk kategori acara. Anda dapat menjalankan kueri SQL di beberapa penyimpanan data peristiwa menggunakan

kata kunci SQL JOIN yang didukung. Untuk informasi tentang menjalankan kueri di beberapa penyimpanan data peristiwa, lihatDukungan kueri multi-tabel tingkat lanjut.

Tabel berikut menunjukkan kategori acara yang didukung untuk setiap jenis penyimpanan data peristiwa. Kol om EventCategory menunjukkan nilai yang akan Anda tentukan di pemilih acara lanjutan untuk mengumpulkan peristiwa jenis itu.

Jenis acara (konsol)	Kategori acara (API)	Deskripsi

CloudTrail acara	`Management`
	`Data`
	`NetworkActivity`
		Jenis penyimpanan data peristiwa ini dapat mengumpulkan peristiwa CloudTrai l manajemen, peristiwa data, dan peristiwa aktivitas jaringan. Untuk informasi selengkap nya, lihat Membuat penyimpanan data acara untuk CloudTrail acara.

CloudTrail Peristiwa wawasan	`Insight`	Jenis penyimpanan data peristiwa ini dapat mengumpulkan peristiwa CloudTrail Wawasan. Untuk menerima peristiwa Insights, Anda memerlukan penyimpanan data peristiwa sumber yang mencatat peristiwa CloudTrai l manajemen dan mengaktifkan Wawasan. Untuk informasi tentang membuat penyimpan an data peristiwa sumber dan tujuan, lihat Membuat penyimpanan data peristiwa untuk peristiwa CloudTrail Wawasan.
Item konfigurasi	`ConfigurationItem`	Jenis penyimpanan data peristiwa ini dapat mengumpulkan item AWS Config konfigurasi. Untuk informasi selengkapnya, lihat Membuat penyimpanan data peristiwa untuk item AWS Config konfigurasi.
Peristiwa dari integrasi	`ActivityAuditLog`	Jenis penyimpanan data peristiwa ini dapat mengumpulkan non-AWS peristiwa dari integrasi. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk acara di luar AWS.

Anda juga dapat membuat penyimpanan data peristiwa untuk AWS Audit Manager bukti dengan menggunakan konsol Audit Manager. Untuk informasi selengkapnya tentang mengumpulkan bukti di CloudTrail Lake menggunakan Audit Manager, lihat Memahami cara kerja pencari bukti dengan CloudTrail Lake di Panduan AWS Audit Manager Pengguna.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat membuat penyimpanan data peristiwa, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data peristiwa. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data peristiwa. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

Bagian berikut menjelaskan cara membuat, memperbarui, dan mengelola penyimpanan data acara.

Topik

- Buat, perbarui, dan kelola penyimpanan data peristiwa dengan konsol
- Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI
- Mengelola siklus hidup penyimpanan data acara
- Salin peristiwa jejak ke penyimpanan data peristiwa
- Menyatukan penyimpanan data acara
- Memahami penyimpanan data acara organisasi

Buat, perbarui, dan kelola penyimpanan data peristiwa dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat menggunakan CloudTrail konsol untuk membuat, memperbarui, menghapus, dan memulihkan penyimpanan data acara.

Anda dapat memperbarui pengaturan berikut menggunakan CloudTrail konsol:

- Anda dapat mengubah opsi harga dari harga Seven-year retensi menjadi harga reten si One-year yang dapat diperpanjang.
- Anda dapat memperbarui periode retensi untuk penyimpanan data peristiwa. Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data peristiwa.
- Anda dapat mengonversi penyimpanan data peristiwa multi-wilayah ke penyimpanan data peristiwa satu wilayah, atau mengonversi penyimpanan data peristiwa satu wilayah ke penyimpanan data peristiwa multi-wilayah.
- Akun manajemen untuk AWS Organizations organisasi dapat mengonversi penyimpanan data peristiwa tingkat akun ke penyimpanan data peristiwa organisasi, atau dapat mengonversi penyimpanan data peristiwa organisasi ke penyimpanan data peristiwa tingkat akun. Pengaturan ini tidak tersedia di penyimpanan data peristiwa yang mengumpulkan peristiwa di luar AWS.
- Anda dapat mengaktifkan atau menonaktifkan federasi kueri Danau. Dengan menggabungkan penyimpanan data acara, Anda dapat menanyakan data acara Anda dari Amazon Athena.
- Anda dapat menambahkan atau mengedit kebijakan berbasis sumber daya untuk penyimpanan data peristiwa untuk menyediakan akses lintas akun ke penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.
- Anda dapat menghentikan penyerapan peristiwa dan memulai ulang penyerapan peristiwa pada penyimpanan data peristiwa yang mengumpulkan peristiwa manajemen, peristiwa data, atau item AWS Config konfigurasi.
- Anda dapat mengaktifkan atau menonaktifkan perlindungan penghentian. Mengaktifkan perlindungan penghentian melindungi penyimpanan data peristiwa agar tidak dihapus secara tidak sengaja. Perlindungan penghentian diaktifkan secara default.
- Anda dapat memulihkan penyimpanan data peristiwa yang sedang menunggu penghapusan.
- Anda dapat menambahkan atau menghapus tag. Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda.
- Anda dapat menambahkan kunci KMS untuk mengenkripsi penyimpanan data acara Anda. Anda tidak dapat menghapus kunci KMS dari penyimpanan data peristiwa.

Menggunakan CloudTrail konsol untuk membuat atau memperbarui penyimpanan data acara memberikan keuntungan berikut:

- Jika Anda mengonfigurasi penyimpanan data peristiwa untuk mengumpulkan peristiwa data, menggunakan CloudTrail konsol memungkinkan Anda untuk melihat jenis sumber daya peristiwa data yang tersedia. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data.
- Jika Anda mengonfigurasi penyimpanan data peristiwa untuk mengumpulkan peristiwa aktivitas jaringan, menggunakan CloudTrail konsol memungkinkan Anda untuk melihat sumber peristiwa yang dapat Anda catat peristiwa aktivitas jaringan. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.
- Jika Anda mengonfigurasi penyimpanan data acara untuk mengumpulkan peristiwa di luar AWS, menggunakan CloudTrail konsol memungkinkan Anda melihat informasi tentang mitra yang tersedia. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk acara di luar AWS dengan konsol.

Topik

- Membuat penyimpanan data acara untuk CloudTrail acara dengan konsol
- Membuat penyimpanan data acara untuk acara Insights dengan konsol
- Buat penyimpanan data acara untuk item konfigurasi dengan konsol
- Membuat penyimpanan data acara untuk acara di luar AWS dengan konsol
- Memperbarui penyimpanan data acara dengan konsol
- Hentikan dan mulai penyerapan acara dengan konsol
- Ubah perlindungan penghentian dengan konsol
- Menghapus penyimpanan data acara dengan konsol
- Memulihkan penyimpanan data acara dengan konsol
- Mengekspor data dari CloudTrail Lake Event Data Store ke CloudWatch

Membuat penyimpanan data acara untuk CloudTrail acara dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Penyimpanan data acara untuk CloudTrail acara dapat mencakup peristiwa CloudTrail manajemen, peristiwa data, dan peristiwa aktivitas jaringan. Anda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika memilih opsi harga retensi One-year yang dapat diperpanjang, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi. Seven-year

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat membuat penyimpanan data peristiwa, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data peristiwa. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data peristiwa. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

Untuk membuat penyimpanan data acara untuk CloudTrail acara

Gunakan prosedur ini untuk membuat penyimpanan data peristiwa yang mencatat peristiwa CloudTrail manajemen, peristiwa data, atau peristiwa aktivitas jaringan.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, masukkan nama untuk penyimpanan data peristiwa. Sebuah nama diperlukan.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
     - Periode retensi default: 366 hari

    - Periode retensi maksimum: 3.653 hari
- Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
    - Periode retensi default: 2.557 hari
    - Periode retensi maksimum: 2.557 hari

6. Tentukan periode retensi untuk penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

   CloudTrail Lake menentukan apakah acara akan dipertahankan dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode penyimpanan 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

   > **Note**
   >
   > Jika Anda menyalin peristiwa jejak ke penyimpanan data peristiwa ini, tidak CloudTrail akan menyalin peristiwa jika peristiwa tersebut `eventTime` lebih lama dari periode retensi yang ditentukan. Untuk menentukan periode penyimpanan yang sesuai, ambil jumlah peristiwa terlama yang ingin Anda salin dalam hari dan jumlah hari yang ingin Anda simpan peristiwa di penyimpanan data peristiwa (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika peristiwa terlama yang Anda salin berusia 45 hari dan Anda ingin menyimpan peristiwa di penyimpanan data peristiwa selama 45 hari lagi, Anda akan menetapkan periode retensi menjadi 90 hari.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/`*`MyAliasName`*. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar penyimpanan data acara dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

> **Note**
>
> Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

   Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

   a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

   b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

   c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

10. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag di AWS, lihat Men andai sumber AWS daya di Panduan Pengguna Menandai Sumber AWS Daya.
11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
12. Pada halaman Pilih acara, pilih AWS acara, lalu pilih CloudTrail acara.

13. Untuk CloudTrail acara, pilih setidaknya satu jenis acara. Secara default, acara manajemen dipilih. Anda dapat menambahkan peristiwa manajemen, peristiwa data, dan peristiwa aktivitas jaringan ke penyimpanan data acara Anda.
14. (Opsional) Pilih Salin peristiwa jejak jika Anda ingin menyalin peristiwa dari jejak yang ada untuk menjalankan kueri pada peristiwa sebelumnya. Untuk menyalin peristiwa jejak ke penyimpanan data acara organisasi, Anda harus menggunakan akun manajemen untuk organisasi. Akun administrator yang didelegasikan tidak dapat menyalin peristiwa jejak ke penyimpanan data peristiwa organisasi. Untuk informasi selengkapnya tentang pertimbangan untuk menyalin peristiwa jejak, lihatPertimbangan untuk menyalin acara jejak.
15. Agar penyimpanan data acara Anda mengumpulkan peristiwa dari semua akun dalam AWS Organizations organisasi, pilih Aktifkan untuk semua akun di organisasi saya. Anda harus masuk ke akun manajemen atau akun administrator yang didelegasikan agar organisasi dapat membuat penyimpanan data peristiwa yang mengumpulkan peristiwa untuk organisasi.

    > **Note**
    >
    > Untuk menyalin peristiwa jejak atau mengaktifkan peristiwa Wawasan, Anda harus masuk ke akun manajemen untuk organisasi Anda.

16. Per luas Pengaturan tambahan untuk memilih apakah Anda ingin penyimpanan data acara mengumpulkan peristiwa untuk semua Wilayah AWS, atau hanya saat ini Wilayah AWS, dan pilih apakah penyimpanan data acara menyerap peristiwa. Secara default, penyimpanan data acara Anda mengumpulkan peristiwa dari semua Wilayah di akun Anda dan mulai mengambil peristiwa saat dibuat.

    a. Pilih Sertakan hanya wilayah saat ini di penyimpanan data acara saya untuk menyertakan hanya peristiwa yang dicatat di Wilayah saat ini. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda menyertakan acara dari semua Wilayah.

    b. Batalkan pilihan Ingest event jika Anda tidak ingin penyimpanan data acara mulai mengambil peristiwa. Misalnya, Anda mungkin ingin membatalkan pilihan Ingest event, jika Anda menyalin peristiwa jejak dan tidak ingin penyimpanan data peristiwa menyertakan peristiwa masa depan. Secara default, penyimpanan data peristiwa mulai menyerap peristiwa saat dibuat.

17. Jika penyimpanan data acara Anda menyertakan peristiwa manajemen, Anda dapat memilih dari opsi berikut. Untuk informasi selengkapnya tentang acara manajemen, lihatMencatat log peristiwa manajemen.

a. Pilih antara koleksi acara sederhana atau koleksi acara lanjutan:

   - Pilih Koleksi acara sederhana jika Anda ingin mencatat semua peristiwa, mencatat hanya peristiwa yang dibaca, atau log hanya menulis peristiwa. Anda juga dapat memilih untuk mengecualikan AWS Key Management Service dan acara API Data Amazon RDS.
   - Pilih Koleksi acara lanj utan jika Anda ingin menyertakan atau mengecualikan peristiwa manajemen berdasarkan nilai bidang pemilih peristiwa lanjutan, termasuk bidang`eventName`,`eventType`,`eventSource`,`sessionCredentialFromConsole`, dan`userIdentity.arn`.

b. Jika Anda memilih Koleksi acara sederhana, pilih apakah Anda ingin mencatat semua peristiwa, mencatat hanya peristiwa yang dibaca, atau log hanya menulis peristiwa. Anda juga dapat memilih untuk mengecualikan AWS KMS dan acara API Data Amazon RDS.

c. Jika Anda memilih Koleksi acara lanj utan, buat pilihan berikut:

   i. Di Template pemilih log, pilih template yang telah ditentukan sebelumnya, atau Kustom untuk membuat konfigurasi khusus berdasarkan nilai bidang pemilih peristiwa lanjutan.

      Anda dapat memilih dari template yang telah ditentukan sebelumnya berikut:

      - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
      - Log hanya membaca acara - Pilih template ini untuk mencatat hanya peristiwa baca. Read-only peristiwa adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa.
      - Log hanya menulis peristiwa - Pilih template ini untuk mencatat hanya menulis peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa.
      - Log saja Konsol Manajemen AWS peristiwa - Pilih template ini untuk mencatat hanya peristiwa yang berasal dari Konsol Manajemen AWS.
      - Kecualikan peristiwa yang Layanan AWS dimulai — Pilih template ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` of`AwsServiceEvent`, dan peristiwa yang dimulai dengan peran Layanan AWS-link (SLR).

   ii. (Opsional) Di Nama pemilih, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log

manajemen peristiwa dari Konsol Manajemen AWS sesi". Nama pemilih terdaftar seperti `Name` pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

iii. Jika Anda memilih K ustom, dalam pemilih acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selektor tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

A. Pilih dari bidang berikut.

- **`readOnly`**— `readOnly` dapat disetel menjadi sama dengan nilai `true` atau`false`. Ketika disetel ke`false`, penyimpanan data peristiwa mencatat peristiwa Write-only manajemen. Read-only peristiwa manajemen adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa. Untuk mencatat peristiwa Baca dan Tulis, jangan tambahkan pem `readOnly` ilih.
- **`eventName`**— `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara manajemen apa pun, seperti `CreateAccessPoint` atau`GetAccessPoint`.
- **`userIdentity.arn`**— Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail userIdentity.
- **`sessionCredentialFromConsole`**— Sertakan atau mengecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diset el menjadi sama atau tidak sama dengan nilai`true`.
- **`eventSource`**— Anda dapat menggunakannya untuk memasukkan atau mengecualikan sumber acara tertentu. Biasanya `eventSource` merupakan bentuk pendek dari nama layanan tanpa spasi plus`.amazonaws.com`. Misalnya,

Anda dapat menyetel `eventSource` sama dengan `ec2.amazonaws.com` untuk mencatat hanya peristiwa manajemen Amazon EC2.

- **`eventType`**- EventType untuk disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini menjadi tidak sama untuk `AwsServiceEvent` mengecualikan Layanan AWS peristiwa.

B. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat.

Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua pemilih pada penyimpanan data peristiwa. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi ditambahkan ke pemilih.

C. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan menetapkan nilai yang bertentangan atau duplikat untuk bidang.

iv. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

d. Pilih Aktifkan penangkapan peristiwa Wawasan untuk mengaktifkan Wawasan. Untuk mengaktifkan Wawasan, Anda perlu menyiapkan penyimpanan data peristiwa tujuan untuk mengumpulkan peristiwa Wawasan berdasarkan aktivitas peristiwa manajemen di penyimpanan data acara ini.

Jika Anda memilih untuk mengaktifkan Wawasan, lakukan hal berikut.

i. Pilih toko acara tujuan yang akan mencatat peristiwa Insights. Penyimpanan data acara tujuan akan mengumpulkan peristiwa Wawasan berdasarkan aktivitas acara manajemen di penyimpanan data acara ini. Untuk informasi tentang cara membuat penyimpanan data acara tujuan, lihatUntuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.

ii. Pilih jenis Wawasan. Anda dapat memilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Anda harus mencatat peristiwa manajemen T ulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau T ulis untuk mencatat peristiwa Insights untuk tingkat kesalahan API.

18. Untuk menyertakan peristiwa data di penyimpanan data acara Anda, lakukan hal berikut.

    a. Pilih jenis sumber daya. Ini adalah Layanan AWS sumber daya di mana peristiwa data dicatat.

    b. Di Template pemilih log, pilih template yang telah ditentukan sebelumnya, atau pilih K ustom untuk menentukan kondisi pengumpulan acara Anda sendiri berdasarkan nilai bidang pemilih acara lanjutan.

       Anda dapat memilih dari template yang telah ditentukan sebelumnya berikut:

       - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
       - Log hanya membaca acara - Pilih template ini untuk mencatat hanya peristiwa baca. Read-only peristiwa adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa.
       - Log hanya menulis peristiwa - Pilih template ini untuk mencatat hanya menulis peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau `Write*` peristiwa.
       - Log saja Konsol Manajemen AWS peristiwa - Pilih template ini untuk mencatat hanya peristiwa yang berasal dari Konsol Manajemen AWS.
       - Kecualikan peristiwa yang Layanan AWS dimulai — Pilih template ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` ofAwsServiceEvent, dan peristiwa yang dimulai dengan peran Layanan AWS-link (SLR).

    c. (Opsional) Di Nama pemilih, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti `Name` pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

    d. Jika Anda memilih Kustom, dalam pemilih acara lanj utan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selektor tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

i. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,`Delete*`, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan pem `readOnly` ilih.
- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk memasukkan atau mengecualikan peristiwa data apa pun CloudTrail yang dicatat, sepertiPutBucket,`GetItem`, atau`GetSnapshotBlock`.
- **`eventSource`**— Sumber acara untuk disertakan atau dikecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini menjadi tidak sama untuk `AwsServiceEvent` mengecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType` diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- session CredentialFromConsole — Sertakan atau mengecualikan peristiwa yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur menjadi sama atau tidak sama dengan nilai`true`.
- user Identity.arn — Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail userIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.ARN`, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai`resources.type`.

> **Note**
>
> Anda tidak dapat menggunakan `resources.ARN` bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat T indakan, sumber daya, dan kunci kondisi untuk Layanan AWS di Referensi Otorisasi Layanan.

ii. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data peristiwa Anda, Anda dapat mengatur bidang ke Resources.arn, menyetel operator untuk tidak dimulai dengan, lalu tempel di bucket S3 ARN yang tidak ingin Anda catat peristiwa.

Untuk menambahkan bucket S3 kedua, pilih + Kondisi, lalu ulangi instruksi sebelumnya, tempelkan ARN untuk atau menelusuri bucket yang berbeda.

Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua pemilih pada penyimpanan data peristiwa. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi ditambahkan ke pemilih.

iii. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan menetapkan nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan menentukan ARN dalam satu pemilih untuk sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

e. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

f. Untuk menambahkan jenis sumber daya lain yang digunakan untuk mencatat peristiwa data, pilih Tambahkan jenis peristiwa data. Ulangi langkah a melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk jenis sumber daya.

19. Untuk menyertakan peristiwa aktivitas jaringan di penyimpanan data acara Anda, lakukan hal berikut.

a. Dari Sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

b. Di Template pemilih log, pilih template. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua aktivitas jaringan peristiwa yang ditolak akses, atau memilih K ustom untuk membuat pemilih log khusus untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

d. Dalam pemilih acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan sebelumnya.

   i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

      - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
      - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
      - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilalui operasi. Anda dapat menggunakan operator apa pun dengan `vpcEndpointId`.

   ii. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat.

   iii. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan menetapkan nilai yang bertentangan atau duplikat untuk bidang.

e. Untuk menambahkan sumber peristiwa lain yang ingin Anda catat peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

20. Untuk menyalin peristiwa jejak yang ada ke penyimpanan data acara Anda, lakukan hal berikut.

    a. Pilih jejak yang ingin Anda salin. Secara default, CloudTrail hanya meny CloudTrail alin peristiwa yang terdapat dalam awalan bucket `CloudTrail` S3 dan awalan di dalam `CloudTrail` awalan, dan tidak memeriksa awalan untuk layanan lain AWS . Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, pilih Masukkan URI S3, lalu pilih Jelajahi S3 untuk menelusuri ke awalan. Jika bucket S3 sumber untuk jejak menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data. Jika bucket S3 sumber Anda menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci CloudTrail untuk memungkinkan mendekripsi data dalam bucket. Untuk informasi selengkapnya tentang memperbarui kebijakan kunci KMS, lihatKebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber.

    b. Pilih rentang waktu untuk menyalin acara. CloudTrail memeriksa awalan dan nama file log untuk memverifikasi nama berisi tanggal antara tanggal mulai dan akhir yang dipilih sebelum mencoba menyalin peristiwa jejak. Anda dapat memilih rentang Relatif atau Rentang Absolut. Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang waktu yang lebih awal dari pembuatan penyimpanan data peristiwa.

    > **Note**
    >
    > CloudTrail hanya menyalin peristiwa jejak yang memiliki periode retensi `eventTime` dalam penyimpanan data peristiwa. Misalnya, jika periode retensi penyimpanan data peristiwa adalah 90 hari, maka tidak CloudTrail akan menyalin peristiwa jejak apa pun yang `eventTime` lebih lama dari 90 hari.

    - Jika Anda memilih Rentang relatif, Anda dapat memilih untuk menyalin peristiwa yang dicatat dalam 6 bulan terakhir, 1 tahun, 2 tahun, 7 tahun, atau rentang khusus. CloudTrail menyalin peristiwa yang dicatat dalam periode waktu yang dipilih.
    - Jika Anda memilih Rentang Absolute, Anda dapat memilih tanggal mulai dan akhir tertentu. CloudTrail menyalin peristiwa yang terjadi antara tanggal mulai dan akhir yang dipilih.

    c. Untuk Iz in, pilih dari opsi peran IAM berikut. Jika Anda memilih peran IAM yang ada, verifikasi bahwa kebijakan peran IAM menyediakan izin yang diperlukan. Untuk informasi

selengkapnya tentang memperbarui izin peran IAM, lihatIzin IAM untuk menyalin peristiwa jejak.

- Pilih Buat peran baru (disarankan) untuk membuat peran IAM baru. Untuk Masukkan nama peran IAM, masukkan nama untuk peran tersebut. CloudTrail secara otomatis membuat izin yang diperlukan untuk peran baru ini.
- Pilih Gunakan peran IAM khusus ARN untuk menggunakan peran IAM kustom yang tidak terdaftar. Untuk Masukkan peran IAM ARN, masukkan IAM ARN.
- Pilih peran IAM yang ada dari daftar drop-down.

21. Pilih Berikutnya untuk memperkaya acara Anda dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.
22. Di acara En rich, tambahkan hingga 50 kunci tag sumber daya dan 50 kunci kondisi global IAM untuk memberikan metadata tambahan tentang acara Anda. Ini membantu Anda mengkategorikan dan mengelompokkan acara terkait.

    Jika Anda menambahkan kunci tag resource, CloudTrail akan menyertakan kunci tag yang dipilih terkait dengan resource yang terlibat dalam panggilan API. Peristiwa API yang terkait dengan sumber daya yang dihapus tidak akan memiliki tag sumber daya.

    Jika Anda menambahkan kunci kondisi global IAM, CloudTrail akan menyertakan informasi tentang kunci kondisi yang dipilih yang dievaluasi selama proses otorisasi, termasuk detail tambahan tentang prinsip, sesi, jaringan, dan permintaan itu sendiri.

    Informasi tentang kunci tag sumber daya dan kunci kondisi global IAM ditampilkan di `eventContext` bidang acara. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.

    > **Note**
    >
    > Jika acara berisi sumber daya yang bukan milik Wilayah acara, tag tidak CloudTrail akan diisi untuk sumber daya ini karena pengambilan tag terbatas pada Region acara.

23. Pilih Perluas ukuran acara untuk memperluas payload acara hingga 1 MB dari 256 KB. Opsi ini secara otomatis diaktifkan saat Anda menambahkan kunci tag sumber daya atau kunci kondisi global IAM untuk memastikan semua kunci yang ditambahkan disertakan dalam acara.

Memperluas ukuran acara sangat membantu untuk menganalisis dan memecahkan masalah peristiwa karena memungkinkan Anda melihat konten lengkap bidang berikut selama payload peristiwa kurang dari 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Untuk informasi selengkapnya tentang bidang ini, lihat konten CloudTrail rekaman.

24. Pilih Berikutnya untuk meninjau pilihan Anda.
25. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
26. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.

    Dari titik ini ke depan, penyimpanan data peristiwa menangkap peristiwa yang cocok dengan pemilih acara lanjutannya (jika Anda tetap memilih opsi Ingest events). Peristiwa yang terjadi sebelum Anda membuat penyimpanan data peristiwa tidak ada di penyimpanan data peristiwa, kecuali Anda memilih untuk menyalin peristiwa jejak yang ada.

Anda sekarang dapat menjalankan kueri di penyimpanan data acara baru Anda. Tab Kueri Sampel menyediakan contoh kueri untuk membantu Anda memulai. Untuk informasi selengkapnya tentang membuat dan mengedit kueri, lihatMembuat atau mengedit kueri dengan CloudTrail konsol.

Anda juga dapat melihat dasbor ter kelola, atau membuat dasbor khusus untuk memvisualisasikan tren acara. Untuk informasi lebih lanjut tentang dasbor Danau, lihatCloudTrail Dasbor danau.

Membuat penyimpanan data acara untuk acara Insights dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan menanggapi aktivitas tidak biasa yang terkait dengan tingkat panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen. CloudTrail Wawasan menganalisis pola normal tingkat panggilan API dan tingkat kesalahan API, juga disebut baseline, dan menghasilkan peristiwa Wawasan ketika volume panggilan atau tingkat kesalahan berada di luar pola normal. Peristiwa wawasan tentang tingkat panggilan API dibuat untuk API `write` manajemen, dan peristiwa Wawasan tentang tingkat kesalahan API dibuat untuk kedua API `read` dan API `write` manajemen.

Untuk mencatat peristiwa Insights di CloudTrail Lake, Anda memerlukan penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights dan penyimpanan data peristiwa sumber yang memungkinkan Wawasan dan mencatat peristiwa manajemen.

> **Note**
>
> Untuk mencatat peristiwa Insights pada tingkat panggilan API, penyimpanan data peristiwa sumber harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, penyimpanan data peristiwa sumber harus mencatat `read` atau `write` mengelola peristiwa.

Jika Anda mengaktifkan CloudTrail Insights di penyimpanan data peristiwa sumber dan CloudTrail mendeteksi aktivitas yang tidak biasa, ki CloudTrail rimkan peristiwa Insights ke penyimpanan data acara tujuan Anda. Tidak seperti jenis peristiwa lain yang ditangkap di penyimpanan data CloudTrail peristiwa, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda yang berbeda secara signifikan dari pola penggunaan tipikal akun.

Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya di penyimpanan data peristiwa, CloudTrail mungkin diperlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

CloudTrail Wawasan menganalisis peristiwa manajemen yang terjadi di setiap Wilayah untuk penyimpanan data peristiwa dan menghasilkan peristiwa Wawasan ketika aktivitas tidak biasa terdeteksi yang menyimpang dari baseline. Peristiwa CloudTrail Wawasan dihasilkan di Wilayah yang sama dengan acara manajemen pendukungnya yang dihasilkan.

Untuk penyimpanan data acara organisasi, CloudTrail Insights menganalisis peristiwa manajemen dari setiap akun anggota di organisasi untuk setiap Wilayah dan menghasilkan peristiwa Wawasan ketika aktivitas tidak biasa terdeteksi yang menyimpang dari baseline untuk akun dan Wilayah.

Biaya tambahan berlaku untuk menelan acara Insights di CloudTrail Lake. Anda akan dikenakan biaya secara terpisah jika mengaktifkan Insights untuk jalur dan CloudTrail penyimpanan data acara Lake. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Topik

- Untuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights
- Untuk membuat penyimpanan data peristiwa sumber yang mengaktifkan peristiwa Insights

Untuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights

Saat membuat penyimpanan data peristiwa Insights, Anda memiliki opsi untuk memilih penyimpanan data peristiwa sumber yang ada yang mencatat peristiwa manajemen dan kemudian menentukan jenis Wawasan yang ingin Anda terima. Atau, Anda juga dapat mengaktifkan Wawasan pada penyimpanan data peristiwa baru atau yang sudah ada setelah Anda membuat penyimpanan data peristiwa Wawasan, lalu memilih penyimpanan data peristiwa ini sebagai penyimpanan data peristiwa tujuan.

Prosedur ini menunjukkan cara membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, buka submenu Lake, lalu pilih Event data storage.
3. Pilih Buat penyimpanan data acara.

4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, masukkan nama untuk penyimpanan data peristiwa. Sebuah nama diperlukan.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
     - Periode retensi default: 366 hari
     - Periode retensi maksimum: 3.653 hari
   - Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
     - Periode retensi default: 2.557 hari
     - Periode retensi maksimum: 2.557 hari
6. Tentukan periode retensi untuk penyimpanan data peristiwa dalam hari. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year Penyimpanan data peristiwa menyimpan data peristiwa untuk jumlah hari yang ditentukan.
7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/MyAliasName`. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar penyimpanan data acara dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

> **Note**
>
> Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

   Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

   a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

   b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

   c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

10. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag di AWS, lihat Men andai sumber AWS daya di Panduan Pengguna Menandai Sumber AWS Daya.
11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
12. Pada halaman Pilih acara, pilih AWS acara, lalu pilih peristiwa CloudTrail Wawasan.
13. Di acara CloudTrail Insights, lakukan hal berikut.

a. Pilih Izinkan akses administrator yang didelegasikan jika Anda ingin memberikan akses administrator yang didelegasikan organisasi Anda ke penyimpanan data peristiwa ini. Opsi ini hanya tersedia jika Anda masuk dengan akun manajemen untuk suatu AWS Organizations organisasi.

b. (Opsional) Pilih penyimpanan data peristiwa sumber yang ada yang mencatat peristiwa manajemen dan tentukan jenis Wawasan yang ingin Anda terima.

   Untuk menambahkan penyimpanan data peristiwa sumber, lakukan hal berikut.

   i. Pilih Tambahkan penyimpanan data peristiwa sumber.

   ii. Pilih penyimpanan data peristiwa sumber.

   iii. Pilih jenis Wawasan yang ingin Anda terima.

   - `ApiCallRateInsight`— Jenis In `ApiCallRateInsight` sights menganalisis panggilan API manajemen khusus tulis yang digabungkan per menit terhadap volume panggilan API dasar. Untuk menerima Wawasan`ApiCallRateInsight`, penyimpanan data peristiwa sumber harus mencatat peristiwa manajemen T ulis.
   - `ApiErrorRateInsight`— Jenis In `ApiErrorRateInsight` sights menganalisis panggilan API manajemen yang menghasilkan kode kesalahan. Kesalahan ditampilkan jika panggilan API tidak berhasil. Untuk menerima Wawasan`ApiErrorRateInsight`, penyimpanan data peristiwa sumber harus mencatat peristiwa manajemen T ulis atau Baca.

   iv. Ulangi dua langkah sebelumnya (ii dan iii) untuk menambahkan jenis Wawasan tambahan yang ingin Anda terima.

14. Pilih Berikutnya untuk meninjau pilihan Anda.
15. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
16. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.
17. Jika Anda tidak memilih penyimpanan data peristiwa sumber pada langkah 10, ikuti langkah-langkah Untuk membuat penyimpanan data peristiwa sumber yang mengaktifkan peristiwa Insights untuk membuat penyimpanan data peristiwa sumber.

Untuk membuat penyimpanan data peristiwa sumber yang mengaktifkan peristiwa Insights

Prosedur ini menunjukkan cara membuat penyimpanan data peristiwa sumber yang mengaktifkan peristiwa Insights dan mencatat peristiwa manajemen.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, buka submenu Lake, lalu pilih Event data storage.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, masukkan nama untuk penyimpanan data peristiwa. Sebuah nama diperlukan.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
     - Periode retensi default: 366 hari
     - Periode retensi maksimum: 3.653 hari
   - Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
     - Periode retensi default: 2.557 hari
     - Periode retensi maksimum: 2.557 hari
6. Tentukan periode retensi untuk penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

CloudTrail Lake menentukan apakah acara akan dipertahankan dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode penyimpanan 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/MyAliasName`. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar penyimpanan data acara dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

   Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

   > **Note**
   >
   > Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

   Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

   a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol,

CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

   Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

   Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara

otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

10. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag di AWS, lihat Men andai sumber AWS daya di Panduan Pengguna Menandai Sumber AWS Daya.
11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
12. Pada halaman Pilih acara, pilih AWS acara, lalu pilih CloudTrail acara.
13. Di CloudTrail acara, biarkan acara Manajemen dipilih.
14. Agar penyimpanan data acara Anda mengumpulkan peristiwa dari semua akun dalam AWS Organizations organisasi, pilih Aktifkan untuk semua akun di organisasi saya. Anda harus masuk ke akun manajemen agar organisasi dapat membuat penyimpanan data peristiwa yang mengaktifkan Wawasan.
15. Per luas Pengaturan tambahan untuk memilih apakah Anda ingin penyimpanan data acara mengumpulkan peristiwa untuk semua Wilayah AWS, atau hanya saat ini Wilayah AWS, dan pilih apakah penyimpanan data acara menyerap peristiwa. Secara default, penyimpanan data acara Anda mengumpulkan peristiwa dari semua Wilayah di akun Anda dan mulai mengambil peristiwa saat dibuat.

    a. Pilih Sertakan hanya wilayah saat ini di penyimpanan data acara saya jika Anda ingin menyertakan hanya peristiwa yang dicatat di Wilayah saat ini. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda menyertakan acara dari semua Wilayah.

    b. Biarkan acara Ingest dipilih.

16. Pilih antara koleksi acara sederhana atau koleksi acara lanjutan:

    - Pilih Koleksi acara sederhana jika Anda ingin mencatat semua peristiwa, mencatat hanya peristiwa yang dibaca, atau log hanya menulis peristiwa. Anda juga dapat memilih untuk mengecualikan AWS Key Management Service dan acara API Data Amazon RDS.
    - Pilih Koleksi acara lanj utan jika Anda ingin menyertakan atau mengecualikan peristiwa manajemen berdasarkan nilai bidang pemilih peristiwa lanjutan, termasuk bidang`eventName`,`eventType`,`eventSource`,`sessionCredentialFromConsole`, dan`userIdentity.arn`.

17. Jika Anda memilih Koleksi acara sederhana, pilih apakah Anda ingin mencatat semua peristiwa, mencatat hanya peristiwa yang dibaca, atau log hanya menulis peristiwa. Anda juga dapat memilih untuk mengecualikan AWS KMS dan acara API Data Amazon RDS.
18. Jika Anda memilih Koleksi acara lanj utan, buat pilihan berikut:

    a. Di Template pemilih log, pilih template yang telah ditentukan sebelumnya, atau pilih K ustom untuk menulis kondisi pengumpulan acara Anda sendiri berdasarkan nilai bidang pemilih acara lanjutan.

       Anda dapat memilih dari template yang telah ditentukan sebelumnya berikut:

       - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
       - Log hanya membaca acara - Pilih template ini untuk mencatat hanya peristiwa baca. Read-only peristiwa adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa.
       - Log hanya menulis peristiwa - Pilih template ini untuk mencatat hanya menulis peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa.
       - Log saja Konsol Manajemen AWS peristiwa - Pilih template ini untuk mencatat hanya peristiwa yang berasal dari Konsol Manajemen AWS.
       - Kecualikan peristiwa yang Layanan AWS dimulai — Pilih template ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` of`AwsServiceEvent`, dan peristiwa yang dimulai dengan peran Layanan AWS-link (SLR).

    b. (Opsional) Di Nama pemilih, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log manajemen peristiwa dari Konsol Manajemen AWS sesi”. Nama pemilih terdaftar seperti `Name` pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

    c. Jika Anda memilih K ustom, dalam pemilih acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

       > **Note**
       >
       > Selektor tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat

menggunakanStartsWith,EndsWith,NotStartsWith, atau NotEndsWith untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

i. Pilih dari bidang berikut.

- **readOnly**— readOnly dapat disetel menjadi sama dengan nilai true ataufalse. Ketika disetel kefalse, penyimpanan data peristiwa mencatat peristiwa Write-only manajemen. Read-only peristiwa manajemen adalah peristiwa yang tidak mengubah status sumber daya, seperti Get* atau Describe* peristiwa. Tulis acara menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau Write* peristiwa. Untuk mencatat peristiwa Baca dan Tulis, jangan tambahkan pem readOnly ilih.
- **eventName**— eventName dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara manajemen apa pun, seperti CreateAccessPoint atauGetAccessPoint.
- **userIdentity.arn**— Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail userIdentity.
- **sessionCredentialFromConsole**— Sertakan atau mengecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diset el menjadi sama atau tidak sama dengan nilaitrue.
- **eventSource**— Anda dapat menggunakannya untuk memasukkan atau mengecualikan sumber acara tertentu. Biasanya eventSource merupakan bentuk pendek dari nama layanan tanpa spasi plus.amazonaws.com. Misalnya, Anda dapat menyetel eventSource sama dengan ec2.amazonaws.com untuk mencatat hanya peristiwa manajemen Amazon EC2.
- **eventType**- EventType untuk disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini menjadi tidak sama untuk AwsServiceEvent mengecualikan Layanan AWS peristiwa.

ii. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat.

Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua pemilih pada penyimpanan data peristiwa. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi ditambahkan ke pemilih.

iii. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan menetapkan nilai yang bertentangan atau duplikat untuk bidang.

d. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

19. Pilih Aktifkan penangkapan peristiwa Wawasan.
20. Pilih toko acara tujuan yang akan mencatat peristiwa Insights. Penyimpanan data acara tujuan akan mengumpulkan peristiwa Wawasan berdasarkan aktivitas acara manajemen di penyimpanan data acara ini. Untuk informasi tentang cara membuat penyimpanan data acara tujuan, lihatUntuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.
21. Pilih jenis Wawasan. Anda dapat memilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Anda harus mencatat peristiwa manajemen T ulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau T ulis untuk mencatat peristiwa Insights untuk tingkat kesalahan API.
22. Pilih Berikutnya untuk memperkaya acara Anda dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.
23. Di acara En rich, tambahkan hingga 50 kunci tag sumber daya dan 50 kunci kondisi global IAM untuk memberikan metadata tambahan tentang acara Anda. Ini membantu Anda mengkategorikan dan mengelompokkan acara terkait.

    Jika Anda menambahkan kunci tag resource, CloudTrail akan menyertakan kunci tag yang dipilih terkait dengan resource yang terlibat dalam panggilan API. Peristiwa API yang terkait dengan sumber daya yang dihapus tidak akan memiliki tag sumber daya.

    Jika Anda menambahkan kunci kondisi global IAM, CloudTrail akan menyertakan informasi tentang kunci kondisi yang dipilih yang dievaluasi selama proses otorisasi, termasuk detail tambahan tentang prinsip, sesi, jaringan, dan permintaan itu sendiri.

Informasi tentang kunci tag sumber daya dan kunci kondisi global IAM ditampilkan di `eventContext` bidang acara. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.

> **Note**
>
> Jika acara berisi sumber daya yang bukan milik Wilayah acara, tag tidak CloudTrail akan diisi untuk sumber daya ini karena pengambilan tag terbatas pada Region acara.

24. Pilih Perluas ukuran acara untuk memperluas payload acara hingga 1 MB dari 256 KB. Opsi ini secara otomatis diaktifkan saat Anda menambahkan kunci tag sumber daya atau kunci kondisi global IAM untuk memastikan semua kunci yang ditambahkan disertakan dalam acara.

    Memperluas ukuran acara sangat membantu untuk menganalisis dan memecahkan masalah peristiwa karena memungkinkan Anda melihat konten lengkap bidang berikut selama payload peristiwa kurang dari 1 MB:

    - `annotation`
    - `requestID`
    - `additionalEventData`
    - `serviceEventDetails`
    - `userAgent`
    - `errorCode`
    - `responseElements`
    - `requestParameters`
    - `errorMessage`

    Untuk informasi selengkapnya tentang bidang ini, lihat konten CloudTrail rekaman.

25. Pilih Berikutnya untuk meninjau pilihan Anda.
26. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
27. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.

Dari titik ini ke depan, penyimpanan data peristiwa menangkap peristiwa yang cocok dengan pemilih acara lanjutnya. Setelah Anda mengaktifkan CloudTrail Wawasan untuk pertama kalinya di penyimpanan data peristiwa sumber, CloudTrail mungkin diperlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Wawasan, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

Anda dapat melihat dasbor CloudTrail Lake untuk memvisualisasikan peristiwa Wawasan di penyimpanan data acara tujuan Anda. Untuk informasi lebih lanjut tentang dasbor Danau, lihatCloudTrail Dasbor danau.

Biaya tambahan berlaku untuk menelan acara Insights di CloudTrail Lake. Anda akan dikenakan biaya terpisah jika mengaktifkan Insights untuk trek dan penyimpanan data acara. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Buat penyimpanan data acara untuk item konfigurasi dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat membuat penyimpanan data peristiwa untuk menyertakan item AWS Config konfigurasi, dan menggunakan penyimpanan data peristiwa untuk menyelidiki perubahan yang tidak sesuai pada lingkungan produksi Anda. Dengan penyimpanan data peristiwa, Anda dapat menghubungkan aturan yang tidak sesuai dengan pengguna dan sumber daya yang terkait dengan perubahan. Item konfigurasi mewakili tampilan point-in-time dari atribut AWS sumber daya yang didukung yang ada di akun Anda. AWS Config membuat item konfigurasi setiap kali mendeteksi perubahan pada jenis sumber daya yang direkam. AWS Config juga membuat item konfigurasi saat snapshot konfigurasi diambil.

Anda dapat menggunakan keduanya AWS Config dan CloudTrail Lake untuk menjalankan kueri terhadap item konfigurasi Anda. Anda dapat menggunakan AWS Config untuk menanyakan status konfigurasi sumber AWS daya saat ini berdasarkan properti konfigurasi untuk satu Akun AWS dan Wilayah AWS, atau di beberapa akun dan Wilayah. Sebaliknya, Anda dapat menggunakan CloudTrail

Lake untuk menanyakan berbagai sumber data seperti CloudTrail peristiwa, item konfigurasi, dan evaluasi aturan. CloudTrail Kueri Lake mencakup semua item AWS Config konfigurasi termasuk konfigurasi sumber daya dan riwayat kepatuhan.

Membuat penyimpanan data peristiwa untuk item konfigurasi tidak memengaruhi kueri lanjutan yang ada AWS Config , atau AWS Config agregator yang dikonfigurasi. Anda dapat terus menjalankan kueri lanjutan menggunakan AWS Config, dan AWS Config terus mengirimkan file riwayat ke bucket S3 Anda.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat membuat penyimpanan data peristiwa, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data peristiwa. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data peristiwa. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

Batasan

Batasan berikut berlaku untuk penyimpanan data peristiwa untuk item konfigurasi.

- Tidak ada dukungan untuk item konfigurasi khusus
- Tidak ada dukungan untuk pemfilteran acara menggunakan pemilih acara lanjutan

Prasyarat

Sebelum Anda membuat penyimpanan data acara, siapkan AWS Config perekaman untuk semua akun dan Wilayah Anda. Anda dapat menggunakan Pengaturan C epat, kemampuan AWS Systems Manager, untuk dengan cepat membuat perekam konfigurasi yang didukung oleh AWS Config.

> **Note**
>
> Anda akan dikenakan biaya penggunaan layanan saat AWS Config mulai merekam konfigurasi. Untuk informasi selengkapnya tentang harga, lihat AWS Config Harga. Untuk informasi tentang mengelola perekam konfigurasi, lihat M engelola Perekam Konfigurasi di Panduan AWS Config Pengembang.

Selain itu, tindakan berikut direkomendasikan, tetapi tidak diperlukan untuk membuat penyimpanan data peristiwa.

- Siapkan bucket Amazon S3 untuk menerima snapshot konfigurasi berdasarkan permintaan dan riwayat konfigurasi. Untuk informasi selengkapnya tentang snapshot, lihat M engelola Saluran Pengiriman dan Men girimkan Snapshot Konfigurasi ke Bucket Amazon S3 di Panduan Peng AWS Config embang.
- Tentukan aturan yang ingin Anda gunakan AWS Config untuk mengevaluasi informasi kepatuhan untuk jenis sumber daya yang direkam. Beberapa kueri sampel CloudTrail Lake diperlukan Aturan AWS Config untuk AWS Config mengevaluasi status kepatuhan AWS sumber daya Anda. Untuk informasi selengkapnya Aturan AWS Config, lihat Mengevaluasi Sumber Daya dengan Aturan AWS Config di Panduan AWS Config Pengembang.

Untuk membuat penyimpanan data acara untuk item konfigurasi

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, masukkan nama untuk penyimpanan data peristiwa. Sebuah nama diperlukan.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
     - Periode retensi default: 366 hari
     - Periode retensi maksimum: 3.653 hari
   - Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.

- Periode retensi default: 2.557 hari
- Periode retensi maksimum: 2.557 hari

6. Tentukan periode retensi untuk penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

   CloudTrail Lake menentukan apakah acara akan dipertahankan dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode penyimpanan 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/`*`MyAliasName`*. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar penyimpanan data acara dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

   Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

   > **Note**
   >
   > Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

   Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

   Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

10. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag di AWS, lihat Men andai sumber AWS daya di Panduan Pengguna Menandai Sumber AWS Daya.
11. Pilih Berikutnya.
12. Pada halaman Pilih acara, pilih AWS acara, lalu pilih I tem konfigurasi.
13. CloudTrail menyimpan sumber daya penyimpanan data peristiwa di Wilayah tempat Anda membuatnya, tetapi secara default, item konfigurasi yang dikumpulkan di penyimpanan data berasal dari semua Wilayah di akun Anda yang telah mengaktifkan perekaman. Secara opsional, Anda dapat memilih Ser takan hanya wilayah saat ini di penyimpanan data acara saya untuk menyertakan hanya item konfigurasi yang diambil di Wilayah saat ini. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda menyertakan item konfigurasi dari semua Wilayah yang mengaktifkan perekaman.
14. Agar penyimpanan data acara Anda mengumpulkan item konfigurasi dari semua akun dalam AWS Organizations organisasi, pilih Aktifkan untuk semua akun di organisasi saya. Anda harus masuk ke akun manajemen atau akun administrator yang didelegasikan agar organisasi dapat membuat penyimpanan data peristiwa yang mengumpulkan item konfigurasi untuk organisasi.
15. Pilih Berikutnya untuk meninjau pilihan Anda.
16. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
17. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.

Dari titik ini ke depan, penyimpanan data peristiwa menangkap item konfigurasi. Item konfigurasi yang terjadi sebelum Anda membuat penyimpanan data peristiwa tidak ada di penyimpanan data peristiwa.

Skema item konfigurasi

Tabel berikut menjelaskan elemen skema yang diperlukan dan opsional yang cocok dengan yang ada di catatan item konfigurasi. Isi `eventData` disediakan oleh item konfigurasi Anda; bidang lain disediakan oleh CloudTrail setelah konsumsi.

CloudTrail konten catatan peristiwa dijelaskan secara lebih rinci diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

- Bidang yang disediakan CloudTrail setelah konsumsi
- Bidang yang disediakan oleh acara Anda

Bidang yang disediakan CloudTrail setelah konsumsi

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
Versi acara	string	Diperlukan	Versi format AWS acara.
Kategori acara	string	Diperlukan	Kategori acara. Untuk item konfigurasi, nilai yang valid adalah`ConfigurationItem` .
eventType	string	Diperlukan	Jenis peristiwa. Untuk item konfigurasi, nilai yang valid adalah`AwsConfigurationItem` .
EvenID	string	Diperlukan	ID unik untuk acara.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
eventTime	string	Diperlukan	Stempel waktu acara, dalam `yyyy-MM-DDTHH:mm:ss` format, dalam Waktu Terkoordinasi Universal (UTC).
awsRegion	string	Diperlukan	Wilayah AWS Tempat untuk menetapkan acara.
penerima AccountId	string	Diperlukan	Merupakan Akun AWS ID yang menerima acara ini.
Tambahan	Tambahan	Opsional	Menampilkan informasi tentang mengapa suatu acara ditunda. Jika informasi hilang dari peristiwa yang ada, blok addendum menyertakan informasi yang hilang dan alasan mengapa itu hilang.

Bidang di **`EventData`** disediakan oleh item konfigurasi Anda

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
Data peristiwa	-	Diperlukan	Bidang di EventData disediakan oleh item konfigurasi Anda.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• konfigurasi ItemVersion	string	Opsional	Versi item konfigurasi dari sumbernya.
• konfigurasi ItemCaptureTime	string	Opsional	Waktu ketika perekaman konfigurasi dimulai.
• konfigurasi ItemStatus	string	Opsional	Status item konfigurasi. Nilai yang valid adalah `OK`, `ResourceDiscovered`, `ResourceNotRecorded`, `ResourceDeleted`, dan `ResourceDeletedNotRecorded`.
• accountId	string	Opsional	Akun AWS ID 12 digit yang terkait dengan sumber daya.
• resourceType	string	Opsional	Jenis sumber AWS daya. Untuk informasi selengkapnya tentang jenis sumber daya yang valid, lihat ConfigurationItem di Refer AWS Configensi API.
• ID sumber daya	string	Opsional	ID sumber daya (misalnya., sg-*xxxxxx*).

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• Nama Sumber Daya	string	Opsional	Nama kustom sumber daya, jika tersedia.
• arn	string	Opsional	Nama Sumber Daya Amazon (ARN) yang terkait dengan sumber daya.
• awsRegion	string	Opsional	Di Wilayah AWS mana sumber daya berada.
• availabilityZone	string	Opsional	Zona Ketersediaan yang terkait dengan sumber daya.
• sumber daya CreationTime	string	Opsional	Cap waktu saat sumber daya dibuat.
• konfigurasi	JSON	Opsional	Deskripsi konfigurasi sumber daya.
• Konfigurasi Tambahan	JSON	Opsional	Atribut konfigurasi yang AWS Config mengembalikan untuk jenis sumber daya tertentu untuk melengkapi informasi yang dikembalikan untuk parameter konfigurasi.
• RelateDevents	string	Opsional	Daftar ID CloudTrail peristiwa.
• hubungan	-	Opsional	Daftar sumber AWS daya terkait.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• • name	string	Opsional	Jenis hubungan dengan sumber daya terkait.
• • resourceType	string	Opsional	Jenis sumber daya dari sumber daya terkait.
• • ID sumber daya	string	Opsional	ID sumber daya terkait (misalnya, sg-*xxxxxx*).
• • Nama Sumber Daya	string	Opsional	Nama kustom sumber daya terkait, jika tersedia.
• tag	JSON	Opsional	Pemetaan tag nilai kunci yang terkait dengan sumber daya.

Contoh berikut menunjukkan hierarki elemen skema yang cocok dengan yang ada dalam catatan item konfigurasi.

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
```

```
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

Membuat penyimpanan data acara untuk acara di luar AWS dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat membuat penyimpanan data peristiwa untuk menyertakan peristiwa di luar AWS, lalu menggunakan CloudTrail Lake untuk mencari, menanyakan, dan menganalisis data yang dicatat dari aplikasi Anda.

Anda dapat menggunakan integrasi CloudTrail Lake untuk mencatat dan menyimpan data aktivitas pengguna dari luar AWS; dari sumber apa pun di lingkungan hibrida Anda, seperti aplikasi in-house atau SaaS yang dihosting di lokasi atau di cloud, mesin virtual, atau wadah.

Saat membuat penyimpanan data peristiwa untuk integrasi, Anda juga membuat saluran, dan melampirkan kebijakan sumber daya ke saluran.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat membuat penyimpanan data peristiwa, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data peristiwa. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, serta periode retensi default dan maksimum untuk penyimpanan data peristiwa. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

Untuk membuat penyimpanan data acara untuk acara di luar AWS

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Konfigurasi penyimpanan data peristiwa, di Detail umum, masukkan nama untuk penyimpanan data peristiwa. Sebuah nama diperlukan.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

   - One-year harga retensi yang dapat diperpanjang - Umumnya disarankan jika Anda mengharapkan untuk mengkonsumsi kurang dari 25 TB data acara per bulan dan menginginkan periode retensi fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.

- Periode retensi default: 366 hari
- Periode retensi maksimum: 3.653 hari

- Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk mengkonsumsi lebih dari 25 TB data acara per bulan dan membutuhkan periode penyimpanan hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
  - Periode retensi default: 2.557 hari
  - Periode retensi maksimum: 2.557 hari

6. Tentukan periode retensi untuk penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

   CloudTrail Lake menentukan apakah acara akan dipertahankan dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode penyimpanan 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat kunci untuk Anda, atau pilih Sudah ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format `alias/`*`MyAliasName`*. Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS agar penyimpanan data acara dapat dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-wilayah, lihat Menggunakan kunci Multi-wilayah di Panduan Peng AWS Key Management Service embang.

   Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

   > **Note**
   >
   > Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data peristiwa organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin menanyakan data acara menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Lake. Federasi memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

   Untuk mengaktifkan federasi kueri Lake, pilih Akti fkan dan kemudian lakukan hal berikut:

   a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih peran yang sudah ada, pastikan kebijakan untuk peran tersebut menyediakan izin minimum yang diperlukan.

   b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

   c. Jika Anda menggunakan peran yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

   Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

   Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`

- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

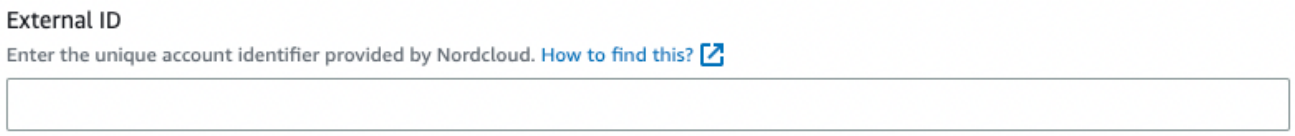
10. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag di AWS, lihat Men andai sumber AWS daya di Panduan Pengguna Menandai Sumber AWS Daya.
11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
12. Pada halaman Pilih acara, pilih A cara dari integrasi.
13. Dari Acara dari integrasi, pilih sumber untuk mengirimkan acara ke penyimpanan data acara.
14. Berikan nama untuk mengidentifikasi saluran integrasi. Namanya bisa 3-128 karakter. Hanya huruf, angka, titik, garis bawah, dan tanda hubung yang diperbolehkan.
15. Di Kebijakan sumber daya, konfigurasikan kebijakan sumber daya untuk saluran integrasi. Kebijakan sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya dan dalam kondisi tertentu. Akun yang didefinisikan sebagai prinsipal dalam kebijakan sumber daya dapat memanggil `PutAuditEvents` API untuk mengirimkan acara ke saluran Anda. Pemilik sumber daya memiliki akses implisit ke sumber daya jika kebijakan IAM miliknya mengizinkan tindakan `cloudtrail-data:PutAuditEvents` tersebut.

Informasi yang diperlukan untuk kebijakan ditentukan oleh jenis integrasi. Untuk integrasi arah, CloudTrail secara otomatis menambahkan ID AWS akun mitra, dan mengharuskan Anda memasukkan ID eksternal unik yang disediakan oleh mitra. Untuk integrasi solusi, Anda harus menentukan setidaknya satu ID AWS akun sebagai prinsipal, dan dapat secara opsional memasukkan ID eksternal untuk mencegah wakil yang bingung.

> **Note**
>
> Jika Anda tidak membuat kebijakan sumber daya untuk saluran, hanya pemilik saluran yang dapat memanggil `PutAuditEvents` API di saluran.

a. Untuk integrasi langsung, masukkan ID eksternal yang disediakan oleh mitra Anda. Partner integrasi menyediakan ID eksternal yang unik, seperti ID akun atau string yang dibuat secara acak, untuk digunakan dalam integrasi guna mencegah masalah keamanan. Partner bertanggung jawab untuk membuat dan memberikan ID eksternal yang unik.

   Anda dapat memilih Bagaimana menemukan ini? untuk melihat dokumentasi mitra yang menjelaskan cara menemukan ID eksternal.



> **Note**
>
> Jika kebijakan sumber daya menyertakan ID eksternal, semua panggilan ke `PutAuditEvents` API harus menyertakan ID eksternal. Namun, jika kebijakan tidak menentukan ID eksternal, mitra masih dapat memanggil `PutAuditEvents` API dan menentukan `externalId` parameter.

b. Untuk integrasi solusi, pilih Tam bah AWS akun untuk menentukan setiap ID AWS akun yang akan ditambahkan sebagai prinsipal dalam kebijakan.

16. Pilih Berikutnya untuk meninjau pilihan Anda.
17. Pada halaman T injau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.

18. Penyimpanan data peristiwa baru terlihat di tabel penyimpanan data peristiwa di halaman penyimpanan data acara.
19. Berikan saluran Nama Sumber Daya Amazon (ARN) ke aplikasi mitra. Petunjuk untuk menyediakan saluran ARN ke aplikasi mitra ditemukan di situs web dokumentasi mitra. Untuk informasi selengkapnya, pilih tautan Pel ajari lebih lanjut untuk mitra di tab Sumber yang tersedia di halaman Integrasi untuk membuka halaman mitra di AWS Marketplace.

Penyimpanan data acara mulai menyerap peristiwa mitra CloudTrail melalui saluran integrasi saat Anda, mitra, atau aplikasi mitra memanggil `PutAuditEvents` API di saluran.

Memperbarui penyimpanan data acara dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Bagian ini menjelaskan cara memperbarui pengaturan penyimpanan data peristiwa menggunakan Konsol Manajemen AWS. Untuk informasi tentang cara memperbarui penyimpanan data peristiwa menggunakan AWS CLI, lihatPerbarui penyimpanan data acara dengan AWS CLI.

Untuk memperbarui penyimpanan data peristiwa

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara yang ingin Anda perbarui. Tindakan ini membuka halaman detail penyimpanan data acara.
4. Di Detail Umum, pilih Edit untuk mengubah pengaturan berikut:

   - Nama penyimpanan data acara - Ubah nama yang mengidentifikasi penyimpanan data acara Anda.
   - Opsi harga - Untuk penyimpanan data acara yang menggunakan opsi harga Seven-year retensi, Anda dapat memilih untuk menggunakan harga retensi yang dapat One-

year diperpanjang sebagai gantinya. Kami merekomendasikan harga retensi yang dapat diperpanjang satu tahun untuk penyimpanan data acara yang menyerap kurang dari 25 TB data peristiwa setiap bulan. Kami juga merekomendasikan harga retensi yang dapat diperpanjang satu tahun jika Anda mencari periode retensi fleksibel hingga 10 tahun. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga dan Mengelola biaya CloudTrail Danau.

> **Note**
>
> Anda tidak dapat mengubah opsi harga untuk penyimpanan data acara yang menggunakan harga retensi One-year yang dapat diperpanjang. Jika Anda ingin menggunakan harga Seven-year retensi, h entikan penyerapan di penyimpanan data peristiwa Anda saat ini. Kemudian buat penyimpanan data peristiwa baru dengan opsi harga Seven-year retensi.

- Periode retensi - Mengubah periode retensi untuk penyimpanan data peristiwa. Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data peristiwa. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi One-year yang dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

> **Note**
>
> Jika Anda mengurangi periode retensi penyimpanan data peristiwa, CloudTrail akan menghapus setiap peristiwa dengan periode retensi yang `eventTime` lebih lama dari periode retensi baru. Misalnya, jika periode penyimpanan sebelumnya adalah 365 hari dan Anda menguranginya menjadi 100 hari, CloudTrail akan menghapus peristiwa yang `eventTime` lebih lama dari 100 hari.

- Enkripsi - Untuk mengenkripsi penyimpanan data acara Anda menggunakan kunci KMS Anda sendiri, pilih Gunakan milik saya sendiri AWS KMS key. Secara default, semua peristiwa di penyimpanan data peristiwa dienkripsi oleh CloudTrail. Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi.

> **Note**
>
> Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

- Untuk menyertakan hanya peristiwa yang dicatat saat ini Wilayah AWS, pilih Ser takan pada wilayah saat ini di penyimpanan data acara saya. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda menyertakan acara dari semua Wilayah.
- Agar penyimpanan data acara Anda mengumpulkan peristiwa dari semua akun dalam AWS Organizations organisasi, pilih Aktifkan untuk semua akun di organisasi saya. Opsi ini hanya tersedia jika Anda masuk dengan akun manajemen untuk organisasi Anda, dan jenis Peristiwa untuk penyimpanan data peristiwa adalah CloudTrail peristiwa atau item Konfigurasi.

Pilih Simpan perubahan setelah selesai.

5. Di federasi kueri Lake, pilih Edit untuk mengaktifkan atau menonaktifkan federasi kueri Lake. Mengaktifkan federasi kueri Lake memungkinkan Anda melihat metadata untuk penyimpanan data acara Anda di Katalog AWS Glue Data dan menjalankan kueri SQL pada data acara menggunakan Amazon Athena. Menonaktifkan federasi kueri Lake menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Lake, Anda tidak dapat lagi menanyakan data Anda di Athena. Tidak ada data CloudTrail Lake yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Lake.

   Untuk mengaktifkan federasi, lakukan hal berikut:

   a. Pilih Aktifkan.
   b. Pilih apakah akan membuat peran IAM baru, atau menggunakan peran yang sudah ada. Saat Anda membuat peran baru, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda menggunakan peran yang sudah ada, pastikan kebijakan peran tersebut memberikan izin minimum yang diperlukan.
   c. Jika Anda membuat peran IAM baru, masukkan nama untuk peran tersebut.
   d. Jika Anda memilih peran IAM yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

   Pilih Simpan perubahan saat Anda selesai.

6. Di Kebijakan sumber daya, pilih Edit untuk menambahkan atau merevisi kebijakan berbasis sumber daya untuk penyimpanan data peristiwa.

   Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan

kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsi pal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan kepala sekolah pada sumber daya penyimpanan data peristiwa.

Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

7. Edit setelan tambahan yang spesifik untuk jenis Event penyimpanan data acara Anda.

   Pengaturan untuk CloudTrail acara

   - Untuk mengubah peristiwa yang menyimpan log data peristiwa Anda, pilih Edit di CloudTrail acara.
   - Di Acara manajemen, pilih Edit untuk mengubah pengaturan untuk acara manajemen. Untuk informasi selengkapnya, lihat Memperbarui pengaturan acara manajemen untuk penyimpanan data acara yang ada.

- Di acara data, pilih Edit untuk mengubah pengaturan peristiwa data. Anda dapat memilih jenis sumber daya yang ingin Anda log dan memilih template pemilih log yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa data menggunakan konsol.
- Di Acara aktivitas jaringan, pilih Edit untuk mengubah pengaturan untuk peristiwa aktivitas jaringan. Anda dapat memilih jenis peristiwa aktivitas jaringan yang ingin Anda log dan memilih template pemilih log yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan.
- Di Enrich events, perluas ukuran acara, pilih Edit untuk menambah atau menghapus tag sumber daya dan kunci kondisi global IAM, dan perluas ukuran acara.

  Di acara En rich, tambahkan hingga 50 kunci tag sumber daya dan 50 kunci kondisi global IAM untuk memberikan metadata tambahan tentang acara Anda. Ini membantu Anda mengkategorikan dan mengelompokkan acara terkait.

  Jika Anda menambahkan kunci tag resource, CloudTrail akan menyertakan kunci tag yang dipilih terkait dengan resource yang terlibat dalam panggilan API. Peristiwa API yang terkait dengan sumber daya yang dihapus tidak akan memiliki tag sumber daya.

  Jika Anda menambahkan kunci kondisi global IAM, CloudTrail akan menyertakan informasi tentang kunci kondisi yang dipilih yang dievaluasi selama proses otorisasi, termasuk detail tambahan tentang prinsip, sesi, jaringan, dan permintaan itu sendiri.

  Informasi tentang kunci tag sumber daya dan kunci kondisi global IAM ditampilkan di `eventContext` bidang acara. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.

  > **Note**
  >
  > Jika acara berisi sumber daya yang bukan milik Wilayah acara, tag tidak CloudTrail akan diisi untuk sumber daya ini karena pengambilan tag terbatas pada Region acara.

  Pilih Perluas ukuran acara untuk memperluas payload acara hingga 1 MB dari 256 KB. Opsi ini secara otomatis diaktifkan saat Anda menambahkan kunci tag sumber daya atau kunci kondisi global IAM untuk memastikan semua kunci yang ditambahkan disertakan dalam acara.

Memperluas ukuran acara sangat membantu untuk menganalisis dan memecahkan masalah peristiwa karena memungkinkan Anda melihat konten lengkap bidang berikut selama payload peristiwa kurang dari 1 MB:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

Untuk informasi selengkapnya tentang bidang ini, lihat konten CloudTrail rekaman.

Pilih Simpan perubahan setelah selesai.

Pengaturan untuk Acara dari integrasi

Di Integrasi, pilih integrasi Anda. Kemudian pilih Edit untuk mengubah pengaturan berikut:

- Di Detail Integrasi, ubah nama yang mengidentifikasi saluran integrasi Anda.
- Di Lokasi pengiriman acara, pilih tujuan acara Anda.
- Di Kebijakan sumber daya, konfigurasikan kebijakan sumber daya untuk saluran integrasi.

Pilih Simpan perubahan setelah selesai.

Untuk informasi selengkapnya tentang pengaturan ini, lihat Buat integrasi dengan CloudTrail mitra dengan konsol.

8. Untuk menambah, mengubah, atau menghapus tag, pilih Edit di Tag. Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Pilih Simpan perubahan setelah selesai.

Hentikan dan mulai penyerapan acara dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Secara default, penyimpanan data acara dikonfigurasi untuk menyerap peristiwa. Anda dapat menghentikan penyimpanan data peristiwa agar tidak menyerap peristiwa dengan menggunakan konsol, AWS CLI, atau API.

Opsi untuk Mulai penyerapan dan Hentikan penyerapan hanya tersedia di penyimpanan data peristiwa yang berisi CloudTrail peristiwa (peristiwa manajemen, peristiwa data, dan peristiwa aktivitas jaringan), atau item AWS Config konfigurasi.

Saat Anda menghentikan penyerapan pada penyimpanan data peristiwa, status penyimpanan data peristiwa berubah menjadi`STOPPED_INGESTION`. Anda masih dapat menjalankan kueri pada acara apa pun yang sudah ada di penyimpanan data acara. Anda juga dapat menyalin peristiwa jejak ke penyimpanan data peristiwa (jika hanya berisi CloudTrail peristiwa).

Untuk menghentikan penyimpanan data peristiwa agar tidak menelan peristiwa

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari T ind akan, pilih Hentikan konsumsi.
5. Ketika Anda diminta untuk mengonfirmasi, pilih H entikan konsumsi. Penyimpanan data acara akan berhenti menelan acara langsung.
6. Untuk melanjutkan konsumsi, pilih Mulai konsumsi.

Untuk memulai ulang penyerapan acara

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari Tind akan, pilih Mulai konsumsi.

Ubah perlindungan penghentian dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Secara default, penyimpanan data peristiwa di AWS CloudTrail Lake dikonfigurasi dengan perlindungan penghentian diaktifkan. Perlindungan penghentian mencegah penyimpanan data peristiwa dari penghapusan yang tidak disengaja. Jika Anda ingin menghapus penyimpanan data peristiwa, Anda harus menonaktifkan perlindungan penghentian. Anda dapat menonaktifkan perlindungan penghentian dengan menggunakan operasi Konsol Manajemen AWS AWS CLI,, atau API.

Untuk mematikan perlindungan penghentian

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari T indakan, pilih U bah perlindungan penghentian.
5. Pilih Din onaktifkan.
6. Pilih Simpan. Anda sekarang dapat menghapus penyimpanan data acara.

Untuk mengaktifkan perlindungan penghentian

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari T indakan, pilih U bah perlindungan penghentian.
5. Untuk mengaktifkan perlindungan penghentian, pilih Di aktifkan.
6. Pilih Simpan.

Menghapus penyimpanan data acara dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Bagian ini menjelaskan cara menghapus penyimpanan data peristiwa menggunakan CloudTrail konsol. Untuk informasi tentang cara menghapus penyimpanan data peristiwa menggunakan AWS CLI, lihatHapus penyimpanan data acara dengan AWS CLI.

> **Note**
>
> Anda tidak dapat menghapus penyimpanan data peristiwa jika perlindungan penghentian atau federasi kueri Lake diaktifkan. Secara default, mengaktifkan CloudTrail perlindungan penghentian untuk melindungi penyimpanan data peristiwa agar tidak dihapus secara tidak sengaja.
>
> Untuk menghapus penyimpanan data peristiwa dengan jenis peristiwa Acara dari integrasi, Anda harus terlebih dahulu menghapus saluran integrasi. Anda dapat menghapus saluran dari halaman detail integrasi atau dengan menggunakan aws cloudtrail delete-channel perintah. Untuk informasi selengkapnya, lihat Hapus saluran untuk menghapus integrasi dengan AWS CLI

Untuk menghapus penyimpanan data peristiwa

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari Tindakan, pilih Hapus.
5. Ketik nama penyimpanan data acara untuk mengonfirmasi bahwa Anda ingin menghapusnya.
6. Pilih Hapus.

Setelah Anda menghapus penyimpanan data peristiwa, status penyimpanan data peristiwa berubah menjadi `PENDING_DELETION` dan tetap dalam status tersebut selama 7 hari. Anda dapat memulihkan penyimpanan data peristiwa selama periode tunggu 7 hari. Saat berada di `PENDING_DELETION` status, penyimpanan data peristiwa tidak tersedia untuk kueri, dan tidak ada operasi lain yang dapat dilakukan pada penyimpanan data peristiwa kecuali operasi pemulihan. Penyimpanan data peristiwa yang tertunda penghapusan tidak menyerap peristiwa dan tidak menimbulkan biaya. Penyimpanan data peristiwa yang tertunda penghapusan dihitung terhadap kuota penyimpanan data peristiwa yang dapat ada dalam satu Wilayah AWS.

Memulihkan penyimpanan data acara dengan konsol

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Setelah Anda menghapus penyimpanan data peristiwa di AWS CloudTrail Lake, statusnya berubah menjadi `PENDING_DELETION` dan tetap dalam status tersebut selama 7 hari. Selama waktu ini, Anda dapat memulihkan penyimpanan data peristiwa dengan menggunakan Konsol Manajemen AWS, AWS CLI, atau operasi RestoreEventDataStore API.

Bagian ini menjelaskan cara memulihkan penyimpanan data peristiwa menggunakan konsol. Untuk informasi tentang cara memulihkan penyimpanan data peristiwa menggunakan AWS CLI, lihatKembalikan penyimpanan data acara dengan AWS CLI.

Untuk memulihkan penyimpanan data peristiwa

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari T indakan, pilih Pu lihkan.

Mengekspor data dari CloudTrail Lake Event Data Store ke CloudWatch

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Membuat data CloudTrail Danau tersedia CloudWatch memberikan beberapa keuntungan:

- Manajemen log terpusat - Gabungkan CloudTrail peristiwa dengan log aplikasi, log infrastruktur, dan sumber data lainnya di CloudWatch.
- Integrasi yang disederhanakan - CloudWatch menangani proses impor hanya dengan beberapa langkah - tentukan penyimpanan data acara dan rentang data.
- Akses data historis - Impor data CloudTrail Danau historis untuk menganalisis peristiwa masa lalu bersama data operasional saat ini.
- Tidak ada CloudTrail biaya tambahan - Impor data CloudTrail Danau yang disederhanakan tersedia tanpa CloudTrail biaya tambahan. Namun, Anda akan dikenakan CloudWatch biaya dengan penetapan harga log khusus Akses Langsung yang diterapkan.

Bagian ini menjelaskan cara mengekspor data dari penyimpanan data peristiwa menggunakan CloudTrail konsol. Untuk informasi tentang cara melakukan ini melalui SDK atau AWS CLI, lihat CloudWatch Dokumentasi

Untuk mengekspor data dari penyimpanan data peristiwa

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Dari T ind akan, pilih Ekspor ke CloudWatch.
5. Pilih rentang waktu untuk mengekspor data untuk EDS.
6. Gunakan petunjuk untuk membuat atau menyediakan peran IAM yang CloudTrail akan digunakan untuk mengakses data Anda untuk ekspor.
7. Pilih Ekspor.

Saat membuat data CloudTrail Lake tersedia untuk diekspor CloudWatch, pertimbangkan hal berikut:

- Harga - Meskipun ekspor data CloudTrail Lake yang disederhanakan tersedia tanpa CloudTrail biaya tambahan, Anda dikenakan CloudWatch biaya berdasarkan harga log khusus
- Retensi data - Pastikan periode penyimpanan data acara CloudTrail Lake Anda mencakup data historis yang ingin Anda ekspor
- Ketersediaan regional - Periksa CloudWatch dokumentasi untuk AWS wilayah yang didukung untuk fitur ini
- Akses penyimpanan data acara - Anda harus memiliki akses ke Event Data Store tempat data akan diekspor.

Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Bagian ini menjelaskan AWS CLI perintah yang dapat Anda gunakan untuk membuat, memperbarui, dan mengelola penyimpanan data acara CloudTrail Lake Anda.

Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Perintah yang tersedia untuk penyimpanan data acara

Perintah untuk membuat dan memperbarui penyimpanan data acara di CloudTrail Lake meliputi:

- `create-event-data-store`untuk membuat penyimpanan data acara.
- `get-event-data-store`untuk mengembalikan informasi tentang penyimpanan data acara termasuk pemilih acara lanjutan yang dikonfigurasi untuk penyimpanan data acara.
- `update-event-data-store`untuk mengubah konfigurasi penyimpanan data peristiwa yang ada.
- `list-event-data-stores`untuk daftar penyimpanan data acara.
- `delete-event-data-store`untuk menghapus penyimpanan data acara.
- `restore-event-data-store`untuk memulihkan penyimpanan data acara yang tertunda penghapusan.
- `start-import`untuk memulai impor peristiwa jejak ke penyimpanan data peristiwa, atau mencoba lagi impor yang gagal.
- `get-import`untuk mengembalikan informasi tentang impor tertentu.
- `stop-import`untuk menghentikan impor peristiwa jejak ke penyimpanan data acara.
- `list-imports`untuk mengembalikan informasi tentang semua impor, atau satu set impor tertentu oleh `ImportStatus` atau. `Destination`
- `list-import-failures`untuk mencantumkan kegagalan impor untuk impor yang ditentukan.
- `stop-event-data-store-ingestion`untuk menghentikan konsumsi acara pada penyimpanan data acara.
- `start-event-data-store-ingestion`untuk memulai ulang konsumsi acara pada penyimpanan data acara.
- `enable-federation`untuk mengaktifkan federasi pada penyimpanan data acara untuk menanyakan penyimpanan data acara di Amazon Athena.
- `disable-federation`untuk menonaktifkan federasi pada penyimpanan data acara. Setelah menonaktifkan federasi, Anda tidak dapat lagi melakukan kueri terhadap data penyimpanan data acara di Amazon Athena. Anda dapat melanjutkan pertanyaan di CloudTrail Danau.

- `put-insight-selectors` untuk menambahkan atau memodifikasi pemilih acara Insights untuk penyimpanan data peristiwa yang ada, dan mengaktifkan atau menonaktifkan peristiwa Wawasan.
- `get-insight-selectors` untuk mengembalikan informasi tentang pemilih acara Insights yang dikonfigurasi untuk penyimpanan data peristiwa.
- `add-tags` untuk menambahkan satu atau lebih tag (pasangan kunci-nilai) ke penyimpanan data peristiwa yang ada.
- `remove-tags` untuk menghapus satu atau beberapa tag dari penyimpanan data acara.
- `list-tags` untuk mengembalikan daftar tag yang terkait dengan penyimpanan data acara.
- `get-event-configuration` untuk mengembalikan kunci tag sumber daya dan kunci kondisi global IAM yang dikonfigurasi untuk penyimpanan data acara. Perintah ini juga mengembalikan apakah penyimpanan data peristiwa dikonfigurasi untuk mengumpulkan peristiwa `Standard` ukuran atau peristiwa `Large` ukuran.
- `put-event-configuration` untuk memperluas ukuran acara dan menambah atau menghapus kunci tag sumber daya dan kunci kondisi global IAM. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.
- `put-resource-policy` untuk melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa. Kebijakan berbasis sumber daya memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.
- `get-resource-policy` untuk mendapatkan kebijakan berbasis sumber daya yang dilampirkan ke penyimpanan data acara.
- `delete-resource-policy` untuk menghapus kebijakan berbasis sumber daya yang dilampirkan ke penyimpanan data peristiwa.

Untuk daftar perintah yang tersedia untuk kueri CloudTrail Lake, lihatPerintah yang tersedia untuk kueri CloudTrail Lake.

Untuk daftar perintah yang tersedia untuk dasbor CloudTrail Lake, lihatPerintah yang tersedia untuk dasbor.

Untuk daftar perintah yang tersedia untuk integrasi CloudTrail Lake, lihatPerintah yang tersedia untuk integrasi CloudTrail Lake.

Buat toko data acara dengan AWS CLI

Bagian ini menjelaskan cara menggunakan `create-event-data-store`perintah untuk membuat penyimpanan data peristiwa dan memberikan contoh berbagai jenis penyimpanan data peristiwa yang dapat Anda buat.

Saat Anda membuat penyimpanan data peristiwa, satu-satunya parameter yang diperlukan adalah`--name`, yang digunakan untuk mengidentifikasi penyimpanan data peristiwa. Anda dapat mengonfigurasi parameter opsional tambahan, termasuk:

- `--advanced-event-selectors`- Menentukan jenis acara untuk dimasukkan dalam penyimpanan data acara. Secara default, data acara menyimpan log semua peristiwa manajemen. Untuk informasi selengkapnya tentang penyeleksi peristiwa lanjutan, lihat AdvancedEventSelectordi Referensi CloudTrail API.
- `--kms-key-id`- Menentukan ID kunci KMS untuk digunakan untuk mengenkripsi peristiwa yang disampaikan oleh. CloudTrail Nilai dapat berupa nama alias yang diawali oleh`alias/`, ARN yang ditentukan sepenuhnya ke alias, ARN yang ditentukan sepenuhnya ke kunci, atau pengidentifikasi unik global.
- `--multi-region-enabled`- Membuat penyimpanan data acara Multi-wilayah yang mencatat peristiwa untuk semua yang ada Wilayah AWS di akun Anda. Secara default, `--multi-region-enabled` diatur, bahkan jika parameter tidak ditambahkan.
- `--organization-enabled`- Memungkinkan penyimpanan data acara untuk mengumpulkan acara untuk semua akun dalam suatu organisasi. Secara default, penyimpanan data acara tidak diaktifkan untuk semua akun dalam organisasi.
- `--billing-mode`- Menentukan biaya untuk menelan dan menyimpan acara, dan periode retensi default dan maksimum untuk penyimpanan data acara.

  Berikut ini adalah nilai yang mungkin:

  - `EXTENDABLE_RETENTION_PRICING`- Mode penagihan ini umumnya direkomendasikan jika Anda menelan kurang dari 25 TB data acara sebulan dan menginginkan periode retensi yang fleksibel hingga 3653 hari (sekitar 10 tahun). Periode retensi default untuk mode penagihan ini adalah 366 hari.
  - `FIXED_RETENTION_PRICING`- Mode penagihan ini disarankan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara per bulan dan membutuhkan periode retensi hingga 2557 hari (sekitar 7 tahun). Periode retensi default untuk mode penagihan ini adalah 2557 hari.

  Nilai default-nya adalah `EXTENDABLE_RETENTION_PRICING`.

- `--retention-period`- Jumlah hari untuk menyimpan acara di penyimpanan data acara. Nilai yang valid adalah bilangan bulat antara 7 dan 3653 jika `--billing-mode` ada`EXTENDABLE_RETENTION_PRICING`, atau antara 7 dan 2557 jika `--billing-mode` diatur ke. `FIXED_RETENTION_PRICING` Jika Anda tidak menentukan`--retention-period`, CloudTrail menggunakan periode retensi default untuk`--billing-mode`.
- `--start-ingestion`- `--start-ingestion` Parameter memulai konsumsi acara pada penyimpanan data acara saat dibuat. Parameter ini diatur bahkan jika parameter tidak ditambahkan.

  Tentukan `--no-start-ingestion` jika Anda tidak ingin penyimpanan data acara menelan acara langsung. Misalnya, Anda mungkin ingin mengatur parameter ini jika Anda menyalin peristiwa ke penyimpanan data peristiwa dan hanya berencana untuk menggunakan data peristiwa untuk menganalisis peristiwa masa lalu. `--no-start-ingestion`Parameter ini hanya valid jika `eventCategory` adalah`Management`,`Data`, atau`ConfigurationItem`.

Contoh berikut menunjukkan cara membuat berbagai jenis penyimpanan data acara.

Contoh:

- Buat penyimpanan data acara untuk peristiwa data S3 dengan AWS CLI
- Buat penyimpanan data acara untuk acara aktivitas jaringan KMS dengan AWS CLI
- Buat penyimpanan data acara untuk item AWS Config konfigurasi dengan AWS CLI
- Buat penyimpanan data acara organisasi untuk acara manajemen dengan AWS CLI
- Membuat penyimpanan data acara untuk acara Insights dengan AWS CLI

Buat penyimpanan data acara untuk peristiwa data S3 dengan AWS CLI

create-event-data-storePerintah example AWS Command Line Interface (AWS CLI) berikut membuat penyimpanan data peristiwa bernama `my-event-data-store` yang memilih semua peristiwa data Amazon S3 dan dienkripsi menggunakan kunci KMS.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
```

```
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
    ]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
```

```
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

Buat penyimpanan data acara untuk acara aktivitas jaringan KMS dengan AWS CLI

Contoh berikut menunjukkan cara membuat penyimpanan data acara untuk menyertakan peristiwa aktivitas `VpceAccessDenied` jaringan untuk AWS KMS. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa dan `eventSource` bidang sama dengan`kms.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
```

```
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Untuk informasi selengkapnya tentang peristiwa aktivitas jaringan, lihatMencatat peristiwa aktivitas jaringan.

Buat penyimpanan data acara untuk item AWS Config konfigurasi dengan AWS CLI

Contoh AWS CLI create-event-data-store perintah berikut menciptakan sebuah event data store bernama `config-items-eds` yang memilih item AWS Config konfigurasi. Untuk mengumpulkan item konfigurasi, tentukan bahwa `eventCategory` `ConfigurationItem` bidang Sama dengan pemilih acara lanjutan.

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

Buat penyimpanan data acara organisasi untuk acara manajemen dengan AWS CLI

AWS CLI create-event-data-storePerintah contoh berikut membuat penyimpanan data acara organisasi yang mengumpulkan semua peristiwa manajemen dan menetapkan `--billing-mode` parameter ke`FIXED_RETENTION_PRICING`.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

Membuat penyimpanan data acara untuk acara Insights dengan AWS CLI

Untuk mencatat peristiwa Insights di CloudTrail Lake, Anda memerlukan penyimpanan data acara tujuan yang mengumpulkan peristiwa Wawasan dan penyimpanan data peristiwa sumber yang memungkinkan Insights dan peristiwa manajemen log.

Prosedur ini menunjukkan kepada Anda cara membuat penyimpanan data peristiwa tujuan dan sumber, lalu mengaktifkan peristiwa Wawasan.

1. Jalankan aws cloudtrail create-event-data-storeperintah untuk membuat penyimpanan data acara tujuan yang mengumpulkan peristiwa Wawasan. Nilai untuk `eventCategory` harus `Insight`. Ganti *`retention-period-days`* dengan jumlah hari Anda ingin menyimpan acara di penyimpanan data acara Anda. Nilai yang valid adalah bilangan bulat antara 7 dan 3653 jika `--billing-mode` ada`EXTENDABLE_RETENTION_PRICING`, atau antara 7 dan 2557 jika `--billing-mode` diatur ke. `FIXED_RETENTION_PRICING` Jika Anda tidak menentukan`--retention-period`, CloudTrail menggunakan periode retensi default untuk`--billing-mode`.

   Jika Anda masuk dengan akun manajemen untuk AWS Organizations organisasi, sertakan `--organization-enabled` parameter jika Anda ingin memberikan akses administrator yang didelegasikan ke penyimpanan data peristiwa.

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
         "Name": "Select Insights events",
         "FieldSelectors": [
             { "Field": "eventCategory", "Equals": ["Insight"] }
           ]
       }
     ]'
   ```

   Berikut ini adalah contoh respons.

   ```
   {
       "Name": "insights-event-data-store",
       "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
   EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
   ```

```
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
             ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

Anda akan menggunakan ARN (atau akhiran ID ARN) dari respons sebagai nilai untuk parameter `--insights-destination` pada langkah 3.

2. Jalankan aws cloudtrail create-event-data-storeperintah untuk membuat penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen. Secara default, data acara menyimpan log semua peristiwa manajemen. Anda tidak perlu menentukan pemilih acara lanjutan jika Anda ingin mencatat semua peristiwa manajemen. Ganti *`retention-period-days`* dengan jumlah hari Anda ingin menyimpan acara di penyimpanan data acara Anda. Nilai yang valid adalah bilangan bulat antara 7 dan 3653 jika `--billing-mode` ada`EXTENDABLE_RETENTION_PRICING`, atau antara 7 dan 2557 jika `--billing-mode` diatur ke. `FIXED_RETENTION_PRICING` Jika Anda tidak menentukan`--retention-period`, CloudTrail menggunakan periode retensi default untuk`--billing-mode`. Jika Anda membuat penyimpanan data acara organisasi, sertakan `--organization-enabled` parameternya.

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

Anda akan menggunakan ARN (atau akhiran ID ARN) dari respons sebagai nilai untuk parameter `--event-data-store` pada langkah 3.

3. Jalankan put-insight-selectorsperintah untuk mengaktifkan peristiwa Insights. Nilai pemilih wawasan dapat berupa`ApiCallRateInsight`,`ApiErrorRateInsight`, atau keduanya. Untuk `--event-data-store` parameter, tentukan ARN (atau akhiran ID ARN) dari penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen dan akan mengaktifkan Wawasan. Untuk `--insights-destination` parameternya, tentukan ARN (atau akhiran ID ARN) dari penyimpanan data peristiwa tujuan yang akan mencatat peristiwa Wawasan.

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
```

```
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Hasil berikut menunjukkan pemilih peristiwa Insights yang dikonfigurasi untuk penyimpanan data peristiwa.

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data acara, CloudTrail mungkin memerlukan waktu hingga 7 hari untuk mulai mengirimkan peristiwa Insights, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

CloudTrail Wawasan menganalisis peristiwa manajemen yang terjadi di satu Wilayah, bukan secara global. Peristiwa CloudTrail Wawasan dihasilkan di Wilayah yang sama dengan peristiwa manajemen pendukungnya yang dihasilkan.

Untuk penyimpanan data acara organisasi, CloudTrail menganalisis peristiwa manajemen dari akun masing-masing anggota alih-alih menganalisis agregasi semua peristiwa manajemen untuk organisasi.

Biaya tambahan berlaku untuk menelan acara Insights di CloudTrail Danau. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jalur dan acara. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Impor peristiwa jejak ke penyimpanan data acara dengan AWS CLI

Bagian ini menunjukkan cara membuat dan mengkonfigurasi penyimpanan data peristiwa dengan menjalankan create-event-data-storeperintah dan kemudian bagaimana mengimpor peristiwa ke penyimpanan data peristiwa dengan menggunakan start-importperintah. Untuk informasi selengkapnya tentang mengimpor acara jejak, lihatSalin peristiwa jejak ke penyimpanan data peristiwa.

Bersiap untuk mengimpor acara jejak

Sebelum Anda mengimpor acara jejak, buat persiapan berikut.

- Pastikan Anda memiliki peran dengan izin yang diperlukan untuk mengimpor peristiwa jejak ke penyimpanan data peristiwa.
- Tentukan --billing-modenilai yang ingin Anda tentukan untuk penyimpanan data acara. Ini `--billing-mode` menentukan biaya menelan dan menyimpan acara, dan periode retensi default dan maksimum untuk penyimpanan data acara.

  Saat Anda mengimpor peristiwa jejak ke CloudTrail Lake, CloudTrail buka ritsleting log yang disimpan dalam format gzip (terkompresi). Kemudian CloudTrail salin peristiwa yang terkandung dalam log ke penyimpanan data acara Anda. Ukuran data yang tidak terkompresi bisa lebih besar dari ukuran penyimpanan Amazon S3 yang sebenarnya. Untuk mendapatkan perkiraan umum ukuran data yang tidak terkompresi, kalikan ukuran log di bucket S3 dengan 10. Anda dapat menggunakan estimasi ini untuk memilih `--billing-mode` nilai untuk kasus penggunaan Anda.
- Tentukan nilai yang ingin Anda tentukan untuk`--retention-period`. CloudTrail tidak akan menyalin peristiwa jika `eventTime` lebih tua dari periode retensi yang ditentukan.

  Untuk menentukan periode retensi yang sesuai, ambil jumlah peristiwa tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara seperti yang ditunjukkan dalam persamaan ini:

  Periode retensi = *`oldest-event-in-days`* + *`number-days-to-retain`*

  Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.
- Putuskan apakah Anda ingin menggunakan penyimpanan data acara untuk menganalisis peristiwa masa depan. Jika Anda tidak ingin menelan peristiwa masa depan, sertakan `--no-start-ingestion` parameter saat Anda membuat penyimpanan data acara. Secara default, toko data acara mulai menelan peristiwa saat dibuat.

Untuk membuat penyimpanan data acara dan mengimpor peristiwa jejak ke penyimpanan data acara tersebut

1. Jalankan create-event-data-store perintah untuk membuat penyimpanan data acara baru. Dalam contoh ini, `--retention-period` diatur ke `120` karena acara tertua yang disalin adalah 90 hari dan kami ingin mempertahankan acara selama 30 hari. `--no-start-ingestion`Parameter diatur karena kami tidak ingin menelan peristiwa masa depan apa pun. Dalam contoh ini, `--billing-mode` tidak disetel, karena kami menggunakan nilai default `EXTENDABLE_RETENTION_PRICING` seperti yang kami harapkan untuk menelan kurang dari 25 TB data peristiwa.

   > **Note**
   >
   > Jika Anda membuat penyimpanan data acara untuk menggantikan jejak Anda, kami sarankan untuk mengonfigurasi `--advanced-event-selectors` agar sesuai dengan pemilih acara jejak Anda untuk memastikan Anda memiliki cakupan acara yang sama. Secara default, data acara menyimpan log semua peristiwa manajemen.

   ```
   aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
    120 --no-start-ingestion
   ```

   Berikut ini adalah contoh responsnya:

   ```
   {
       "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
   EXAMPLEa-4357-45cd-bce5-17ec652719d9",
       "Name": "import-trail-eds",
       "Status": "CREATED",
       "AdvancedEventSelectors": [
           {
               "Name": "Default management events",
               "FieldSelectors": [
                   {
                       "Field": "eventCategory",
                       "Equals": [
                           "Management"
                       ]
                   }
   ```

```
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

Awal `Status` adalah `CREATED` jadi kita akan menjalankan get-event-data-store perintah untuk memverifikasi konsumsi dihentikan.

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

Tanggapan menunjukkan `Status` sekarang`STOPPED_INGESTION`, yang menunjukkan penyimpanan data acara tidak menelan acara langsung.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. Jalankan start-import perintah untuk mengimpor peristiwa jejak ke penyimpanan data acara yang dibuat pada langkah 1. Tentukan ARN (atau akhiran ID dari ARN) dari penyimpanan data peristiwa sebagai nilai untuk parameter. `--destinations` Untuk `--start-event-time` tentukan `eventTime` untuk acara tertua yang ingin Anda salin dan untuk `--end-event-time` tentukan `eventTime` acara terbaru yang ingin Anda salin. Untuk `--import-source` menentukan URI S3 untuk bucket S3 yang berisi log jejak Anda, bucket Wilayah AWS untuk S3, dan ARN peran yang digunakan untuk mengimpor peristiwa jejak.

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

Berikut ini adalah contoh respons.

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
```

```
    },
    "ImportStatus": "INITIALIZING",
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. Jalankan get-importperintah untuk mendapatkan informasi tentang impor.

```
aws cloudtrail get-import --import-id import-id
```

Berikut ini adalah contoh respons.

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

Impor selesai dengan a `ImportStatus` of `COMPLETED` jika tidak ada kegagalan, atau `FAILED` jika ada kegagalan.

Jika impor memilikiFailedEntries, Anda dapat menjalankan list-import-failuresperintah untuk mengembalikan daftar kegagalan.

```
aws cloudtrail list-import-failures --import-id import-id
```

Untuk mencoba lagi impor yang mengalami kegagalan, jalankan start-import perintah hanya dengan --import-id parameter. Saat Anda mencoba kembali impor, CloudTrail melanjutkan impor di lokasi di mana kegagalan terjadi.

```
aws cloudtrail start-import --import-id import-id
```

Perbarui penyimpanan data acara dengan AWS CLI

Bagian ini memberikan contoh yang menunjukkan cara memperbarui pengaturan penyimpanan data peristiwa dengan menjalankan AWS CLI update-event-data-store perintah.

Contoh:

- Perbarui mode penagihan dengan AWS CLI
- Perbarui mode retensi, aktifkan perlindungan terminasi, dan tentukan a AWS KMS key dengan AWS CLI
- Nonaktifkan perlindungan terminasi dengan AWS CLI

Perbarui mode penagihan dengan AWS CLI

--billing-modeUntuk penyimpanan data acara menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Jika penyimpanan data acara --billing-mode disetel keFIXED_RETENTION_PRICING, Anda dapat mengubah nilainya menjadiEXTENDABLE_RETENTION_PRICING. EXTENDABLE_RETENTION_PRICINGUmumnya direkomendasikan jika penyimpanan data acara Anda menelan kurang dari 25 TB data peristiwa per bulan dan Anda menginginkan periode retensi yang fleksibel hingga 3653 hari. Untuk informasi tentang harga, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

> **Note**
>
> Anda tidak dapat mengubah `--billing-mode` nilai dari `EXTENDABLE_RETENTION_PRICING` ke`FIXED_RETENTION_PRICING`. Jika mode penagihan penyimpanan data peristiwa diatur ke `EXTENDABLE_RETENTION_PRICING` dan Anda ingin menggunakannya `FIXED_RETENTION_PRICING` sebagai gantinya, Anda dapat menghentikan konsumsi pada penyimpanan data acara dan membuat penyimpanan data acara baru yang digunakan. `FIXED_RETENTION_PRICING`

Contoh AWS CLI update-event-data-store perintah berikut mengubah `--billing-mode` untuk penyimpanan data acara dari `FIXED_RETENTION_PRICING` ke`EXTENDABLE_RETENTION_PRICING`. Nilai `--event-data-store` parameter yang diperlukan adalah ARN (atau akhiran ID ARN) dan diperlukan; parameter lainnya bersifat opsional.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Perbarui mode retensi, aktifkan perlindungan terminasi, dan tentukan a AWS KMS key dengan AWS CLI

Contoh AWS CLI update-event-data-store perintah berikut memperbarui penyimpanan data peristiwa untuk mengubah periode retensi menjadi 100 hari, dan mengaktifkan perlindungan penghentian. Nilai `--event-data-store` parameter yang diperlukan adalah ARN (atau akhiran ID ARN) dan diperlukan; parameter lainnya bersifat opsional. Dalam contoh ini, `--retention-period` parameter ditambahkan untuk mengubah periode retensi menjadi 100 hari. Secara opsional, Anda dapat memilih untuk mengaktifkan AWS Key Management Service enkripsi dan menentukan AWS KMS key dengan menambahkan `--kms-key-id` ke perintah, dan menentukan ARN kunci KMS sebagai nilai. `--termination-protection-enabled`ditambahkan untuk mengaktifkan perlindungan penghentian pada penyimpanan data peristiwa yang tidak mengaktifkan perlindungan penghentian.

Penyimpanan data peristiwa yang mencatat peristiwa dari luar AWS tidak dapat diperbarui untuk mencatat AWS peristiwa. Demikian pula, penyimpanan data peristiwa yang mencatat AWS peristiwa tidak dapat diperbarui untuk mencatat peristiwa dari luar AWS.

> **Note**
>
> Jika Anda mengurangi periode retensi penyimpanan data acara, CloudTrail akan menghapus peristiwa dengan periode retensi yang `eventTime` lebih lama dari periode penyimpanan baru. Misalnya, jika periode retensi sebelumnya adalah 365 hari dan Anda menguranginya menjadi 100 hari, CloudTrail akan menghapus acara dengan `eventTime` lebih dari 100 hari.

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
```

```
--termination-protection-enabled
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Nonaktifkan perlindungan terminasi dengan AWS CLI

Secara default, perlindungan penghentian diaktifkan pada penyimpanan data peristiwa untuk melindungi penyimpanan data peristiwa dari penghapusan yang tidak disengaja. Anda tidak dapat menghapus penyimpanan data peristiwa saat perlindungan penghentian diaktifkan. Jika Anda ingin menghapus penyimpanan data acara, Anda harus menonaktifkan perlindungan penghentian terlebih dahulu.

Contoh AWS CLI update-event-data-store perintah berikut menonaktifkan perlindungan terminasi dengan melewati `--no-termination-protection-enabled` parameter.

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": false,
```

```
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Mengelola penyimpanan data acara dengan AWS CLI

Bagian ini menjelaskan beberapa perintah lain yang dapat Anda jalankan untuk mendapatkan informasi tentang penyimpanan data acara Anda, memulai dan menghentikan konsumsi pada penyimpanan data acara, dan mengaktifkan dan menonaktifkan federasi pada penyimpanan data acara.

Topik

- Dapatkan penyimpanan data acara dengan AWS CLI
- Daftar semua penyimpanan data acara di akun dengan AWS CLI
- Tambahkan kunci tag sumber daya dan kunci kondisi global IAM, dan perluas ukuran acara
- Dapatkan konfigurasi acara untuk penyimpanan data acara
- Dapatkan kebijakan berbasis sumber daya untuk penyimpanan data acara dengan AWS CLI
- Lampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa dengan AWS CLI
- Hapus kebijakan berbasis sumber daya yang dilampirkan ke penyimpanan data peristiwa dengan AWS CLI
- Hentikan konsumsi pada penyimpanan data acara dengan AWS CLI
- Mulai menelan pada penyimpanan data acara dengan AWS CLI
- Aktifkan federasi pada penyimpanan data acara
- Nonaktifkan federasi pada penyimpanan data acara
- Kembalikan penyimpanan data acara dengan AWS CLI

Dapatkan penyimpanan data acara dengan AWS CLI

Contoh AWS CLI get-event-data-store perintah berikut mengembalikan informasi tentang penyimpanan data peristiwa yang ditentukan oleh `--event-data-store` parameter yang diperlukan, yang menerima ARN atau akhiran ID dari ARN.

```
aws cloudtrail get-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Berikut ini adalah contoh respons. Pembuatan dan waktu pembaruan terakhir dalam `timestamp` format.

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::amzn-s3-demo-bucket"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

Daftar semua penyimpanan data acara di akun dengan AWS CLI

AWS CLI list-event-data-storesPerintah contoh berikut mengembalikan informasi tentang semua data peristiwa yang disimpan di akun, di Wilayah saat ini. Parameter opsional termasuk`--max-results`, untuk menentukan jumlah maksimum hasil yang Anda inginkan perintah untuk kembali pada satu halaman. Jika ada lebih banyak hasil daripada `--max-results` nilai yang Anda tentukan, jalankan perintah lagi dengan menambahkan `NextToken` nilai yang dikembalikan untuk mendapatkan halaman hasil berikutnya.

```
aws cloudtrail list-event-data-stores
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
```

```
}
```

Tambahkan kunci tag sumber daya dan kunci kondisi global IAM, dan perluas ukuran acara

Jalankan AWS CLI `put-event-configuration` perintah untuk memperluas ukuran acara maksimum dan menambahkan hingga 50 kunci tag sumber daya dan 50 kunci kondisi global IAM untuk memberikan metadata tambahan tentang acara Anda.

`put-event-configuration`Perintah menerima argumen berikut:

- `--event-data-store`— Tentukan ARN dari penyimpanan data acara atau akhiran ID dari ARN. Parameter ini diperlukan.
- `--max-event-size`— Setel `Large` untuk mengatur ukuran acara maksimum ke 1 MB. Secara default, nilainya adalah`Standard`, yang menentukan ukuran acara maksimum 256 KB.

> **Note**
>
> Untuk menambahkan kunci tag sumber daya atau kunci kondisi global IAM, Anda harus mengatur ukuran acara `Large` untuk memastikan semua kunci yang ditambahkan disertakan dalam acara tersebut.

- `--context-key-selectors`— Tentukan jenis kunci yang ingin Anda sertakan dalam acara yang dikumpulkan oleh penyimpanan data acara Anda. Anda dapat menyertakan kunci tag sumber daya dan kunci kondisi global IAM. Informasi tentang tag sumber daya yang ditambahkan dan kunci kondisi global IAM ditampilkan di `eventContext` bidang dalam acara tersebut. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.
  - Atur `Type` to `TagContext` to pass dalam array hingga 50 kunci tag sumber daya. Jika Anda menambahkan tag sumber daya, CloudTrail peristiwa akan menyertakan kunci tag yang dipilih yang terkait dengan sumber daya yang terlibat dalam panggilan API. Peristiwa API yang terkait dengan sumber daya yang dihapus tidak akan memiliki tag sumber daya.
  - Atur `Type` to `RequestContext` to pass dalam array hingga 50 kunci kondisi global IAM. Jika Anda menambahkan kunci kondisi global IAM, CloudTrail peristiwa akan menyertakan informasi tentang kunci kondisi yang dipilih yang dievaluasi selama proses otorisasi, termasuk detail tambahan tentang prinsipal, sesi, jaringan, dan permintaan itu sendiri.

Contoh berikut menetapkan ukuran acara maksimum `Large` dan menambahkan dua kunci tag sumber daya `myTagKey1` dan`myTagKey2`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"TagContext", "Equals":["myTagKey1","myTagKey2"]}]'
```

Contoh berikutnya menetapkan ukuran acara maksimum `Large` dan menambahkan IAM; global condition key (`aws:MultiFactorAuthAge`).

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"RequestContext", "Equals":
["aws:MultiFactorAuthAge"]}]'
```

Contoh terakhir menghapus semua kunci tag sumber daya dan kunci kondisi global IAM dan menetapkan ukuran peristiwa maksimum ke`Standard`.

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Standard \
--context-key-selectors
```

Dapatkan konfigurasi acara untuk penyimpanan data acara

Jalankan AWS CLI `get-event-configuration` perintah untuk mengembalikan konfigurasi acara untuk penyimpanan data peristiwa yang mengumpulkan CloudTrail peristiwa. Perintah ini mengembalikan ukuran acara maksimum dan mencantumkan kunci tag sumber daya dan kunci kondisi global IAM (jika ada) yang disertakan dalam CloudTrail peristiwa.

```
aws cloudtrail get-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Dapatkan kebijakan berbasis sumber daya untuk penyimpanan data acara dengan AWS CLI

Contoh berikut menjalankan `get-resource-policy` perintah pada penyimpanan data acara organisasi.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

Karena perintah dijalankan pada penyimpanan data peristiwa organisasi, output akan menampilkan kebijakan berbasis sumber daya yang disediakan dan yang `DelegatedAdminResourcePolicy`dihasilkan untuk akun administrator yang didelegasikan.

Lampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa dengan AWS CLI

Untuk menjalankan kueri di dasbor selama penyegaran manual atau terjadwal, Anda perlu melampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa yang terkait dengan widget di dasbor. Hal ini memungkinkan CloudTrail Lake untuk menjalankan kueri atas nama Anda. Untuk informasi selengkapnya tentang kebijakan berbasis sumber daya, lihat. Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor

Contoh berikut melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa yang memungkinkan CloudTrail untuk menjalankan kueri di dasbor saat dasbor di-refresh. Kebijakan dibuat dalam file terpisah*policy.json*, dengan contoh pernyataan kebijakan berikut:

JSON

```
{ "Version":"2012-10-17",        "Statement": [{ "Sid": "EDSPolicy", "Effect":
    "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
event_data_store_ID",
    "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE",
    "AWS:SourceAccount": "123456789012" } } } ] }
```

Ganti *123456789012* dengan ID akun Anda, *arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/event_data_store_ID* dengan ARN penyimpanan data acara yang CloudTrail akan menjalankan kueri, dan *arn:aws:cloudtrail:us-*

east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy file://policy.json
```

Berikut ini adalah contoh responsnya.

```
{ "ResourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE", "ResourcePolicy": "policy-statement" }
```

Untuk contoh kebijakan tambahan, lihatResource-based contoh kebijakan untuk penyimpanan data acara.

Hapus kebijakan berbasis sumber daya yang dilampirkan ke penyimpanan data peristiwa dengan AWS CLI

Contoh berikut menghapus kebijakan berbasis sumber daya yang dilampirkan ke penyimpanan data peristiwa. Ganti *eds-arn* dengan ARN dari penyimpanan data acara.

```
aws cloudtrail delete-resource-policy --resource-arn eds-arn
```

Perintah ini tidak menghasilkan output jika berhasil.

Hentikan konsumsi pada penyimpanan data acara dengan AWS CLI

Contoh AWS CLI stop-event-data-store-ingestion perintah berikut menghentikan penyimpanan data peristiwa dari menelan peristiwa. Untuk menghentikan konsumsi, penyimpanan data acara `Status` harus `ENABLED` dan `eventCategory` harus`Management`,`Data`, atau. `ConfigurationItem` Penyimpanan data peristiwa ditentukan oleh`--event-data-store`, yang menerima ARN penyimpanan data peristiwa, atau akhiran ID ARN. Setelah Anda menjalankanstop-event-data-store-ingestion, status penyimpanan data acara berubah menjadi`STOPPED_INGESTION`.

Penyimpanan data acara dihitung terhadap akun Anda maksimal sepuluh penyimpanan data peristiwa saat statusnya`STOPPED_INGESTION`.

```
aws cloudtrail stop-event-data-store-ingestion \
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Tidak ada respon jika operasi berhasil.

Mulai menelan pada penyimpanan data acara dengan AWS CLI

Contoh AWS CLI start-event-data-store-ingestion perintah berikut memulai konsumsi acara pada penyimpanan data acara. Untuk memulai konsumsi, penyimpanan data acara `Status` harus `STOPPED_INGESTION` dan `eventCategory` harus`Management`,`Data`, atau. `ConfigurationItem` Penyimpanan data peristiwa ditentukan oleh`--event-data-store`, yang menerima ARN penyimpanan data peristiwa, atau akhiran ID ARN. Setelah Anda menjalankan`start-event-data-store-ingestion`, status penyimpanan data acara berubah menjadi`ENABLED`.

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

Tidak ada respon jika operasi berhasil.

Aktifkan federasi pada penyimpanan data acara

Untuk mengaktifkan federasi, jalankan aws cloudtrail enable-federation perintah, berikan yang diperlukan `--event-data-store` dan `--role` parameter. Untuk`--event-data-store`, berikan ARN penyimpanan data acara (atau akhiran ID ARN). Untuk`--role`, berikan ARN untuk peran federasi Anda. Peran harus ada di akun Anda dan memberikan izin minimum yang diperlukan.

```
aws cloudtrail enable-federation \
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Contoh ini menunjukkan bagaimana administrator yang didelegasikan dapat mengaktifkan federasi pada penyimpanan data acara organisasi dengan menentukan ARN penyimpanan data acara di akun manajemen dan ARN peran federasi dalam akun administrator yang didelegasikan.

```
aws cloudtrail enable-federation \
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-
id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Nonaktifkan federasi pada penyimpanan data acara

Untuk menonaktifkan federasi pada penyimpanan data acara, jalankan aws cloudtrail disable-federation perintah. Penyimpanan data peristiwa ditentukan oleh`--event-data-store`, yang menerima ARN penyimpanan data peristiwa atau akhiran ID ARN.

```
aws cloudtrail disable-federation \
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Jika ini adalah penyimpanan data acara organisasi, gunakan ID akun untuk akun manajemen.

Kembalikan penyimpanan data acara dengan AWS CLI

Contoh AWS CLI restore-event-data-store perintah berikut mengembalikan penyimpanan data peristiwa yang tertunda penghapusan. Penyimpanan data peristiwa ditentukan oleh`--event-data-store`, yang menerima ARN penyimpanan data peristiwa atau akhiran ID ARN. Anda hanya dapat memulihkan penyimpanan data peristiwa yang dihapus dalam periode tunggu tujuh hari setelah penghapusan.

```
aws cloudtrail restore-event-data-store \
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Tanggapan tersebut mencakup informasi tentang penyimpanan data acara, termasuk ARN, pemilih acara lanjutan, dan status restorasi.

Hapus penyimpanan data acara dengan AWS CLI

Bagian ini menunjukkan cara menghapus penyimpanan data acara dengan menjalankan perintah AWS CLI `delete-event-data-store`

Untuk menghapus penyimpanan data peristiwa, tentukan `--event-data-store` dengan menyediakan ARN penyimpanan data acara, atau akhiran ID ARN. Setelah Anda menjalankandelete-event-data-store, status akhir dari penyimpanan data acara adalah`PENDING_DELETION`, dan penyimpanan data acara secara otomatis dihapus setelah masa tunggu 7 hari.

Setelah Anda menjalankan delete-event-data-store penyimpanan data peristiwa, Anda tidak dapat menjalankan list-queriesdescribe-query, atau get-query-results pada kueri yang menggunakan penyimpanan data yang dinonaktifkan. Penyimpanan data acara dihitung terhadap akun Anda maksimal sepuluh penyimpanan data peristiwa di Wilayah AWS saat penghapusan tertunda.

> **Note**
>
> Anda tidak dapat menghapus penyimpanan data peristiwa jika `--termination-protection-enabled` disetel atau `FederationStatus` sudah diatur`ENABLED`. Untuk menghapus penyimpanan data peristiwa dengan `eventCategory` dari`ActivityAuditLog`, Anda harus terlebih dahulu menghapus saluran integrasi. Anda dapat menghapus saluran dengan menggunakan `aws cloudtrail delete-channel` perintah. Untuk informasi selengkapnya, lihat Hapus saluran untuk menghapus integrasi dengan AWS CLI.

```
aws cloudtrail delete-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Tidak ada respon jika operasi berhasil.

Mengelola siklus hidup penyimpanan data acara

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Berikut ini adalah tahapan siklus hidup penyimpanan data peristiwa:

- `CREATED`— Status jangka pendek yang menunjukkan bahwa penyimpanan data peristiwa telah dibuat.
- `ENABLED`— Penyimpanan data acara aktif dan menelan peristiwa. Anda dapat menjalankan kueri dan menyalin peristiwa jejak ke penyimpanan data peristiwa.

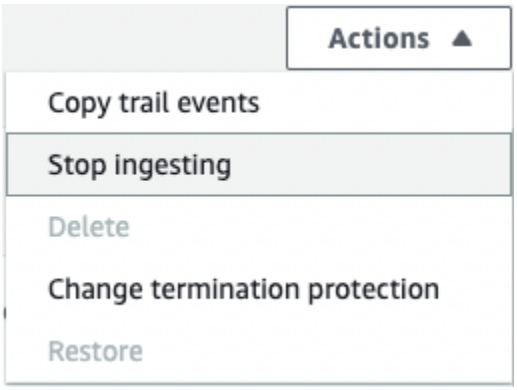
- `STARTING_INGESTION`— Status jangka pendek yang menunjukkan bahwa penyimpanan data acara akan mulai menelan acara langsung.
- `STOPPING_INGESTION`— Status jangka pendek yang menunjukkan bahwa penyimpanan data acara akan berhenti menelan acara langsung.
- `STOPPED_INGESTION`— Penyimpanan data acara tidak mencerna acara langsung. Anda masih dapat menjalankan kueri pada peristiwa apa pun yang sudah ada di penyimpanan data peristiwa dan menyalin peristiwa jejak ke penyimpanan data peristiwa.
- `PENDING_DELETION`— Penyimpanan data acara berada dalam `STOPPED_INGESTION` status `ENABLED` atau dan telah dihapus tetapi berada dalam periode tunggu 7 hari sebelum penghapusan permanen. Anda tidak dapat menjalankan kueri di penyimpanan data peristiwa, dan tidak ada operasi yang dapat dilakukan pada penyimpanan data peristiwa kecuali pemulihan.

Anda hanya dapat menghapus penyimpanan data peristiwa jika perlindungan federasi dan penghentian dinonaktifkan. Perlindungan penghentian mencegah penyimpanan data peristiwa dihapus secara tidak sengaja. Secara default, perlindungan penghentian diaktifkan pada penyimpanan data peristiwa. Federasi memungkinkan Anda menanyakan data penyimpanan data acara Anda di Athena dan dinonaktifkan secara default.

Setelah Anda menghapus penyimpanan data peristiwa, penyimpanan data akan tetap dalam `PENDING_DELETION` status selama 7 hari sebelum dihapus secara permanen. Anda dapat memulihkan penyimpanan data peristiwa selama periode tunggu 7 hari. Saat berada di `PENDING_DELETION` status, penyimpanan data peristiwa tidak tersedia untuk kueri, dan tidak ada operasi lain yang dapat dilakukan pada penyimpanan data peristiwa kecuali operasi pemulihan. Penyimpanan data peristiwa yang tertunda penghapusan tidak menyerap peristiwa dan tidak menimbulkan biaya. Namun, penyimpanan data peristiwa yang tertunda penghapusan dihitung terhadap kuota penyimpanan data peristiwa yang dapat ada dalam satu Wilayah AWS.

Tindakan yang tersedia di penyimpanan data acara

Untuk menghapus atau memulihkan penyimpanan data peristiwa, meny alin peristiwa jejak, memulai atau menghentikan penyerapan peristiwa, atau mengaktifkan atau menonaktifkan perlindungan penghentian penyimpanan data peristiwa, gunakan perintah pada menu Tindakan pada halaman detail penyimpanan data peristiwa.



Opsi untuk Sal in peristiwa jejak hanya tersedia di penyimpanan data peristiwa yang berisi CloudTrail peristiwa. Opsi untuk Mulai penyerapan dan Hentikan penyerapan hanya tersedia di penyimpanan data peristiwa yang berisi CloudTrail peristiwa (peristiwa manajemen dan data), atau item AWS Config konfigurasi.

Salin peristiwa jejak ke penyimpanan data peristiwa

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake untuk membuat snapshot point-in-time dari peristiwa yang dicatat ke jejak. Menyalin peristiwa jejak tidak mengganggu kemampuan jejak untuk mencatat peristiwa dan tidak mengubah jejak dengan cara apa pun.

Anda dapat menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada yang dikonfigurasi untuk CloudTrail acara, atau Anda dapat membuat penyimpanan data CloudTrail acara baru dan memilih opsi Salin peristiwa jejak sebagai bagian dari pembuatan penyimpanan data acara. Untuk informasi selengkapnya tentang menyalin peristiwa jejak ke penyimpanan data acara yang ada, lihatSalin peristiwa jejak ke penyimpanan data acara yang ada dengan konsol. Untuk informasi selengkapnya tentang membuat penyimpanan data acara baru, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

Jika Anda menyalin peristiwa jejak ke penyimpanan data acara organisasi, Anda harus menggunakan akun manajemen untuk organisasi. Anda tidak dapat menyalin peristiwa jejak menggunakan akun administrator yang didelegasikan untuk organisasi.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Danau, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

Saat Anda menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data tidak terkompresi yang dikonsumsi oleh penyimpanan data acara.

Saat Anda menyalin peristiwa jejak ke CloudTrail Lake, CloudTrail buka ritsleting log yang disimpan dalam format gzip (terkompresi) dan kemudian menyalin peristiwa yang terdapat dalam log ke penyimpanan data acara Anda. Ukuran data yang tidak terkompresi bisa lebih besar dari ukuran penyimpanan S3 yang sebenarnya. Untuk mendapatkan perkiraan umum ukuran data yang tidak terkompresi, Anda dapat mengalikan ukuran log di bucket S3 dengan 10.

Anda dapat mengurangi biaya dengan menentukan rentang waktu yang lebih sempit untuk acara yang disalin. Jika Anda berencana untuk hanya menggunakan penyimpanan data acara untuk menanyakan peristiwa yang disalin, Anda dapat menonaktifkan konsumsi acara untuk menghindari timbulnya biaya pada peristiwa masa depan. Untuk informasi lebih lanjut, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

Skenario

Tabel berikut menjelaskan beberapa skenario umum untuk menyalin peristiwa jejak dan bagaimana Anda menyelesaikan setiap skenario menggunakan konsol.

Skenario	Bagaimana cara melakukannya di konsol?
Menganalisis dan menanyakan peristiwa jejak sejarah di CloudTrail Danau tanpa menelan peristiwa baru	Buat penyimpanan data acara baru dan pilih opsi Salin peristiwa jejak sebagai bagian dari pembuatan penyimpanan data acara. Saat membuat penyimpanan data acara, batalkan pilihan acara Ingest (langkah 15 dari prosedur) untuk memastikan penyimpanan data acara hanya berisi peristiwa historis untuk jejak Anda dan tidak ada peristiwa masa depan.

Skenario	Bagaimana cara melakukannya di konsol?
Ganti jejak Anda yang ada dengan penyimpanan data acara CloudTrail Lake	Buat penyimpanan data acara dengan pemilih acara yang sama dengan jejak Anda untuk memastikan bahwa penyimpanan data acara memiliki cakupan yang sama dengan jejak Anda. Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang tanggal untuk peristiwa yang disalin yang lebih awal dari pembuatan penyimpanan data peristiwa. Setelah penyimpanan data acara Anda dibuat, Anda dapat mematikan pencatatan untuk jejak untuk menghindari biaya tambahan.

Topik

- Pertimbangan untuk menyalin acara jejak
- Izin yang diperlukan untuk menyalin peristiwa jejak
- Salin peristiwa jejak ke penyimpanan data acara yang ada dengan konsol
- Salin peristiwa jejak ke penyimpanan data acara baru dengan konsol
- Lihat detail salinan acara dengan CloudTrail konsol

Pertimbangan untuk menyalin acara jejak

Pertimbangkan faktor-faktor berikut saat menyalin peristiwa jejak.

- Saat menyalin peristiwa jejak, CloudTrail gunakan operasi S3 `GetObject`API untuk mengambil peristiwa jejak di bucket S3 sumber. Ada beberapa kelas penyimpanan yang diarsipkan S3, seperti S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts, dan S3 Deep Archive tingkatan yang tidak dapat diakses dengan menggunakan. Intelligent-Tiering `GetObject` Untuk menyalin peristiwa jejak yang disimpan di kelas penyimpanan yang diarsipkan ini, Anda harus terlebih dahulu memulihkan salinan menggunakan operasi S3`RestoreObject`. Untuk informasi tentang memulihkan objek yang diarsipkan, lihat Memulihkan Objek yang Diarsipkan di Panduan Pengguna Amazon S3.

- Saat Anda menyalin peristiwa jejak ke penyimpanan data peristiwa, CloudTrail menyalin semua peristiwa jejak terlepas dari konfigurasi jenis acara penyimpanan data acara tujuan, pemilih acara lanjutan, atau Wilayah AWS.
- Sebelum menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada, pastikan opsi harga dan periode retensi penyimpanan data acara dikonfigurasi dengan tepat untuk kasus penggunaan Anda.
  - Opsi harga: Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan acara. Untuk informasi selengkapnya tentang opsi harga, lihat AWS CloudTrail Harga danOpsi harga toko data acara.
  - Periode retensi: Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Untuk menentukan periode retensi yang sesuai, ambil jumlah acara tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.
- Jika Anda menyalin peristiwa jejak ke penyimpanan data acara untuk diselidiki dan tidak ingin menelan peristiwa masa depan, Anda dapat menghentikan konsumsi di penyimpanan data acara. Saat membuat penyimpanan data acara, batalkan pilihan opsi Ingest event (langkah 15 dari prosedur) untuk memastikan penyimpanan data acara hanya berisi peristiwa historis untuk jejak Anda dan tidak ada peristiwa masa depan.
- Sebelum menyalin peristiwa jejak, nonaktifkan daftar kontrol akses (ACL) apa pun yang dilampirkan ke bucket S3 sumber, dan perbarui kebijakan bucket S3 untuk penyimpanan data peristiwa tujuan. Untuk informasi selengkapnya tentang memperbarui kebijakan bucket S3, lihatKebijakan bucket Amazon S3 untuk menyalin peristiwa jejak. Untuk informasi selengkapnya tentang menonaktifkan ACL, lihat Mengontrol kepemilikan objek dan menonaktifkan ACL untuk bucket Anda.
- CloudTrail hanya menyalin peristiwa jejak dari file log terkompresi Gzip yang ada di bucket S3 sumber. CloudTrail tidak menyalin peristiwa jejak dari file log yang tidak terkompresi, atau file log yang dikompresi menggunakan format selain Gzip.
- Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang waktu untuk peristiwa yang disalin yang lebih awal dari pembuatan penyimpanan data peristiwa.

- Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam awalan bucket S3 dan `CloudTrail` awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, Anda harus memilih awalan saat menyalin peristiwa jejak.
- Untuk menyalin peristiwa jejak ke penyimpanan data acara organisasi, Anda harus menggunakan akun manajemen untuk organisasi. Anda tidak dapat menggunakan akun administrator yang didelegasikan untuk menyalin peristiwa jejak ke penyimpanan data acara organisasi.

Izin yang diperlukan untuk menyalin peristiwa jejak

Sebelum menyalin peristiwa jejak, pastikan Anda memiliki semua izin yang diperlukan untuk peran IAM Anda. Anda hanya perlu memperbarui izin peran IAM jika memilih peran IAM yang ada untuk menyalin peristiwa jejak. Jika Anda memilih untuk membuat peran IAM baru, CloudTrail berikan semua izin yang diperlukan untuk peran tersebut.

Jika bucket S3 sumber menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Jika bucket S3 sumber menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci agar memungkinkan CloudTrail untuk mendekripsi data dalam bucket.

Topik

- Izin IAM untuk menyalin peristiwa jejak
- Kebijakan bucket Amazon S3 untuk menyalin peristiwa jejak
- Kebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber

Izin IAM untuk menyalin peristiwa jejak

Saat menyalin peristiwa jejak, Anda memiliki opsi untuk membuat peran IAM baru, atau menggunakan peran IAM yang ada. Saat Anda memilih peran IAM baru, CloudTrail buat peran IAM dengan izin yang diperlukan dan tidak ada tindakan lebih lanjut yang diperlukan di pihak Anda.

Jika Anda memilih peran yang ada, pastikan kebijakan peran IAM memungkinkan CloudTrail untuk menyalin peristiwa jejak dari bucket S3 sumber. Bagian ini memberikan contoh izin peran IAM dan kebijakan kepercayaan yang diperlukan.

Contoh berikut menyediakan kebijakan izin, yang memungkinkan CloudTrail untuk menyalin peristiwa jejak dari bucket S3 sumber. Ganti *`amzn-s3-demo-bucket`*`myAccountID`,*`region`*,*`prefix`*,, dan

eventDataStoreId dengan nilai yang sesuai untuk konfigurasi Anda. *myAccountID*Ini adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

Ganti *key-regionkeyAccountID*,, dan *keyID* dengan nilai untuk kunci KMS yang digunakan untuk mengenkripsi bucket S3 sumber. Anda dapat menghilangkan `AWSCloudTrailImportKeyAccess` pernyataan jika bucket S3 sumber tidak menggunakan kunci KMS untuk enkripsi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
       }
    },
```

```
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

Contoh berikut memberikan kebijakan kepercayaan IAM, yang memungkinkan CloudTrail untuk mengambil peran IAM untuk menyalin peristiwa jejak dari bucket S3 sumber. Ganti *myAccountIDregion*,, dan *eventDataStoreArn* dengan nilai yang sesuai untuk konfigurasi Anda. *myAccountID*Ini adalah Akun AWS ID yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Kebijakan bucket Amazon S3 untuk menyalin peristiwa jejak

Secara default, ember dan objek Amazon S3 bersifat pribadi. Hanya pemilik sumber daya (AWS akun yang membuat bucket) yang dapat mengakses bucket dan objek yang dikandungnya. Pemilik

sumber daya dapat memberikan izin akses ke sumber daya dan pengguna lain dengan menulis kebijakan akses.

Sebelum menyalin peristiwa jejak, Anda harus memperbarui kebijakan bucket S3 CloudTrail agar dapat menyalin peristiwa jejak dari bucket S3 sumber.

Anda dapat menambahkan pernyataan berikut ke kebijakan bucket S3 untuk memberikan izin ini. Ganti *roleArn* dan *amzn-s3-demo-bucket* dengan nilai yang sesuai untuk konfigurasi Anda.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

Kebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber

Jika bucket S3 sumber menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS menyediakan `kms:Decrypt` dan `kms:GenerateDataKey` izin yang diperlukan untuk menyalin peristiwa jejak dari bucket S3 CloudTrail dengan enkripsi diaktifkan. SSE-KMS Jika bucket S3 sumber Anda menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci. Memperbarui kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data di bucket S3 sumber, menjalankan pemeriksaan validasi untuk memastikan bahwa peristiwa sesuai dengan CloudTrail standar, dan menyalin peristiwa ke penyimpanan data peristiwa Lake. CloudTrail

Contoh berikut menyediakan kebijakan kunci KMS, yang memungkinkan CloudTrail untuk mendekripsi data dalam bucket S3 sumber. Ganti *roleArnamzn-s3-demo-bucket*,*myAccountID*,*region*,, dan *eventDataStoreId* dengan nilai yang sesuai untuk

konfigurasi Anda. *myAccountID*Ini adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

Salin peristiwa jejak ke penyimpanan data acara yang ada dengan konsol

Gunakan prosedur berikut untuk menyalin peristiwa jejak ke penyimpanan data acara yang ada. Untuk informasi tentang cara membuat penyimpanan data acara baru, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

> **Note**
>
> Sebelum menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada, pastikan opsi harga dan periode retensi penyimpanan data acara dikonfigurasi dengan tepat untuk kasus penggunaan Anda.
>
> - Opsi harga: Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan acara. Untuk informasi selengkapnya tentang opsi harga, lihat AWS CloudTrail Harga danOpsi harga toko data acara.

- Periode retensi: Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Untuk menentukan periode retensi yang sesuai, ambil jumlah acara tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.

Untuk menyalin peristiwa jejak ke penyimpanan data acara

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih Salin acara jejak.
4. Pada halaman Salin peristiwa jejak, untuk sumber Acara, pilih jejak yang ingin Anda salin. Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam awalan bucket S3 dan `CloudTrail` awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, pilih Masukkan URI S3, lalu pilih Browse S3 untuk menelusuri awalan. Jika bucket S3 sumber untuk jejak menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data. Jika bucket S3 sumber Anda menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci agar memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Untuk informasi selengkapnya tentang memperbarui kebijakan kunci KMS, lihatKebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber.

   Kebijakan bucket S3 harus memberikan CloudTrail akses untuk menyalin peristiwa jejak dari bucket S3 Anda. Untuk informasi selengkapnya tentang memperbarui kebijakan bucket S3, lihatKebijakan bucket Amazon S3 untuk menyalin peristiwa jejak.
5. Untuk Tentukan rentang waktu acara, pilih rentang waktu untuk menyalin acara. CloudTrail memeriksa awalan dan nama file log untuk memverifikasi nama berisi tanggal antara tanggal mulai dan akhir yang dipilih sebelum mencoba menyalin peristiwa jejak. Anda dapat memilih rentang Relatif atau rentang Absolut. Untuk menghindari duplikasi peristiwa antara jejak sumber

dan penyimpanan data peristiwa tujuan, pilih rentang waktu yang lebih awal dari pembuatan penyimpanan data acara.

> **Note**
>
> CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Misalnya, jika periode penyimpanan data acara adalah 90 hari, maka tidak CloudTrail akan menyalin peristiwa jejak apa pun dengan `eventTime` lebih dari 90 hari.

- Jika Anda memilih Rentang relatif, Anda dapat memilih untuk menyalin peristiwa yang dicatat dalam 6 bulan terakhir, 1 tahun, 2 tahun, 7 tahun, atau rentang khusus. CloudTrail menyalin peristiwa yang dicatat dalam periode waktu yang dipilih.
- Jika Anda memilih Rentang absolut, Anda dapat memilih tanggal mulai dan berakhir tertentu. CloudTrail menyalin peristiwa yang terjadi antara tanggal mulai dan akhir yang dipilih.

6. Untuk lokasi Pengiriman, pilih penyimpanan data acara tujuan dari daftar drop-down.
7. Untuk Izin, pilih dari opsi peran IAM berikut. Jika Anda memilih peran IAM yang ada, verifikasi bahwa kebijakan peran IAM menyediakan izin yang diperlukan. Untuk informasi selengkapnya tentang memperbarui izin peran IAM, lihat. Izin IAM untuk menyalin peristiwa jejak

   - Pilih Buat peran baru (disarankan) untuk membuat peran IAM baru. Untuk Masukkan nama peran IAM, masukkan nama untuk peran tersebut. CloudTrail secara otomatis membuat izin yang diperlukan untuk peran baru ini.
   - Pilih Gunakan ARN peran IAM kustom untuk menggunakan peran IAM kustom yang tidak terdaftar. Untuk Masukkan peran IAM ARN, masukkan ARN IAM.
   - Pilih peran IAM yang ada dari daftar drop-down.

8. Pilih Salin acara.
9. Anda diminta untuk mengkonfirmasi. Saat Anda siap untuk mengonfirmasi, pilih Salin acara jejak ke Danau, lalu pilih Salin acara.
10. Pada halaman Salin detail, Anda dapat melihat status salinan dan meninjau kegagalan apa pun. Ketika salinan peristiwa jejak selesai, status Salinannya disetel ke Selesai jika tidak ada kesalahan, atau Gagal jika terjadi kesalahan.

> **Note**
>
> Detail yang ditampilkan di halaman detail salinan acara tidak dalam waktu nyata. Nilai sebenarnya untuk detail seperti Awalan yang disalin mungkin lebih tinggi dari yang ditampilkan di halaman. CloudTrail memperbarui detail secara bertahap selama salinan acara.

11. Jika status Salin Gagal, perbaiki kesalahan yang ditampilkan dalam kegagalan Salin, lalu pilih Coba lagi salin. Ketika Anda mencoba kembali salinan, CloudTrail lanjutkan salinan di lokasi di mana kegagalan terjadi.

Untuk informasi selengkapnya tentang melihat detail salinan acara jejak, lihatLihat detail salinan acara dengan CloudTrail konsol.

Salin peristiwa jejak ke penyimpanan data acara baru dengan konsol

Panduan ini menunjukkan kepada Anda cara menyalin peristiwa jejak ke penyimpanan data peristiwa CloudTrail Danau baru untuk analisis historis. Untuk informasi selengkapnya tentang menyalin peristiwa jejak, lihatSalin peristiwa jejak ke penyimpanan data peristiwa.

Untuk menyalin peristiwa jejak ke penyimpanan data acara baru

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Configure event data store, dalam Rincian umum, berikan nama penyimpanan data acara Anda, seperti*my-management-events-eds*. Sebagai praktik terbaik, gunakan nama yang dengan cepat mengidentifikasi tujuan penyimpanan data acara. Untuk informasi tentang persyaratan CloudTrail penamaan, lihatPersyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS.
5. Pilih opsi Harga yang ingin Anda gunakan untuk penyimpanan data acara Anda. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan acara, serta periode retensi default dan maksimum untuk penyimpanan data acara Anda. Untuk informasi lebih lanjut, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

   Berikut ini adalah opsi yang tersedia:

- One-year Harga retensi yang dapat diperpanjang - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data peristiwa per bulan dan menginginkan periode retensi yang fleksibel hingga 10 tahun. Untuk 366 hari pertama (periode retensi default), penyimpanan disertakan tanpa biaya tambahan dengan harga penyerapan. Setelah 366 hari, retensi yang diperpanjang tersedia dengan harga bayar sesuai pemakaian. Ini adalah pilihan default.
  - Periode retensi default: 366 hari
  - Periode retensi maksimum: 3,653 hari
- Seven-year harga retensi - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data peristiwa per bulan dan membutuhkan periode retensi hingga 7 tahun. Retensi disertakan dengan harga penyerapan tanpa biaya tambahan.
  - Periode retensi default: 2,557 hari
  - Periode retensi maksimum: 2.557 hari

6. Tentukan periode retensi untuk penyimpanan data acara. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi yang One-year dapat diperpanjang, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi. Seven-year

   CloudTrail Lake menentukan apakah akan mempertahankan suatu peristiwa dengan memeriksa apakah acara tersebut berada dalam periode retensi yang ditentukan. `eventTime` Misalnya, jika Anda menentukan periode retensi 90 hari, CloudTrail akan menghapus peristiwa ketika mereka `eventTime` lebih tua dari 90 hari.

   > **Note**
   >
   > CloudTrail tidak akan menyalin peristiwa jika `eventTime` lebih tua dari periode retensi yang ditentukan.
   > Untuk menentukan periode retensi yang sesuai, ambil jumlah acara tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.

7. (Opsional) Dalam Enkripsi. pilih apakah Anda ingin mengenkripsi penyimpanan data acara menggunakan kunci KMS Anda sendiri. Secara default, semua peristiwa di penyimpanan data

acara dienkripsi dengan CloudTrail menggunakan kunci KMS yang AWS memiliki dan mengelola untuk Anda.

Untuk mengaktifkan enkripsi menggunakan kunci KMS Anda sendiri, pilih Gunakan sendiri AWS KMS key. Pilih Baru untuk AWS KMS key membuat untuk Anda, atau pilih yang ada untuk menggunakan kunci KMS yang ada. Di Masukkan alias KMS, tentukan alias, dalam format. `alias/` *`MyAliasName`* Menggunakan kunci KMS Anda sendiri mengharuskan Anda mengedit kebijakan kunci KMS Anda untuk memungkinkan CloudTrail log dienkripsi dan didekripsi. Untuk informasi lebih lanjut, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

Menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

> **Note**
>
> Untuk mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data acara organisasi, Anda harus menggunakan kunci KMS yang ada untuk akun manajemen.

8. (Opsional) Jika Anda ingin melakukan kueri terhadap data peristiwa menggunakan Amazon Athena, pilih Aktifkan di federasi kueri Danau. Federation memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL terhadap data peristiwa di Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menyatukan penyimpanan data acara.

   Untuk mengaktifkan federasi kueri Lake, pilih Aktifkan dan lakukan hal berikut:

   a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data acara federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda memilih

peran yang ada, pastikan kebijakan untuk peran tersebut memberikan izin minimum yang diperlukan.

b. Jika Anda membuat peran baru, masukkan nama untuk mengidentifikasi peran tersebut.

c. Jika Anda menggunakan peran yang ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) Pilih Aktifkan kebijakan sumber daya untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Resource-based kebijakan memungkinkan Anda untuk mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Misalnya, Anda dapat menambahkan kebijakan berbasis sumber daya yang memungkinkan pengguna root di akun lain untuk menanyakan penyimpanan data peristiwa ini dan melihat hasil kueri. Untuk kebijakan-kebijakan contoh, lihat Resource-based contoh kebijakan untuk penyimpanan data acara.

   Kebijakan berbasis sumber daya mencakup satu atau lebih pernyataan. Setiap pernyataan dalam kebijakan mendefinisikan prinsipal yang diizinkan atau ditolak akses ke penyimpanan data peristiwa dan tindakan yang dapat dilakukan oleh prinsipal pada sumber daya penyimpanan data acara.

   Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   Untuk penyimpanan data peristiwa organisasi, CloudTrail buat kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data peristiwa organisasi. Izin dalam kebijakan ini berasal dari izin administrator yang didelegasikan di. AWS Organizations Kebijakan ini diperbarui secara

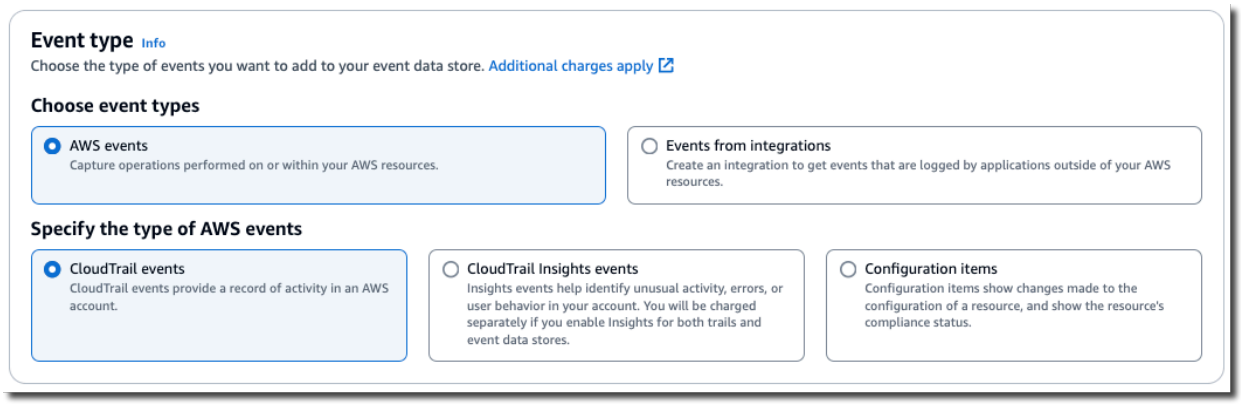
otomatis setelah perubahan pada penyimpanan data peristiwa organisasi atau organisasi (misalnya, akun administrator yang CloudTrail didelegasikan terdaftar atau dihapus).

10. (Opsional) Di Tag, tambahkan satu atau beberapa tag kustom (pasangan kunci-nilai) ke penyimpanan data acara Anda. Tag dapat membantu Anda mengidentifikasi penyimpanan data CloudTrail acara Anda. Misalnya, Anda bisa melampirkan tag dengan nama **`stage`** dan nilainya**`prod`**. Anda dapat menggunakan tag untuk membatasi akses ke penyimpanan data acara Anda. Anda juga dapat menggunakan tag untuk melacak kueri dan biaya konsumsi untuk penyimpanan data acara Anda.

    Untuk informasi tentang cara menggunakan tag untuk melacak biaya, lihatMembuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake. Untuk informasi tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Sumber AWS Daya Penandaan.

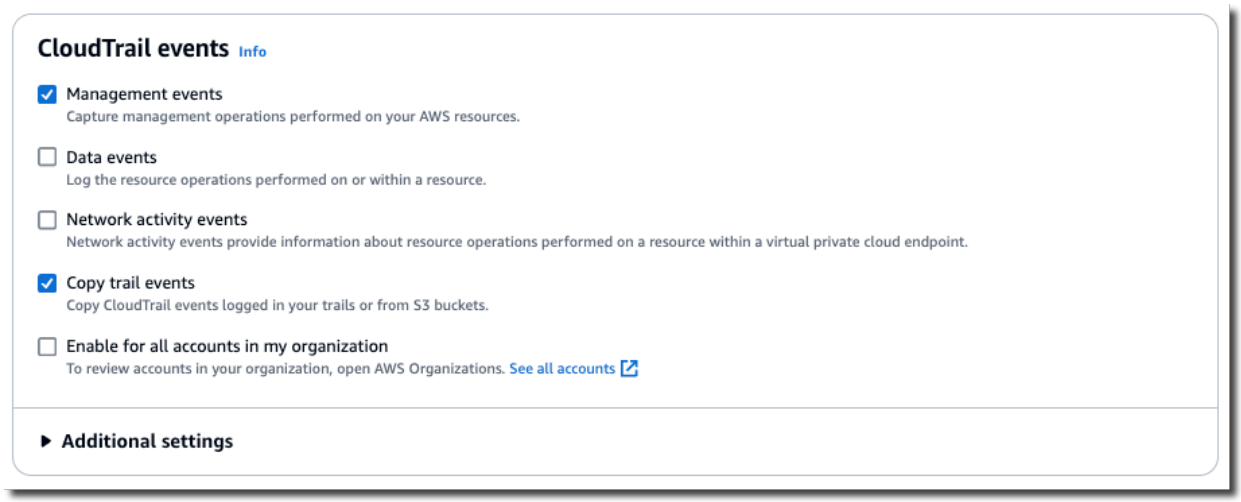
11. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.

12. Pada halaman Pilih acara, tinggalkan pilihan default untuk jenis Acara.



13. Untuk CloudTrail acara, kami akan membiarkan acara Manajemen dipilih dan memilih Salin acara jejak. Dalam contoh ini, kami tidak khawatir tentang jenis acara karena kami hanya menggunakan penyimpanan data peristiwa untuk menganalisis peristiwa masa lalu dan tidak menelan peristiwa masa depan.

    Jika Anda membuat penyimpanan data acara untuk menggantikan jejak yang ada, pilih pemilih acara yang sama dengan jejak Anda untuk memastikan penyimpanan data acara memiliki cakupan acara yang sama.



14. Pilih Aktifkan untuk semua akun di organisasi saya jika ini adalah penyimpanan data acara organisasi. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi AWS Organizations.

> **Note**
>
> Jika Anda membuat penyimpanan data acara organisasi, Anda harus masuk dengan akun manajemen untuk organisasi karena hanya akun manajemen yang dapat menyalin peristiwa jejak ke penyimpanan data acara organisasi.

15. Untuk pengaturan Tambahan, kami akan membatalkan pilihan acara Ingest, karena dalam contoh ini kami tidak ingin penyimpanan data acara menyerap peristiwa masa depan karena kami hanya tertarik untuk menanyakan peristiwa yang disalin. Secara default, penyimpanan data acara mengumpulkan peristiwa untuk semua Wilayah AWS dan mulai menelan peristiwa saat dibuat.
16. Untuk acara Manajemen, kami akan meninggalkan pengaturan default.
17. Di area Copy trail events, selesaikan langkah-langkah berikut.

    a. Pilih jejak yang ingin Anda salin. Dalam contoh ini, kita akan memilih jejak bernama*`management-events`*.

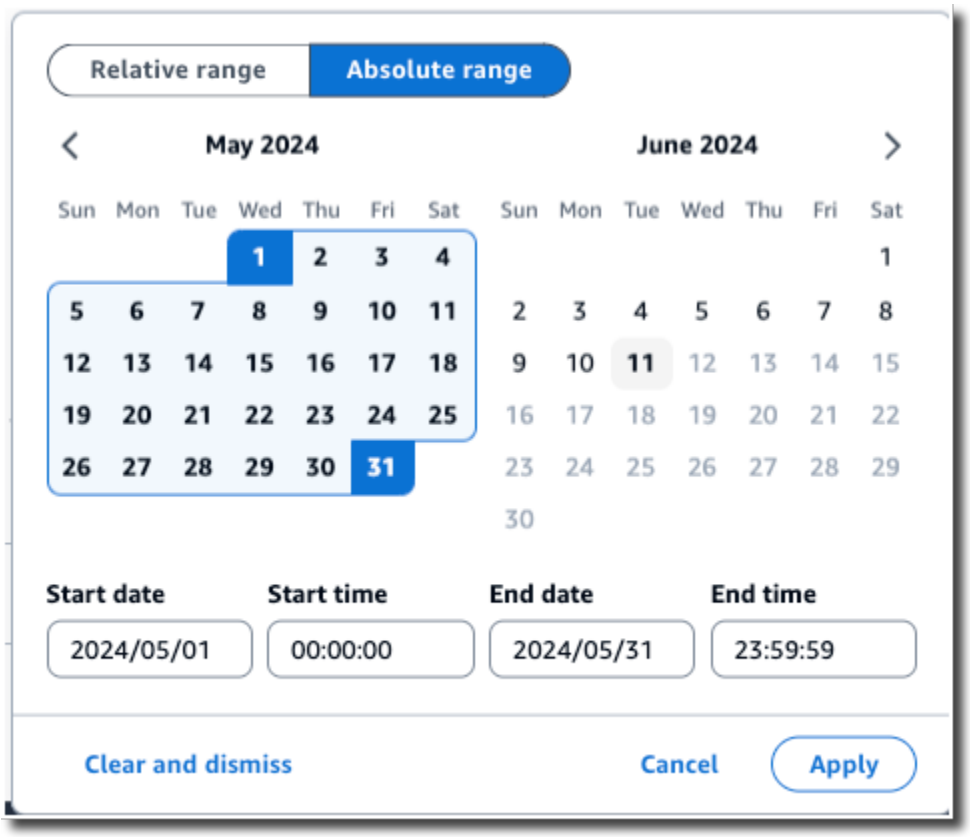
    Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam awalan bucket S3 dan `CloudTrail` awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, pilih Masukkan URI S3, lalu pilih Browse S3 untuk menelusuri awalan. Jika bucket S3 sumber untuk jejak menggunakan kunci KMS untuk

enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data. Jika bucket S3 sumber Anda menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci agar memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Untuk informasi selengkapnya tentang memperbarui kebijakan kunci KMS, lihatKebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber.

b. Pilih rentang waktu untuk menyalin acara. CloudTrail memeriksa awalan dan nama file log untuk memverifikasi nama berisi tanggal antara tanggal mulai dan akhir yang dipilih sebelum mencoba menyalin peristiwa jejak. Anda dapat memilih rentang Relatif atau rentang Absolut. Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang waktu yang lebih awal dari pembuatan penyimpanan data acara.

   - Jika Anda memilih Rentang relatif, Anda dapat memilih untuk menyalin peristiwa yang dicatat dalam 6 bulan terakhir, 1 tahun, 2 tahun, 7 tahun, atau rentang khusus. CloudTrail menyalin peristiwa yang dicatat dalam periode waktu yang dipilih.
   - Jika Anda memilih Rentang absolut, Anda dapat memilih tanggal mulai dan berakhir tertentu. CloudTrail menyalin peristiwa yang terjadi antara tanggal mulai dan akhir yang dipilih.

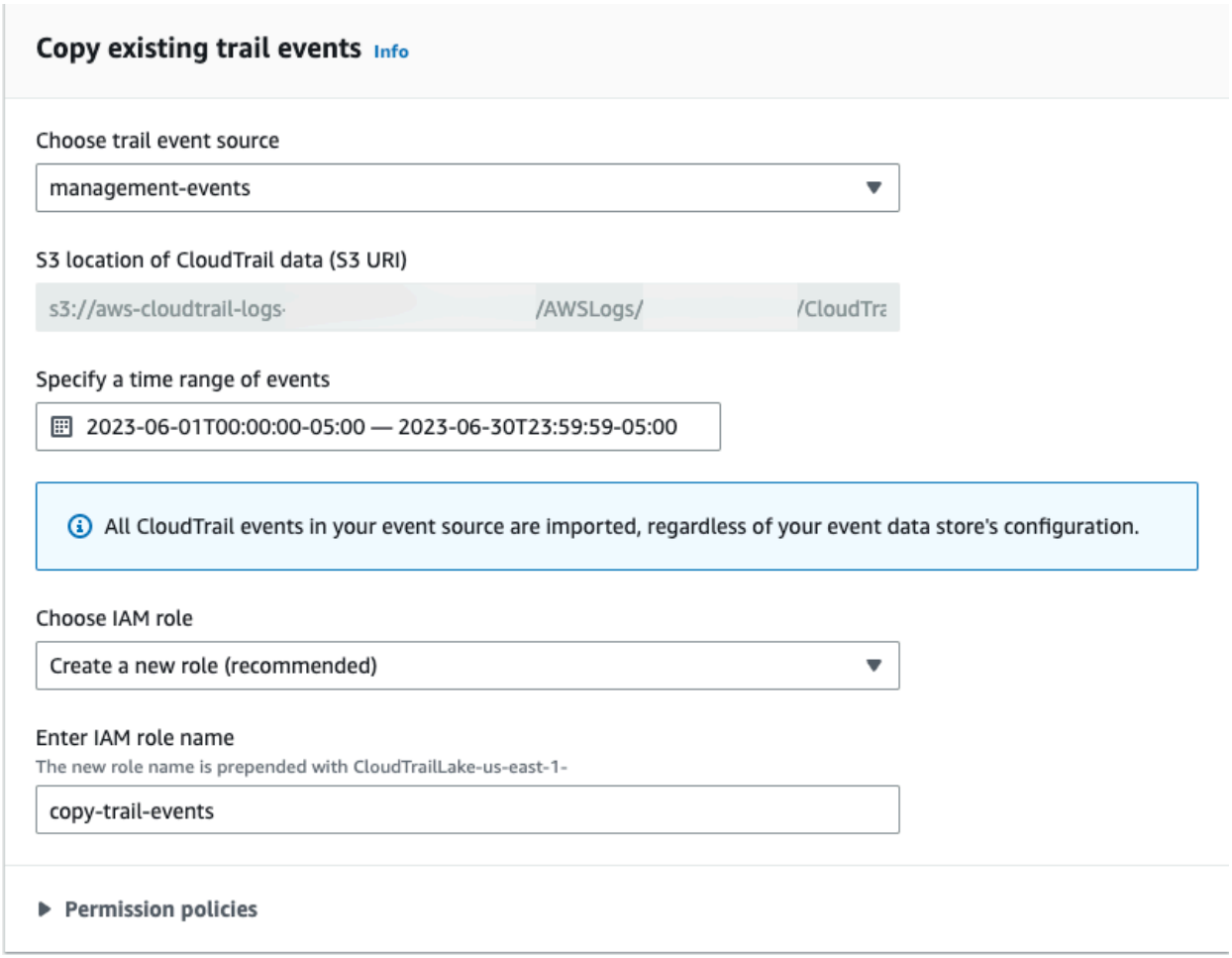
   Dalam contoh ini, kita akan memilih rentang Absolute dan kita akan memilih seluruh bulan Mei.



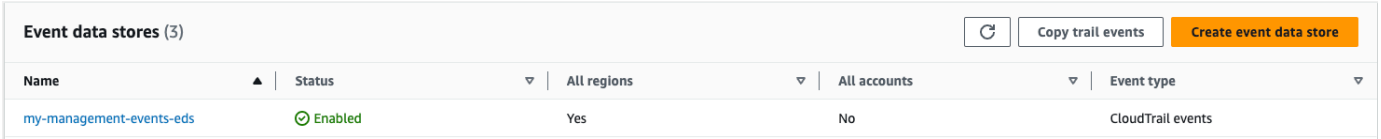
c. Untuk Izin, pilih dari opsi peran IAM berikut. Jika Anda memilih peran IAM yang ada, verifikasi bahwa kebijakan peran IAM menyediakan izin yang diperlukan. Untuk informasi selengkapnya tentang memperbarui izin peran IAM, lihat. Izin IAM untuk menyalin peristiwa jejak

   - Pilih Buat peran baru (disarankan) untuk membuat peran IAM baru. Untuk Masukkan nama peran IAM, masukkan nama untuk peran tersebut. CloudTrail secara otomatis membuat izin yang diperlukan untuk peran baru ini.
   - Pilih Gunakan ARN peran IAM kustom untuk menggunakan peran IAM kustom yang tidak terdaftar. Untuk Masukkan peran IAM ARN, masukkan ARN IAM.
   - Pilih peran IAM yang ada dari daftar drop-down.

   Dalam contoh ini, kita akan memilih Buat peran baru (disarankan) dan akan memberikan nama**`copy-trail-events`**.



18. Pilih Berikutnya untuk meninjau pilihan Anda.
19. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada suatu bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
20. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.

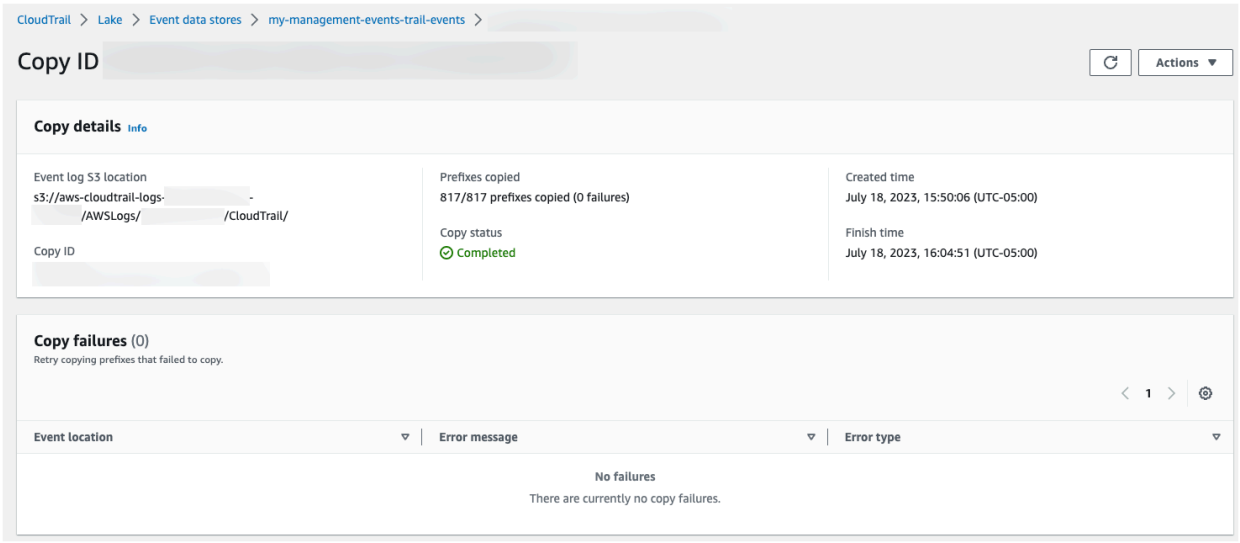


21. Pilih nama penyimpanan data acara untuk melihat halaman detailnya. Halaman detail menunjukkan detail untuk penyimpanan data acara Anda dan status salinannya. Status penyalinan peristiwa ditampilkan di area status salinan Acara.

Ketika salinan peristiwa jejak selesai, status Salinannya disetel ke Selesai jika tidak ada kesalahan, atau Gagal jika terjadi kesalahan.



22. Untuk melihat detail lebih lanjut tentang salinan, pilih nama salin di kolom Lokasi S3 log peristiwa, atau pilih opsi Lihat detail dari menu Tindakan. Untuk informasi selengkapnya tentang melihat detail salinan acara jejak, lihatLihat detail salinan acara dengan CloudTrail konsol.



23. Area kegagalan Salin menunjukkan kesalahan apa pun yang terjadi saat menyalin peristiwa jejak. Jika status Salin Gagal, perbaiki kesalahan yang ditampilkan dalam kegagalan Salin, lalu pilih Coba lagi salin. Ketika Anda mencoba kembali salinan, CloudTrail lanjutkan salinan di lokasi di mana kegagalan terjadi.

Lihat detail salinan acara dengan CloudTrail konsol

Setelah salinan peristiwa jejak dimulai, Anda dapat melihat detail salinan acara, termasuk status salinan, dan informasi tentang kegagalan salinan apa pun.

> **Note**
>
> Detail yang ditampilkan di halaman detail salinan acara tidak dalam waktu nyata. Nilai sebenarnya untuk detail seperti Awalan yang disalin mungkin lebih tinggi dari yang

ditampilkan di halaman. CloudTrail memperbarui detail secara bertahap selama salinan acara.

Untuk mengakses halaman detail salinan acara

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi kiri, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara.
4. Pilih salinan acara di bagian Status salinan acara.

Salin detail

Dari detail Salin, Anda dapat melihat detail berikut tentang salinan acara jejak.

- Lokasi log peristiwa S3 - Lokasi bucket S3 sumber yang berisi file log peristiwa jejak.
- Copy ID - ID untuk salinan.
- Awalan disalin - Merupakan jumlah awalan S3 yang disalin. Selama salinan peristiwa jejak, CloudTrail menyalin peristiwa dalam file log jejak yang disimpan dalam awalan.
- Status salinan - Status salinan.
  - Inisialisasi - Status awal ditampilkan saat salinan acara jejak dimulai.
  - Sedang berlangsung - Menunjukkan salinan acara jejak sedang berlangsung.

    > **Note**
    >
    > Anda tidak dapat menyalin peristiwa jejak jika salinan acara jejak lainnya sedang berlangsung. Untuk menghentikan salinan acara jejak, pilih Hentikan salinan.

  - Berhenti - Menunjukkan tindakan Stop copy terjadi. Untuk mencoba kembali salinan acara jejak, pilih Coba lagi salin.
  - Gagal - Salinan selesai, tetapi beberapa peristiwa jejak gagal disalin. Tinjau pesan kesalahan dalam kegagalan Salin. Untuk mencoba kembali salinan acara jejak, pilih Coba lagi salin. Saat Anda mencoba kembali salinan, CloudTrail lanjutkan salinan di lokasi di mana kegagalan terjadi.
  - Selesai - Salinan selesai tanpa kesalahan. Anda dapat menanyakan peristiwa jejak yang disalin di penyimpanan data acara.

- Waktu yang dibuat - Menunjukkan kapan salinan acara jejak dimulai.
- Waktu selesai - Menunjukkan kapan salinan acara jejak selesai atau dihentikan.

Kegagalan penyalinan

Dari kegagalan Salin, Anda dapat meninjau lokasi kesalahan, pesan kesalahan, dan jenis kesalahan untuk setiap kegagalan salinan. Alasan umum kegagalan, termasuk jika awalan S3 berisi file yang tidak dikompresi, atau berisi file yang dikirimkan oleh layanan selain. CloudTrail Kemungkinan penyebab kegagalan lainnya terkait dengan masalah akses. Misalnya, jika bucket S3 penyimpanan data peristiwa tidak memberikan CloudTrail akses untuk mengimpor peristiwa, Anda akan mendapatkan `AccessDenied` kesalahan.

Untuk setiap kegagalan salinan, tinjau informasi kesalahan berikut.

- Lokasi Kesalahan - Menunjukkan lokasi di bucket S3 tempat kesalahan terjadi. Jika terjadi kesalahan karena bucket S3 sumber berisi file yang tidak terkompresi, lokasi Error akan menyertakan awalan di mana Anda akan menemukan file itu.
- Pesan Kesalahan - Memberikan penjelasan mengapa kesalahan terjadi.
- Jenis kesalahan - Menyediakan jenis kesalahan. Misalnya, jenis Kesalahan`AccessDenied`, menunjukkan bahwa kesalahan terjadi karena masalah izin. Untuk informasi selengkapnya tentang izin yang diperlukan untuk menyalin peristiwa jejak, lihat. Izin yang diperlukan untuk menyalin peristiwa jejak

Setelah menyelesaikan kegagalan, pilih Coba lagi salin. Saat Anda mencoba kembali salinan, CloudTrail lanjutkan salinan di lokasi di mana kegagalan terjadi.

Menyatukan penyimpanan data acara

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Menggabungkan penyimpanan data peristiwa memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data, mendaftarkan Katalog Data dengan AWS Lake Formation, dan memungkinkan Anda menjalankan kueri SQL terhadap data acara menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri.

Anda dapat mengaktifkan federasi dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi EnableFederation API. Saat Anda mengaktifkan federasi kueri CloudTrail Lake, membuat database ter `aws:cloudtrail` kelola bernama (jika database belum ada) dan tabel federasi terkelola di Katalog AWS Glue Data. ID penyimpanan data peristiwa digunakan untuk nama tabel. CloudTrail mendaftarkan peran federasi ARN dan penyimpanan data peristiwa AWS Lake Formation, layanan yang bertanggung jawab untuk memungkinkan kontrol akses berbutir halus dari sumber daya federasi dalam Katalog Data. AWS Glue

Untuk mengaktifkan federasi kueri Lake, Anda harus membuat peran IAM baru atau memilih peran yang sudah ada. Lake Formation menggunakan peran ini untuk mengelola izin untuk penyimpanan data peristiwa federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat izin yang diperlukan untuk peran tersebut. Jika Anda memilih peran yang ada, pastikan peran tersebut memberikan izin minimum.

Anda dapat menonaktifkan federasi dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi DisableFederation API. Saat Anda menonaktifkan federasi, CloudTrail menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Lake, Anda tidak dapat lagi menanyakan data acara Anda di Athena. Tidak ada data CloudTrail Lake yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Lake.

Tidak ada CloudTrail biaya untuk menggabungkan penyimpanan data acara CloudTrail Lake. Ada biaya untuk menjalankan kueri di Amazon Athena. Untuk informasi selengkapnya tentang harga Athena, lihat Harga Amazon Athena.

Analisis Log Aktivitas dengan AWS CloudTrail Danau dan Amazon Athena

Topik

- Pertimbangan-pertimbangan
- Izin yang diperlukan untuk federasi
- Aktifkan federasi kueri Danau

- Nonaktifkan federasi kueri Danau
- Mengelola sumber daya federasi CloudTrail Danau dengan AWS Lake Formation

Pertimbangan-pertimbangan

Pertimbangkan faktor-faktor berikut saat menggabungkan penyimpanan data peristiwa:

- Tidak ada CloudTrail biaya untuk menggabungkan penyimpanan data acara CloudTrail Lake. Ada biaya untuk menjalankan kueri di Amazon Athena. Untuk informasi selengkapnya tentang harga Athena, lihat Harga Amazon Athena.
- Formasi Danau digunakan untuk mengelola izin untuk sumber daya federasi. Jika Anda menghapus peran federasi, atau mencabut izin ke sumber daya dari Lake Formation atau AWS Glue, Anda tidak dapat menjalankan kueri dari Athena. Untuk informasi lebih lanjut tentang bekerja dengan Formasi Danau, lihatMengelola sumber daya federasi CloudTrail Danau dengan AWS Lake Formation.
- Siapa pun yang menggunakan Amazon Athena untuk menanyakan data yang terdaftar di Lake Formation harus memiliki kebijakan izin IAM yang memungkinkan tindakan tersebut`lakeformation:GetDataAccess`. Kebijakan AWS terkelola: AmazonAthenaFullAccess memungkinkan tindakan ini. Jika Anda menggunakan kebijakan inline, pastikan untuk memperbarui kebijakan izin untuk mengizinkan tindakan ini. Untuk informasi selengkapnya, lihat M engelola Formasi Danau dan izin pengguna Athena.
- Untuk membuat tampilan pada tabel federasi di Athena, Anda memerlukan database tujuan selain. `aws:cloudtrail` Ini karena `aws:cloudtrail` database dikelola oleh CloudTrail.
- Untuk membuat dataset di Amazon Quick, Anda harus memilih opsi Gunakan SQL khusus. Untuk informasi selengkapnya, lihat Membuat dataset menggunakan data Amazon Athena.
- Jika federasi diaktifkan, Anda tidak dapat menghapus penyimpanan data peristiwa. Untuk menghapus penyimpanan data peristiwa federasi, Anda harus menonaktifkan federasi dan perlindungan penghentian terlebih dahulu jika diaktifkan.
- Pertimbangan berikut berlaku untuk penyimpanan data acara organisasi:
  - Hanya satu akun administrator yang didelegasikan atau akun manajemen yang dapat mengaktifkan federasi pada penyimpanan data acara organisasi. Akun administrator yang didelegasikan lainnya masih dapat menanyakan dan berbagi informasi menggunakan fitur berbagi data Lake Formation.
  - Setiap akun administrator yang didelegasikan atau akun manajemen organisasi dapat menonaktifkan federasi.

Izin yang diperlukan untuk federasi

Sebelum menggabungkan penyimpanan data peristiwa, pastikan Anda memiliki semua izin yang diperlukan untuk peran federasi dan untuk mengaktifkan dan menonaktifkan federasi. Anda hanya perlu memperbarui izin peran federasi jika Anda memilih peran IAM yang ada untuk mengaktifkan federasi. Jika Anda memilih untuk membuat peran IAM baru menggunakan CloudTrail konsol, CloudTrail berikan semua izin yang diperlukan untuk peran tersebut.

Topik

- Izin IAM untuk menyatukan penyimpanan data acara
- Izin yang diperlukan untuk mengaktifkan federasi
- Izin yang diperlukan untuk menonaktifkan federasi

Izin IAM untuk menyatukan penyimpanan data acara

Saat Anda mengaktifkan federasi, Anda memiliki opsi untuk membuat peran IAM baru, atau menggunakan peran IAM yang ada. Saat Anda memilih peran IAM baru, buat peran CloudTrail IAM dengan izin yang diperlukan dan tidak ada tindakan lebih lanjut yang diperlukan dari pihak Anda.

Jika Anda memilih peran yang ada, pastikan kebijakan peran IAM memberikan izin yang diperlukan untuk mengaktifkan federasi. Bagian ini memberikan contoh kebijakan izin dan kepercayaan peran IAM yang diperlukan.

Contoh berikut menyediakan kebijakan izin untuk peran federasi. Untuk pernyataan pertama, berikan ARN lengkap penyimpanan data acara Anda untuk`Resource`.

Pernyataan kedua dalam kebijakan ini memungkinkan Lake Formation mendekripsi data untuk penyimpanan data peristiwa yang dienkripsi dengan kunci KMS. G *`key-region`* anti*`account-id`*,, dan *`key-id`* dengan nilai untuk kunci KMS Anda. Anda dapat menghilangkan pernyataan ini jika penyimpanan data peristiwa Anda tidak menggunakan kunci KMS untuk enkripsi.

JSON

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

```
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "LakeFederationKMSDecryptAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id"
        }
    ]
}
```

Contoh berikut menyediakan kebijakan kepercayaan IAM, yang memungkinkan AWS Lake Formation untuk mengambil peran IAM untuk mengelola izin untuk penyimpanan data peristiwa federasi.

JSON

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

Izin yang diperlukan untuk mengaktifkan federasi

Kebijakan contoh berikut menyediakan izin minimum yang diperlukan untuk mengaktifkan federasi pada penyimpanan data peristiwa. Kebijakan ini memungkinkan CloudTrail untuk mengaktifkan

federasi pada penyimpanan data peristiwa, AWS Glue untuk membuat sumber daya federasi di Katalog AWS Glue Data, dan AWS Lake Formation untuk mengelola pendaftaran sumber daya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailEnableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "FederationRoleAccess",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/federation-role-name"
        },
        {
            "Sid": "GlueResourceCreation",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-
id",
                "arn:aws:glue:us-east-1:111111111111:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "LakeFormationRegistration",
            "Effect": "Allow",
```

```
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource":
 "arn:aws:lakeformation:region:111111111111:catalog:111111111111"
        }
    ]
}
```

Izin yang diperlukan untuk menonaktifkan federasi

Kebijakan contoh berikut menyediakan sumber daya minimum yang diperlukan untuk menonaktifkan federasi pada penyimpanan data peristiwa. Kebijakan ini memungkinkan CloudTrail untuk menonaktifkan federasi pada penyimpanan data peristiwa, AWS Glue untuk menghapus tabel federasi terkelola di Katalog AWS Glue Data, dan Lake Formation untuk membatalkan pendaftaran sumber daya federasi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailDisableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "GlueTableDeletion",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-id"
            ]
        },
        {
```

```
            "Sid": "LakeFormationDeregistration",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:us-
east-1:111111111111:catalog:111111111111"
        }
    ]
}
```

Aktifkan federasi kueri Danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat mengaktifkan federasi kueri Lake dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi EnableFederation API. Saat Anda mengaktifkan federasi kueri CloudTrail Lake, membuat database ter `aws:cloudtrail` kelola bernama (jika database belum ada) dan tabel federasi terkelola di Katalog AWS Glue Data. ID penyimpanan data peristiwa digunakan untuk nama tabel. CloudTrail mendaftarkan peran federasi ARN dan penyimpanan data peristiwa AWS Lake Formation, layanan yang bertanggung jawab untuk memungkinkan kontrol akses berbutir halus dari sumber daya federasi dalam Katalog Data. AWS Glue

Bagian ini menjelaskan cara mengaktifkan federasi menggunakan CloudTrail konsol dan AWS CLI.

CloudTrail console

Prosedur berikut menunjukkan cara mengaktifkan federasi kueri Lake pada penyimpanan data peristiwa yang ada.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara yang ingin Anda perbarui. Ini membuka halaman detail penyimpanan data acara.

4. Di federasi kueri Lake, pilih Edit dan kemudian pilih Aktifkan.
5. Pilih apakah akan membuat peran IAM baru, atau menggunakan peran yang sudah ada. Saat Anda membuat peran baru, CloudTrail secara otomatis membuat peran dengan izin yang diperlukan. Jika Anda menggunakan peran yang sudah ada, pastikan kebijakan peran tersebut memberikan izin minimum yang diperlukan.
6. Jika Anda membuat peran IAM baru, masukkan nama untuk peran tersebut.
7. Jika Anda memilih peran IAM yang sudah ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.
8. Pilih Simpan perubahan. Status Federasi berubah menjadi`Enabled`.

AWS CLI

Untuk mengaktifkan federasi, jalankan aws cloudtrail enable-federation perintah, menyediakan --role parameter --event-data-store dan yang diperlukan. Untuk--event-data-store, berikan penyimpanan data peristiwa ARN (atau akhiran ID ARN). Untuk--role, berikan ARN untuk peran federasi Anda. Peran harus ada di akun Anda dan memberikan izin minimum yang diperlukan.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

Contoh ini menunjukkan bagaimana administrator yang didelegasikan dapat mengaktifkan federasi pada penyimpanan data peristiwa organisasi dengan menentukan ARN penyimpanan data peristiwa di akun manajemen dan ARN peran federasi di akun administrator yang didelegasikan.

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Nonaktifkan federasi kueri Danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan

yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat menonaktifkan federasi dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi DisableFederation API. Saat Anda menonaktifkan federasi, CloudTrail menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Lake, Anda tidak dapat lagi menanyakan data acara Anda di Athena. Tidak ada data CloudTrail Lake yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Lake.

Bagian ini menjelaskan cara menonaktifkan federasi menggunakan CloudTrail konsol dan AWS CLI.

CloudTrail console

Prosedur berikut menunjukkan cara menonaktifkan federasi kueri Lake pada penyimpanan data peristiwa yang ada.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Lake, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara yang ingin Anda perbarui. Ini membuka halaman detail penyimpanan data acara.
4. Di federasi kueri Lake, pilih Edit dan kemudian pilih Nonaktifkan.
5. Pilih Simpan perubahan. Status Federasi berubah menjadi`Disabled`.

AWS CLI

Untuk menonaktifkan federasi pada penyimpanan data acara, jalankan aws cloudtrail disable-federation perintah. Penyimpanan data peristiwa ditentukan oleh`--event-data-store`, yang menerima penyimpanan data peristiwa ARN atau akhiran ID ARN.

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> Jika ini adalah penyimpanan data peristiwa organisasi, gunakan ID akun untuk akun manajemen.

Mengelola sumber daya federasi CloudTrail Danau dengan AWS Lake Formation

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal itu. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Saat Anda menyatukan penyimpanan data peristiwa, men CloudTrail daftarkan peran federasi ARN dan penyimpanan data peristiwa di AWS Lake Formation, layanan yang bertanggung jawab untuk mengizinkan kontrol akses halus dari sumber daya federasi dalam Katalog Data. AWS Glue Bagian ini menjelaskan bagaimana Anda dapat menggunakan Formasi Danau untuk mengelola sumber daya federasi CloudTrail Danau.

Saat Anda mengaktifkan federasi CloudTrail , membuat sumber daya berikut di Katalog AWS Glue Data.

- Database terkel CloudTrail ola - membuat 1 database dengan nama `aws:cloudtrail` per akun. CloudTrail mengelola database. Anda tidak dapat menghapus atau memodifikasi database di AWS Glue.
- Tabel federasi ter kel CloudTrail ola - membuat 1 tabel untuk setiap penyimpanan data peristiwa federasi dan menggunakan ID penyimpanan data peristiwa untuk nama tabel. CloudTrail mengelola tabel. Anda tidak dapat menghapus atau memodifikasi tabel di AWS Glue. Untuk menghapus tabel, Anda harus menonaktifkan federasi pada penyimpanan data acara.

Mengontrol akses ke sumber daya federasi

Anda dapat menggunakan salah satu dari dua metode izin untuk mengontrol akses ke database dan tabel yang dikelola.

- Kontrol akses khusus IAM — Dengan kontrol akses khusus IAM, semua pengguna di akun dengan izin IAM yang diperlukan diberikan akses ke semua sumber daya Katalog Data. Untuk informasi tentang cara AWS Glue bekerja dengan IAM, lihat Cara AWS Glue bekerja dengan I AM.

  Pada konsol Lake Formation, metode ini muncul sebagai Gunakan hanya kontrol akses IAM.

  > **Note**
  >
  > Jika Anda ingin membuat filter data dan menggunakan fitur Formasi Danau lainnya, Anda harus menggunakan kontrol akses Formasi Danau.

- Kontrol akses Formasi Danau — Metode ini memberikan keuntungan sebagai berikut.
  - Anda dapat menerapkan keamanan tingkat kolom, tingkat baris, dan tingkat sel dengan membuat filter data. https://docs.aws.amazon.com/lake-formation/latest/dg/data-filters-about.html Untuk informasi selengkapnya, lihat Mengamankan data lake dengan kontrol akses tingkat baris di Panduan Peng AWS Lake Formation embang.
  - Basis data dan tabel hanya terlihat oleh administrator Danau Formation dan pembuat database dan sumber daya. Jika pengguna lain memerlukan akses ke sumber daya ini, Anda harus secara eksplisit memberikan akses dengan menggunakan izin Lake Formation.

Untuk informasi selengkapnya tentang kontrol akses, lihat Metode untuk kontrol akses halus.

Menentukan metode izin untuk sumber daya federasi

Saat Anda mengaktifkan federasi untuk pertama kalinya, membuat database CloudTrail terkelola dan tabel federasi terkelola menggunakan pengaturan danau data Lake Formation Anda.

Setelah CloudTrail mengaktifkan federasi, Anda dapat memverifikasi metode izin mana yang Anda gunakan untuk database terkelola dan tabel federasi terkelola dengan memeriksa izin untuk sumber daya tersebut. Jika `IAM_ALLOWED_PRINCIPALS` pengaturan `ALL` (Super) to ada untuk sumber daya, sumber daya dikelola secara eksklusif oleh izin IAM. Jika pengaturan hilang, sumber daya dikelola oleh izin Formasi Danau. Untuk informasi lebih lanjut tentang izin Formasi Danau, lihat referensi izin Formasi Danau.

Metode izin untuk database terkelola dan tabel federasi terkelola dapat berbeda. Misalnya, jika Anda memeriksa nilai untuk database dan tabel, Anda dapat melihat yang berikut ini:

- Untuk database, nilai yang ditetapkan `ALL` (Super) `IAM_ALLOWED_PRINCIPALS` hadir dalam izin yang menunjukkan bahwa Anda menggunakan kontrol akses hanya IAM untuk database.

- Untuk tabel, nilai yang menetapkan `ALL` (Super) untuk `IAM_ALLOWED_PRINCIPALS` tidak hadir, yang menunjukkan kontrol akses dengan izin Formasi Danau.

Anda dapat beralih di antara metode akses kapan saja dengan menambahkan atau menghapus `ALL` (Super) ke `IAM_ALLOWED_PRINCIPALS` izin pada sumber daya federasi apa pun di Lake Formation.

Cross-account berbagi menggunakan Lake Formation

Bagian ini menjelaskan cara berbagi database terkelola dan tabel federasi terkelola di seluruh akun dengan menggunakan Formasi Danau.

Anda dapat berbagi database terkelola di seluruh akun dengan mengambil langkah-langkah berikut:

1. Perbarui versi berbagi data lintas akun ke versi 4.
2. Hapus `Super` ke `IAM_ALLOWED_PRINCIPALS` izin dari database jika ada untuk beralih ke kontrol akses Formasi Danau.
3. Ber `Describe` ikan izin ke akun eksternal di database.
4. Jika sumber daya Katalog Data dibagikan dengan akun Anda Akun AWS dan akun Anda tidak berada di AWS organisasi yang sama dengan akun berbagi, terima undangan berbagi sumber daya dari AWS Resource Access Manager (AWS RAM). Untuk informasi selengkapnya, lihat Menerima undangan berbagi sumber daya dari AWS RAM.

Setelah menyelesaikan langkah-langkah ini, database harus terlihat oleh akun eksternal. Secara default, berbagi database tidak memberikan akses ke tabel apa pun dalam database.

Anda dapat berbagi semua atau masing-masing tabel federasi terkelola dengan akun eksternal dengan melakukan langkah-langkah berikut:

1. Perbarui versi berbagi data lintas akun ke versi 4.
2. Hapus `Super` ke `IAM_ALLOWED_PRINCIPALS` izin dari tabel jika ada untuk beralih ke kontrol akses Formasi Danau.
3. (Opsional) Tentukan filter data apa pun untuk membatasi kolom atau baris.
4. Ber `Select` ikan izin ke akun eksternal di atas meja.
5. Jika sumber daya Katalog Data dibagikan dengan akun Anda Akun AWS dan akun Anda tidak berada di AWS organisasi yang sama dengan akun berbagi, terima undangan berbagi

sumber daya dari AWS Resource Access Manager (AWS RAM). Untuk organisasi, Anda dapat menerima secara otomatis menggunakan pengaturan RAM. Untuk informasi selengkapnya, lihat Menerima undangan berbagi sumber daya dari AWS RAM.

6. Tabel sekarang harus terlihat. Untuk mengaktifkan kueri Amazon Athena pada tabel ini, buat tautan sumber daya di akun ini dengan tabel bersama.

Akun pemilik dapat mencabut berbagi kapan saja dengan menghapus izin untuk akun eksternal dari Lake Formation, atau dengan menonaktifkan federasi di CloudTrail.

Memahami penyimpanan data acara organisasi

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Jika Anda telah membuat organisasi di AWS Organizations, Anda dapat membuat penyimpanan data acara organisasi yang mencatat semua peristiwa untuk semua Akun AWS di organisasi tersebut. Penyimpanan data acara organisasi dapat berlaku untuk semua Wilayah AWS, atau Wilayah saat ini. Anda tidak dapat menggunakan penyimpanan data acara organisasi untuk mengumpulkan acara dari luar AWS.

Anda dapat membuat penyimpanan data acara organisasi dengan menggunakan akun manajemen atau akun administrator yang didelegasikan. Ketika administrator yang didelegasikan membuat penyimpanan data peristiwa organisasi, penyimpanan data peristiwa organisasi ada di akun manajemen untuk organisasi. Pendekatan ini karena akun manajemen mempertahankan kepemilikan semua sumber daya organisasi.

Akun manajemen untuk organisasi dapat memperbarui penyimpanan data peristiwa tingkat akun untuk menerapkannya ke organisasi.

Ketika penyimpanan data acara organisasi ditetapkan sebagai berlaku untuk organisasi, itu secara otomatis diterapkan ke semua akun anggota di organisasi. Akun anggota tidak dapat melihat penyimpanan data acara organisasi, juga tidak dapat memodifikasi atau menghapusnya. Secara

default, akun anggota tidak memiliki akses ke penyimpanan data acara organisasi, juga tidak dapat menjalankan kueri pada penyimpanan data acara organisasi.

Tabel berikut menunjukkan kemampuan akun manajemen dan akun administrator yang didelegasikan dalam AWS Organizations organisasi.

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan
Daftarkan atau hapus akun administrator yang didelegasikan.	Ya	Tidak
Buat penyimpanan data acara organisasi untuk AWS CloudTrail acara atau item AWS Config konfigurasi.	Ya	Ya
Aktifkan Wawasan tentang penyimpanan data acara organisasi.	Ya	Tidak
Perbarui penyimpanan data acara organisasi.	Ya	Ya [1]
Mulai dan hentikan konsumsi acara di penyimpanan data acara organisasi.	Ya	Ya
Aktifkan federasi kueri Danau di penyimpanan data acara organisasi. [2]	Ya	Ya
Nonaktifkan federasi kueri Danau di penyimpan an data acara organisasi.	Ya	Ya
Hapus penyimpanan data acara organisasi.	Ya	Ya
Salin peristiwa jejak ke penyimpanan data acara.	Ya	Tidak
Jalankan kueri pada penyimpanan data acara organisasi.	Ya	Ya
Melihat dasbor terkelola untuk penyimpanan data acara organisasi.	Ya	Tidak

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan
Aktifkan dasbor Sorotan untuk penyimpanan data acara organisasi.	Ya	Tidak
Buat widget untuk dasbor kustom yang menanyakan penyimpanan data acara organisasi.	Ya	Tidak

[1] Hanya akun manajemen yang dapat mengonversi penyimpanan data acara organisasi ke penyimpanan data peristiwa tingkat akun, atau mengonversi penyimpanan data peristiwa tingkat akun ke penyimpanan data acara organisasi. Tindakan ini tidak diizinkan untuk administrator yang didelegasikan karena penyimpanan data acara organisasi hanya ada di akun manajemen. Ketika penyimpanan data acara organisasi dikonversi ke penyimpanan data peristiwa tingkat akun, hanya akun manajemen yang memiliki akses ke penyimpanan data acara. Demikian juga, hanya penyimpanan data peristiwa tingkat akun di akun manajemen yang dapat dikonversi ke penyimpanan data acara organisasi.

[2] Hanya satu akun administrator yang didelegasikan atau akun manajemen yang dapat mengaktifkan federasi pada penyimpanan data acara organisasi. Akun administrator lain yang didelegasikan dapat menanyakan dan berbagi informasi menggunakan fitur berbagi data Lake Formation. Setiap akun administrator yang didelegasikan serta akun manajemen organisasi dapat menonaktifkan federasi.

Membuat penyimpanan data acara organisasi

Akun manajemen atau akun administrator yang didelegasikan untuk organisasi dapat membuat penyimpanan data acara organisasi untuk mengumpulkan CloudTrail peristiwa (peristiwa manajemen, peristiwa data) atau item AWS Config konfigurasi.

> **Note**
>
> Hanya akun manajemen organisasi yang dapat menyalin peristiwa jejak ke penyimpanan data acara.

CloudTrail console

Untuk membuat penyimpanan data acara organisasi menggunakan konsol

1. Ikuti langkah-langkah dalam membuat penyimpanan data acara untuk prosedur CloudTrail acara untuk membuat penyimpanan data acara organisasi untuk CloudTrail manajemen atau peristiwa data.

   ATAU

   Ikuti langkah-langkah dalam membuat penyimpanan data peristiwa untuk prosedur item AWS Config konfigurasi untuk membuat penyimpanan data acara organisasi untuk item AWS Config konfigurasi.
2. Pada halaman Pilih acara, pilih Aktifkan untuk semua akun di organisasi saya.

AWS CLI

Untuk membuat penyimpanan data acara organisasi, jalankan create-event-data-storeperintah dan sertakan `--organization-enabled` opsi.

AWS CLI `create-event-data-store`Perintah contoh berikut membuat penyimpanan data acara organisasi yang mengumpulkan semua peristiwa manajemen. Karena peristiwa manajemen CloudTrail log secara default, Anda tidak perlu menentukan pemilih peristiwa lanjutan jika penyimpanan data acara Anda mencatat semua peristiwa manajemen dan tidak mengumpulkan peristiwa data apa pun.

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
```

```
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

AWS CLI `create-event-data-store`Perintah contoh berikutnya membuat penyimpanan data acara organisasi bernama `config-items-org-eds` yang mengumpulkan item AWS Config konfigurasi. Untuk mengumpulkan item konfigurasi, tentukan bahwa `eventCategory` `ConfigurationItem` bidang sama dengan pemilih acara lanjutan.

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

Menerapkan penyimpanan data peristiwa tingkat akun ke organisasi

Akun manajemen organisasi dapat mengonversi penyimpanan data peristiwa tingkat akun untuk menerapkannya ke organisasi.

CloudTrail console

Untuk memperbarui penyimpanan data peristiwa tingkat akun menggunakan konsol

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih penyimpanan data acara yang ingin Anda perbarui. Tindakan ini membuka halaman detail toko data acara.
4. Dalam Detail umum, pilih Edit.
5. Pilih Aktifkan untuk semua akun di organisasi saya.
6. Pilih Simpan perubahan.

Untuk informasi tambahan tentang memperbarui penyimpanan data acara, lihatMemperbarui penyimpanan data acara dengan konsol.

AWS CLI

Untuk memperbarui penyimpanan data peristiwa tingkat akun untuk menerapkannya ke organisasi, jalankan update-event-data-storeperintah dan sertakan opsi. `--organization-enabled`

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

Kebijakan sumber daya default untuk administrator yang didelegasikan

CloudTrail secara otomatis menghasilkan kebijakan sumber daya yang dinamai `DelegatedAdminResourcePolicy` untuk penyimpanan data peristiwa organisasi yang mencantumkan tindakan yang diizinkan dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data peristiwa organisasi. Izin `DelegatedAdminResourcePolicy` berasal dari izin administrator yang didelegasikan di. AWS Organizations

Tujuannya `DelegatedAdminResourcePolicy` adalah untuk memastikan bahwa akun administrator yang didelegasikan dapat mengelola penyimpanan data acara organisasi atas nama

organisasi dan tidak secara tidak sengaja ditolak akses ke penyimpanan data acara organisasi ketika kebijakan berbasis sumber daya dilampirkan ke penyimpanan data acara organisasi yang memungkinkan atau menyangkal kepala sekolah melakukan tindakan pada penyimpanan data acara organisasi.

CloudTrail mengevaluasi bersama-sama `DelegatedAdminResourcePolicy` dengan kebijakan berbasis sumber daya yang disediakan untuk penyimpanan data acara organisasi. Akun administrator yang didelegasikan hanya akan ditolak aksesnya jika kebijakan berbasis sumber daya yang disediakan menyertakan pernyataan yang secara eksplisit menolak akun administrator yang didelegasikan melakukan tindakan pada penyimpanan data peristiwa organisasi yang seharusnya dapat dilakukan oleh akun administrator yang didelegasikan.

`DelegatedAdminResourcePolicy`Kebijakan ini diperbarui secara otomatis ketika:

- Akun manajemen mengonversi penyimpanan data acara organisasi ke penyimpanan data peristiwa tingkat akun, atau mengonversi penyimpanan data peristiwa tingkat akun menjadi penyimpanan data acara organisasi.
- Ada perubahan organisasi. Misalnya, akun manajemen mendaftarkan atau menghapus akun administrator yang CloudTrail didelegasikan.

Anda dapat melihat up-to-date kebijakan di bagian Kebijakan sumber daya administrator yang didelegasikan di CloudTrail konsol, atau dengan menjalankan AWS CLI `get-resource-policy` perintah dan meneruskan ARN penyimpanan data peristiwa organisasi.

Contoh berikut menjalankan `get-resource-policy` perintah pada penyimpanan data acara organisasi.

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

Output dari perintah ini akan menampilkan kebijakan berbasis sumber daya dan kebijakan yang dihasilkan untuk akun administrator yang `DelegatedAdminResourcePolicy` didelegasikan.

Sumber daya tambahan

- Administrator delegasi dalam organisasi
- Menambahkan administrator yang CloudTrail didelegasikan
- Menghapus administrator yang CloudTrail didelegasikan

Buat integrasi dengan sumber acara di luar AWS

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

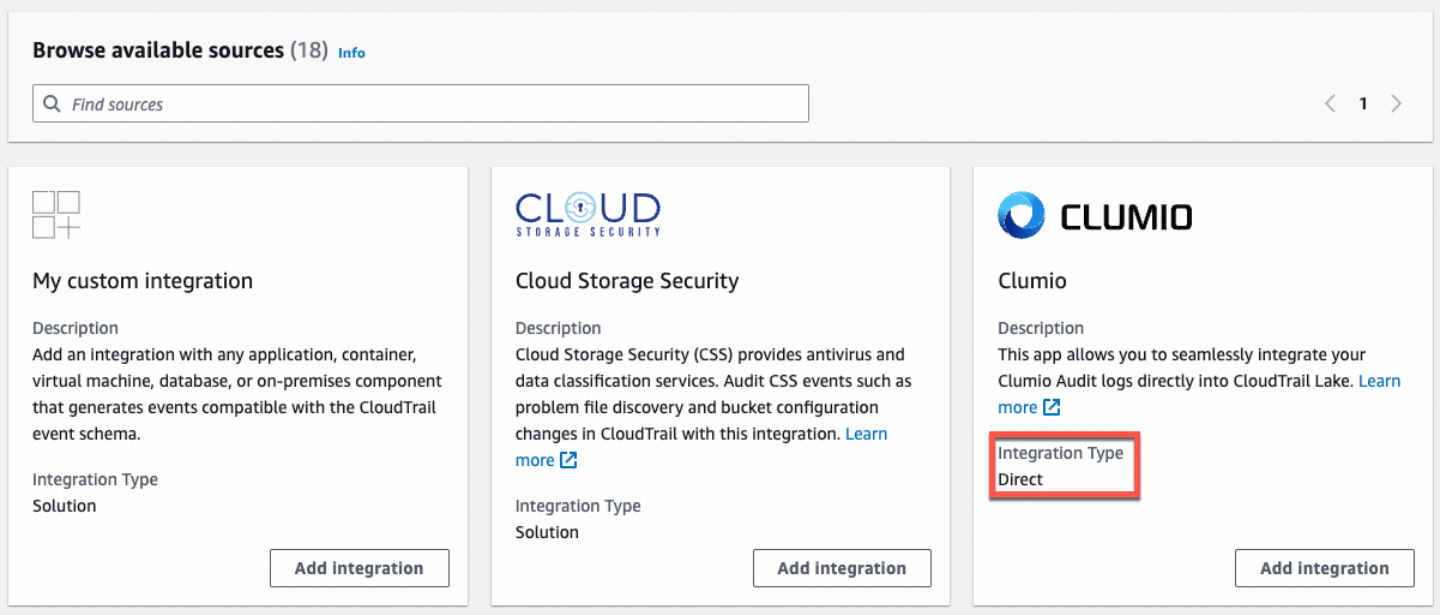
Anda dapat menggunakan CloudTrail untuk mencatat dan menyimpan data aktivitas pengguna dari sumber apa pun di lingkungan hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau kontainer. Anda dapat menyimpan, mengakses, menganalisis, memecahkan masalah, dan mengambil tindakan pada data ini tanpa mempertahankan beberapa agregator log dan alat pelaporan.

Acara aktivitas dari AWS non-sumber bekerja dengan menggunakan saluran untuk membawa acara ke CloudTrail Lake dari mitra eksternal yang bekerja dengan CloudTrail, atau dari sumber Anda sendiri. Saat membuat saluran, Anda memilih satu atau beberapa penyimpanan data acara untuk menyimpan peristiwa yang datang dari sumber saluran. Anda dapat mengubah penyimpanan data peristiwa tujuan untuk saluran sesuai kebutuhan, selama penyimpanan data peristiwa tujuan disetel ke `eventCategory="ActivityAuditLog"` peristiwa log. Saat Anda membuat saluran untuk acara dari mitra eksternal, Anda menyediakan saluran ARN ke mitra atau aplikasi sumber. Kebijakan sumber daya yang dilampirkan ke saluran memungkinkan sumber untuk mengirimkan peristiwa melalui saluran. Jika saluran tidak memiliki kebijakan sumber daya, hanya pemilik saluran yang dapat memanggil `PutAuditEvents` API di saluran tersebut.

CloudTrail telah bermitra dengan banyak penyedia sumber acara, seperti Okta dan. LaunchDarkly Saat Anda membuat integrasi dengan sumber acara di luar AWS, Anda dapat memilih salah satu mitra ini sebagai sumber acara Anda, atau memilih Integrasi kustom saya untuk mengintegrasikan peristiwa dari sumber Anda sendiri ke dalamnya CloudTrail. Maksimal satu saluran diperbolehkan per sumber.

Ada dua jenis integrasi: langsung dan solusi. Dengan integrasi langsung, mitra memanggil `PutAuditEvents` API untuk mengirimkan acara ke penyimpanan data acara untuk AWS akun Anda. Dengan integrasi solusi, aplikasi berjalan di AWS akun Anda dan aplikasi memanggil `PutAuditEvents` API untuk mengirimkan peristiwa ke penyimpanan data acara untuk AWS akun Anda.

Dari halaman Integrasi, Anda dapat memilih tab Sumber yang tersedia untuk melihat jenis Integrasi untuk mitra.



Untuk memulai, buat integrasi untuk mencatat peristiwa dari mitra atau sumber aplikasi lain menggunakan CloudTrail konsol.

Topik

- Buat integrasi dengan CloudTrail mitra dengan konsol
- Buat integrasi khusus dengan konsol
- Buat, perbarui, dan kelola integrasi CloudTrail Lake dengan AWS CLI
- Informasi tambahan tentang mitra integrasi
- CloudTrail Skema acara integrasi danau

Buat integrasi dengan CloudTrail mitra dengan konsol

Saat Anda membuat integrasi dengan sumber acara di luar AWS, Anda dapat memilih salah satu mitra ini sebagai sumber acara Anda. Saat Anda membuat integrasi CloudTrail dengan aplikasi mitra, mitra memerlukan Nama Sumber Daya Amazon (ARN) saluran yang Anda buat dalam alur kerja ini untuk mengirim acara. CloudTrail Setelah Anda membuat integrasi, Anda selesai mengonfigurasi integrasi dengan mengikuti instruksi mitra untuk menyediakan saluran ARN yang diperlukan kepada mitra. Integrasi mulai memasukkan acara mitra ke dalam CloudTrail setelah mitra memanggil `PutAuditEvents` saluran integrasi.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Integrasi.
3. Pada halaman Tambahkan integrasi, masukkan nama untuk saluran Anda. Namanya bisa 3-128 karakter. Hanya huruf, angka, titik, garis bawah, dan tanda hubung yang diizinkan.
4. Pilih sumber aplikasi mitra tempat Anda ingin mendapatkan acara. Jika Anda mengintegrasikan dengan acara dari aplikasi Anda sendiri yang dihosting di tempat atau di cloud, pilih Integrasi kustom saya.
5. Dari lokasi pengiriman acara, pilih untuk mencatat peristiwa aktivitas yang sama ke penyimpanan data acara yang ada, atau buat penyimpanan data acara baru.

   Jika Anda memilih untuk membuat penyimpanan data acara baru, masukkan nama untuk penyimpanan data acara, pilih opsi harga, dan tentukan periode retensi dalam beberapa hari. Penyimpanan data peristiwa menyimpan data peristiwa untuk jumlah hari yang ditentukan.

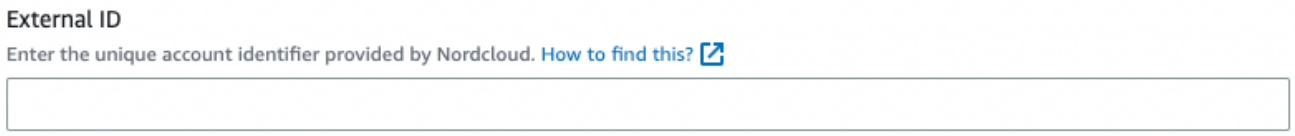
   Jika Anda memilih untuk mencatat peristiwa aktivitas ke satu atau beberapa penyimpanan data peristiwa yang ada, pilih penyimpanan data acara dari daftar. Penyimpanan data acara hanya dapat menyertakan peristiwa aktivitas. Jenis acara di konsol harus Peristiwa dari integrasi. Di API, `eventCategory` nilainya harus`ActivityAuditLog`.
6. Dalam Kebijakan sumber daya, konfigurasikan kebijakan sumber daya untuk saluran integrasi. Kebijakan sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya dan dalam kondisi tertentu. Akun yang didefinisikan sebagai prinsipal dalam kebijakan sumber daya dapat memanggil `PutAuditEvents` API untuk mengirimkan peristiwa ke channel Anda. Pemilik sumber daya memiliki akses implisit ke sumber daya jika kebijakan IAM miliknya mengizinkan tindakan `cloudtrail-data:PutAuditEvents` tersebut.

   Informasi yang diperlukan untuk kebijakan ditentukan oleh jenis integrasi. Untuk integrasi arah, CloudTrail secara otomatis menambahkan ID AWS akun mitra, dan mengharuskan Anda memasukkan ID eksternal unik yang disediakan oleh mitra. Untuk integrasi solusi, Anda harus menentukan setidaknya satu ID AWS akun sebagai prinsipal, dan secara opsional dapat memasukkan ID eksternal untuk mencegah wakil yang bingung.

> **Note**
>
> Jika Anda tidak membuat kebijakan sumber daya untuk saluran, hanya pemilik saluran yang dapat memanggil `PutAuditEvents` API di saluran.

a. Untuk integrasi langsung, masukkan ID eksternal yang disediakan oleh mitra Anda. Partner integrasi menyediakan ID eksternal yang unik, seperti ID akun atau string yang dibuat secara acak, untuk digunakan dalam integrasi guna mencegah masalah keamanan. Partner bertanggung jawab untuk membuat dan memberikan ID eksternal yang unik.

   Anda dapat memilih Bagaimana menemukan ini? untuk melihat dokumentasi mitra yang menjelaskan cara menemukan ID eksternal.



> **Note**
>
> Jika kebijakan sumber daya menyertakan ID eksternal, semua panggilan ke `PutAuditEvents` API harus menyertakan ID eksternal. Namun, jika kebijakan tidak menentukan ID eksternal, mitra masih dapat memanggil `PutAuditEvents` API dan menentukan `externalId` parameter.

b. Untuk integrasi solusi, pilih Tambah AWS akun untuk menentukan ID AWS akun yang akan ditambahkan sebagai prinsipal dalam kebijakan.

7. (Opsional) Di area Tag, Anda dapat menambahkan hingga 50 kunci tag dan pasangan nilai untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan dan saluran data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS
8. Saat Anda siap untuk membuat integrasi baru, pilih Tambahkan integrasi. Tidak ada halaman ulasan. CloudTrail membuat integrasi, tetapi Anda harus memberikan saluran Amazon Resource Name (ARN) ke aplikasi mitra. Petunjuk untuk menyediakan saluran ARN ke aplikasi mitra dapat

ditemukan di situs web dokumentasi mitra. Untuk informasi selengkapnya, pilih tautan Pelajari selengkapnya untuk mitra di tab Sumber yang tersedia di halaman Integrasi untuk membuka halaman mitra. AWS Marketplace

Untuk menyelesaikan penyiapan integrasi Anda, berikan saluran ARN ke mitra atau aplikasi sumber. Bergantung pada jenis integrasi, Anda, mitra, atau aplikasi menjalankan `PutAuditEvents` API untuk mengirimkan peristiwa aktivitas ke penyimpanan data peristiwa untuk AWS akun Anda. Setelah acara aktivitas Anda dikirimkan, Anda dapat menggunakan CloudTrail Lake untuk mencari, menanyakan, dan menganalisis data yang dicatat dari aplikasi Anda. Data acara Anda mencakup bidang yang cocok dengan payload CloudTrail acara, seperti`eventVersion`,`eventSource`, dan`userIdentity`.

Buat integrasi khusus dengan konsol

Anda dapat menggunakan CloudTrail untuk mencatat dan menyimpan data aktivitas pengguna dari sumber apa pun di lingkungan hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau kontainer. Lakukan paruh pertama prosedur ini di konsol CloudTrail Lake, lalu panggil `PutAuditEvents`API untuk menelan peristiwa, menyediakan ARN saluran dan muatan acara Anda. Setelah Anda menggunakan `PutAuditEvents` API untuk menyerap aktivitas aplikasi Anda CloudTrail, Anda dapat menggunakan CloudTrail Lake untuk mencari, menanyakan, dan menganalisis data yang dicatat dari aplikasi Anda.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Integrasi.
3. Pada halaman Tambahkan integrasi, masukkan nama untuk saluran Anda. Namanya bisa 3-128 karakter. Hanya huruf, angka, titik, garis bawah, dan tanda hubung yang diizinkan.
4. Pilih Integrasi kustom saya.
5. Dari lokasi pengiriman acara, pilih untuk mencatat peristiwa aktivitas yang sama ke penyimpanan data acara yang ada, atau buat penyimpanan data acara baru.

   Jika Anda memilih untuk membuat penyimpanan data acara baru, masukkan nama untuk penyimpanan data acara dan tentukan periode retensi dalam beberapa hari. Anda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika Anda memilih opsi harga retensi yang One-year dapat diperpanjang, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi. Seven-year

Jika Anda memilih untuk mencatat peristiwa aktivitas ke satu atau beberapa penyimpanan data peristiwa yang ada, pilih penyimpanan data acara dari daftar. Penyimpanan data acara hanya dapat menyertakan peristiwa aktivitas. Jenis acara di konsol harus Peristiwa dari integrasi. Di API, `eventCategory` nilainya harus`ActivityAuditLog`.

6. Dalam Kebijakan sumber daya, konfigurasikan kebijakan sumber daya untuk saluran integrasi. Kebijakan sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya dan dalam kondisi tertentu. Akun yang didefinisikan sebagai prinsipal dalam kebijakan sumber daya dapat memanggil `PutAuditEvents` API untuk mengirimkan peristiwa ke channel Anda.

   > **Note**
   >
   > Jika Anda tidak membuat kebijakan sumber daya untuk saluran, hanya pemilik saluran yang dapat memanggil `PutAuditEvents` API di saluran.

   a. (Opsional) Masukkan ID eksternal yang unik untuk memberikan lapisan perlindungan tambahan. ID eksternal adalah string unik seperti ID akun atau string yang dihasilkan secara acak, untuk mencegah wakil bingung.

      > **Note**
      >
      > Jika kebijakan sumber daya menyertakan ID eksternal, semua panggilan ke `PutAuditEvents` API harus menyertakan ID eksternal. Namun, jika kebijakan tidak menentukan ID eksternal, Anda masih dapat memanggil `PutAuditEvents` API dan menentukan `externalId` parameter.

   b. Pilih Tambah AWS akun untuk menentukan setiap ID AWS akun yang akan ditambahkan sebagai prinsipal dalam kebijakan sumber daya untuk saluran tersebut.

7. (Opsional) Di area Tag, Anda dapat menambahkan hingga 50 kunci tag dan pasangan nilai untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan dan saluran data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

8. Saat Anda siap untuk membuat integrasi baru, pilih Tambahkan integrasi. Tidak ada halaman ulasan. CloudTrail membuat integrasi, tetapi untuk mengintegrasikan peristiwa kustom Anda, Anda harus menentukan saluran ARN dalam permintaan. `PutAuditEvents`
9. Panggil `PutAuditEvents` API untuk memasukkan acara aktivitas Anda ke dalam CloudTrail. Anda dapat menambahkan hingga 100 acara aktivitas (atau hingga 1 MB) per `PutAuditEvents` permintaan. Anda memerlukan saluran ARN yang Anda buat pada langkah sebelumnya, muatan peristiwa yang ingin Anda tambahkan, dan ID eksternal (jika ditentukan CloudTrail untuk kebijakan sumber daya Anda). Pastikan bahwa tidak ada informasi sensitif atau pengenal pribadi dalam muatan acara sebelum menelannya. CloudTrail Peristiwa yang Anda konsumsi CloudTrail harus mengikuti. CloudTrail Skema acara integrasi danau

> **Tip**
>
> Gunakan AWS CloudShelluntuk memastikan Anda menjalankan AWS API terbaru.

Contoh berikut menunjukkan cara menggunakan perintah put-audit-events CLI. Parameter --audit-events dan --channel-arn diperlukan. Anda memerlukan ARN saluran yang Anda buat pada langkah-langkah sebelumnya, yang dapat Anda salin dari halaman detail integrasi. Nilai dari --audit-events adalah array JSON dari objek acara. `--audit-events`menyertakan ID yang diperlukan dari acara, muatan acara yang diperlukan sebagai nilai`EventData`, dan checksum opsional untuk membantu memvalidasi integritas acara setelah masuk ke dalam. CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

Berikut ini adalah contoh perintah dengan dua contoh acara.

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
```

```
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Contoh perintah berikut menambahkan `--cli-input-json` parameter untuk menentukan file JSON (`custom-events.json`) dari payload acara.

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

Berikut ini adalah contoh isi dari contoh file JSON,`custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(Opsional) Hitung nilai checksum

Checksum yang Anda tentukan sebagai nilai `EventDataChecksum` dalam `PutAuditEvents` permintaan membantu Anda memverifikasi bahwa CloudTrail menerima peristiwa yang cocok dengan checksum; ini membantu memverifikasi integritas peristiwa. Nilai checksum adalah algoritma Base64-SHA256 yang Anda hitung dengan menjalankan perintah berikut.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

Perintah mengembalikan checksum. Berikut adalah contohnya.

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

Nilai checksum menjadi nilai `EventDataChecksum` dalam `PutAuditEvents` permintaan Anda. Jika checksum tidak cocok dengan checksum untuk acara yang disediakan, CloudTrail tolak acara dengan kesalahan`InvalidChecksum`.

Buat, perbarui, dan kelola integrasi CloudTrail Lake dengan AWS CLI

Bagian ini menjelaskan perintah yang dapat Anda gunakan untuk membuat, memperbarui, dan mengelola integrasi CloudTrail Lake Anda menggunakan. AWS CLI

Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Perintah yang tersedia untuk integrasi CloudTrail Lake

Perintah untuk membuat, memperbarui, dan mengelola integrasi di CloudTrail Lake meliputi:

- `create-event-data-store`untuk membuat penyimpanan data acara untuk acara di luar AWS.
- `delete-channel`untuk menghapus saluran yang digunakan untuk integrasi.
- `delete-resource-policy`untuk menghapus kebijakan sumber daya yang dilampirkan ke saluran untuk integrasi CloudTrail Lake.
- `get-channel`untuk mengembalikan informasi tentang CloudTrail saluran.

- `get-resource-policy`untuk mengambil teks JSON dari dokumen kebijakan berbasis sumber daya yang dilampirkan ke saluran. CloudTrail
- `list-channels`untuk membuat daftar saluran di akun saat ini, dan nama sumbernya.
- `put-audit-events`untuk menelan acara aplikasi Anda ke CloudTrail Danau. Parameter yang diperlukan`auditEvents`,, menerima catatan JSON (juga disebut payload) dari peristiwa yang ingin CloudTrail Anda konsumsi. Anda dapat menambahkan hingga 100 acara ini (atau hingga 1 MB) per `PutAuditEvents` permintaan.
- `put-resource-policy`untuk melampirkan kebijakan izin berbasis sumber daya ke CloudTrail saluran yang digunakan untuk integrasi dengan sumber peristiwa di luar. AWSUntuk informasi selengkapnya tentang kebijakan berbasis sumber daya, lihat AWS CloudTrail contoh kebijakan berbasis sumber daya.
- `update-channel`untuk memperbarui saluran yang ditentukan oleh saluran ARN atau UUID yang diperlukan.

Untuk daftar perintah yang tersedia untuk penyimpanan data acara CloudTrail Lake, lihatPerintah yang tersedia untuk penyimpanan data acara.

Untuk daftar perintah yang tersedia untuk kueri CloudTrail Lake, lihatPerintah yang tersedia untuk kueri CloudTrail Lake.

Untuk daftar perintah yang tersedia untuk dasbor CloudTrail Lake, lihatPerintah yang tersedia untuk dasbor.

Buat integrasi untuk mencatat peristiwa dari luar AWS dengan AWS CLI

Bagian ini menjelaskan bagaimana Anda dapat menggunakan AWS CLI untuk membuat integrasi CloudTrail Lake untuk mencatat peristiwa dari luar AWS.

Dalam AWS CLI, Anda membuat integrasi dalam empat perintah (tiga jika Anda sudah memiliki penyimpanan data acara yang memenuhi kriteria). Penyimpanan data peristiwa yang Anda gunakan sebagai tujuan integrasi harus untuk satu Wilayah dan akun tunggal; mereka tidak dapat multi-wilayah, mereka tidak dapat mencatat peristiwa untuk organisasi AWS Organizations, dan mereka hanya dapat menyertakan peristiwa aktivitas. Jenis acara di konsol harus Peristiwa dari integrasi. Di API, `eventCategory` nilainya harus`ActivityAuditLog`. Untuk informasi selengkapnya tentang integrasi, lihatBuat integrasi dengan sumber acara di luar AWS.

1. Jalankan create-event-data-storeuntuk membuat penyimpanan data acara, jika Anda belum memiliki satu atau lebih penyimpanan data acara yang dapat Anda gunakan untuk integrasi.

AWS CLI Perintah contoh berikut membuat penyimpanan data peristiwa yang mencatat peristiwa dari luar AWS. Untuk peristiwa aktivitas, nilai pemilih `eventCategory` bidang adalah`ActivityAuditLog`. Penyimpanan data acara memiliki periode retensi 90 hari yang ditetapkan. Secara default, penyimpanan data acara mengumpulkan peristiwa dari semua Wilayah, tetapi karena ini mengumpulkan AWS non-peristiwa, atur ke satu Wilayah dengan menambahkan `--no-multi-region-enabled` opsi. Perlindungan penghentian diaktifkan secara default, dan penyimpanan data acara tidak mengumpulkan peristiwa untuk akun di organisasi.

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--no-multi-region-enabled \
--retention-period 90 \
--advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

Anda memerlukan ID penyimpanan data peristiwa (akhiran ARN, `EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE` atau contoh respons sebelumnya) untuk melanjutkan ke langkah berikutnya dan membuat saluran Anda.

2. Jalankan create-channelperintah untuk membuat saluran yang memungkinkan mitra atau aplikasi sumber untuk mengirim acara ke penyimpanan data acara di CloudTrail.

   Saluran memiliki komponen-komponen berikut:

   Sumber

   CloudTrail menggunakan informasi ini untuk menentukan mitra yang mengirimkan data acara atas nama Anda. CloudTrail Sumber diperlukan, dan dapat berupa `Custom` untuk semua AWS non-acara yang valid, atau nama sumber acara mitra. Maksimal satu saluran diperbolehkan per sumber.

   Untuk informasi tentang `Source` nilai untuk mitra yang tersedia, lihatInformasi tambahan tentang mitra integrasi.

   Status konsumsi

   Status saluran menunjukkan kapan peristiwa terakhir diterima dari sumber saluran.

   Destinasi

   Tujuannya adalah penyimpanan data acara CloudTrail Danau yang menerima acara dari saluran. Anda dapat mengubah penyimpanan data acara tujuan untuk saluran.

   Untuk berhenti menerima acara dari sumber, hapus saluran.

   Anda memerlukan ID setidaknya satu penyimpanan data acara tujuan untuk menjalankan perintah ini. Jenis tujuan yang valid adalah`EVENT_DATA_STORE`. Anda dapat mengirim peristiwa

yang dicerna ke lebih dari satu penyimpanan data acara. Contoh perintah berikut membuat saluran yang mengirimkan peristiwa ke dua penyimpanan data peristiwa, diwakili oleh mereka IDs dalam `Location` atribut `--destinations` parameter. Diperlukan `--destinations--name`,, dan `--source` parameter. Untuk menelan acara dari CloudTrail pasangan, tentukan nama mitra sebagai nilai. `--source` Untuk menelan peristiwa dari aplikasi Anda sendiri di luar AWS, tentukan `Custom` sebagai nilai. `--source`

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

Dalam menanggapi create-channel perintah Anda, salin ARN dari saluran baru. Anda memerlukan ARN untuk menjalankan `put-audit-events` perintah `put-resource-policy` dan di langkah selanjutnya.

3. Jalankan put-resource-policyperintah untuk melampirkan kebijakan sumber daya ke saluran. Kebijakan sumber daya adalah dokumen kebijakan JSON yang menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya dan dalam kondisi tertentu. Akun yang didefinisikan sebagai prinsipal dalam kebijakan sumber daya saluran dapat memanggil `PutAuditEvents` API untuk mengirimkan peristiwa.

> **Note**
>
> Jika Anda tidak membuat kebijakan sumber daya untuk saluran, hanya pemilik saluran yang dapat memanggil `PutAuditEvents` API di saluran.

Informasi yang diperlukan untuk kebijakan ditentukan oleh jenis integrasi.

- Untuk integrasi arah, CloudTrail mewajibkan kebijakan untuk memuat AWS akun mitra IDs, dan mengharuskan Anda memasukkan ID eksternal unik yang disediakan oleh mitra. CloudTrail secara otomatis menambahkan AWS akun mitra IDs ke kebijakan sumber daya saat Anda membuat integrasi menggunakan CloudTrail konsol. Lihat dokumentasi mitra untuk mempelajari cara mendapatkan nomor AWS akun yang diperlukan untuk kebijakan tersebut.

- Untuk integrasi solusi, Anda harus menentukan setidaknya satu ID AWS akun sebagai prinsipal, dan secara opsional dapat memasukkan ID eksternal untuk mencegah wakil yang bingung.

Berikut ini adalah persyaratan untuk kebijakan sumber daya:

- Sumber daya ARN yang didefinisikan dalam kebijakan harus sesuai dengan saluran ARN yang dilampirkan kebijakan tersebut.
- Kebijakan ini hanya berisi satu tindakan: cloudtrail-data: PutAuditEvents
- Kebijakan tersebut berisi setidaknya satu pernyataan. Kebijakan tersebut dapat memiliki maksimal 20 pernyataan.
- Setiap pernyataan berisi setidaknya satu prinsipal. Sebuah pernyataan dapat memiliki maksimal 50 kepala sekolah.

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
                {
```

```
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

Untuk informasi selengkapnya tentang kebijakan sumber daya, lihatAWS CloudTrail contoh kebijakan berbasis sumber daya.

4. Jalankan `PutAuditEvents`API untuk memasukkan peristiwa aktivitas Anda ke dalam CloudTrail. Anda memerlukan muatan acara yang CloudTrail ingin Anda tambahkan. Pastikan bahwa tidak ada informasi sensitif atau pengenal pribadi dalam muatan acara sebelum menelannya. CloudTrail Perhatikan bahwa `PutAuditEvents` API menggunakan titik akhir `cloudtrail-data` CLI, bukan titik akhir. `cloudtrail`

   Contoh berikut menunjukkan cara menggunakan perintah put-audit-events CLI. Parameter --audit-events dan --channel-arn diperlukan. --external-idParameter diperlukan jika ID eksternal didefinisikan dalam kebijakan sumber daya. Anda memerlukan ARN dari saluran yang Anda buat pada langkah sebelumnya. Nilai dari --audit-events adalah array JSON dari objek acara. `--audit-events`menyertakan ID yang diperlukan dari acara, muatan acara yang diperlukan sebagai nilai`EventData`, dan checksum opsional untuk membantu memvalidasi integritas acara setelah masuk ke dalam. CloudTrail

   ```
   aws cloudtrail-data put-audit-events \
   --channel-arn $ChannelArn \
   --external-id $UniqueExternalIDFromPartner \
   --audit-events \
   id="event_ID",eventData='"{event_payload}"' \
   id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
   ```

   Berikut ini adalah contoh perintah dengan dua contoh acara.

   ```
   aws cloudtrail-data put-audit-events \
   --channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
   a06a-43969EXAMPLE \
   --external-id UniqueExternalIDFromPartner \
   --audit-events \
   id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
   \"eventSource\":\"custom1.domain.com\", ...
   ```

```
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

Contoh perintah berikut menambahkan `--cli-input-json` parameter untuk menentukan file JSON (`custom-events.json`) dari payload acara.

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

Berikut ini adalah contoh isi dari contoh file JSON,`custom-events.json`.

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

Anda dapat memverifikasi bahwa integrasi berfungsi, dan CloudTrail menelan peristiwa dari sumber dengan benar, dengan menjalankan get-channelperintah. Output dari get-channel menunjukkan cap waktu terbaru yang CloudTrail menerima acara.

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(Opsional) Hitung nilai checksum

Checksum yang Anda tentukan sebagai nilai `EventDataChecksum` dalam `PutAuditEvents` permintaan membantu Anda memverifikasi bahwa CloudTrail menerima peristiwa yang cocok dengan checksum; ini membantu memverifikasi integritas peristiwa. Nilai checksum adalah SHA256 algoritma base64- yang Anda hitung dengan menjalankan perintah berikut.

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
       \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
       \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
       \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
       \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
       \"additionalEventData\":{\"key\":\"value\"},
       \"sourceIPAddress\":\"source_IP_address\",
       \"recipientAccountId\":\"recipient_account_ID\"}",
       "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

Perintah mengembalikan checksum. Berikut adalah contohnya.

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

Nilai checksum menjadi nilai `EventDataChecksum` dalam `PutAuditEvents` permintaan Anda. Jika checksum tidak cocok dengan checksum untuk acara yang disediakan, CloudTrail tolak acara dengan kesalahan`InvalidChecksum`.

Perbarui saluran dengan AWS CLI

Bagian ini menjelaskan bagaimana Anda dapat menggunakan AWS CLI untuk memperbarui saluran untuk integrasi CloudTrail Lake. Anda dapat menjalankan `update-channel` perintah untuk memperbarui nama saluran atau untuk menentukan penyimpanan data acara tujuan yang berbeda. Anda tidak dapat memperbarui sumber saluran.

Saat Anda menjalankan perintah, `--channel` parameter diperlukan.

Berikut ini adalah contoh yang menunjukkan cara memperbarui nama saluran dan tujuan.

```
aws cloudtrail update-channel \
```

```
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

Hapus saluran untuk menghapus integrasi dengan AWS CLI

Bagian ini menjelaskan cara menjalankan `delete-channel` perintah untuk menghapus saluran untuk integrasi CloudTrail Lake. Anda akan menghapus saluran, jika Anda ingin berhenti menelan mitra atau acara aktivitas lain di luar. AWS ARN atau ID saluran (akhiran ARN) dari saluran yang ingin Anda hapus diperlukan.

Contoh berikut menunjukkan cara menghapus saluran.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Informasi tambahan tentang mitra integrasi

Tabel di bagian ini memberikan nama sumber untuk setiap mitra integrasi dan mengidentifikasi jenis integrasi (langsung atau solusi).

Informasi di kolom Source name diperlukan saat memanggil `CreateChannel` API. Anda menentukan nama sumber sebagai nilai untuk `Source` parameter.

Nama mitra (konsol)	Nama sumber (API)	Tipe integrasi
Integrasi kustom saya	`Custom`	solusi
Keamanan Penyimpanan Cloud	`CloudStorageSecurityConsole`	solusi
Clumio	`Clumio`	langsung
CrowdStrike	`CrowdStrike`	solusi
CyberArk	`CyberArk`	solusi

Nama mitra (konsol)	Nama sumber (API)	Tipe integrasi
GitHub	`GitHub`	solusi
Hong Kong Inc	`KongGatewayEnterprise`	solusi
LaunchDarkly	`LaunchDarkly`	langsung
Netskope	`NetskopeCloudExchange`	solusi
Nordcloud, Perusahaan IBM	`IBMMulticloud`	langsung
MontyCloud	`MontyCloud`	langsung
Okta	`OktaSystemLogEvents`	solusi
Satu Identitas	`OneLogin`	solusi
Shoreline.io	`Shoreline`	solusi
Snyk.io	`Snyk`	langsung
Wiz	`WizAuditLogs`	solusi

Lihat dokumentasi mitra

Anda dapat mempelajari lebih lanjut tentang integrasi mitra dengan CloudTrail Lake dengan melihat dokumentasi mereka.

Untuk melihat dokumentasi mitra

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Integrasi.
3. Dari halaman Integrasi, pilih Sumber yang tersedia, lalu pilih Pelajari lebih lanjut untuk mitra yang dokumentasinya ingin Anda lihat.

CloudTrail Skema acara integrasi danau

Tabel berikut menjelaskan elemen skema wajib dan opsional yang cocok dengan yang ada dalam catatan CloudTrail peristiwa. Isi `eventData` disediakan oleh acara Anda; bidang lain disediakan oleh CloudTrail setelah konsumsi.

CloudTrail isi catatan acara dijelaskan secara lebih rinci dalamCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

- Bidang yang disediakan oleh CloudTrail setelah konsumsi
- Bidang yang disediakan oleh acara Anda

Bidang berikut disediakan oleh CloudTrail setelah konsumsi:

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
eventVersion	string	Diperlukan	Versi acara.
EventKategori	string	Diperlukan	Kategori acara. Untuk AWS non-event, nilainya adalah`ActivityAuditLog` .
eventType	string	Diperlukan	Jenis peristiwa. Untuk AWS non-event, nilai validnya adalah`ActivityLog` .
EventID	string	Diperlukan	ID unik untuk suatu acara.
eventTime	string	Diperlukan	Stempel waktu acara, dalam `yyyy-MM-DDTHH:mm:ss` format, dalam

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
			Waktu Terkoordinasi Universal (UTC).
awsRegion	string	Diperlukan	Di Wilayah AWS mana `PutAuditEvents` panggilan itu dibuat.
penerima AccountId	string	Diperlukan	Merupakan ID akun yang menerima acara ini. CloudTrail mengisi bidang ini dengan menghitungnya dari payload acara.
addendum	-	Opsional	Menampilkan informasi tentang mengapa pemrosesan acara ditunda. Jika informasi hilang dari peristiwa yang ada, blok addendum mencakup informasi yang hilang dan alasan mengapa itu hilang.
• akal budi	string	Opsional	Alasan bahwa peristiwa atau beberapa isinya hilang.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• UpdatedFields	string	Opsional	Bidang catatan acara yang diperbarui oleh addendum. Ini hanya disediakan jika alasannya`UPDATED_DATA` .
• OriginaLuid	string	Opsional	Event asli UID dari sumbernya. Ini hanya disediakan jika alasannya`UPDATED_DATA` .
• OriginalEventid	string	Opsional	ID acara asli. Ini hanya disediakan jika alasannya`UPDATED_DATA` .
Metadata	-	Diperlukan	Informasi tentang saluran yang digunakan acara tersebut.
• ingestionTime	string	Diperlukan	Stempel waktu saat acara diproses, dalam `yyyy-MM-DDTHH:mm:ss` format, dalam Waktu Terkoordinasi Universal (UTC).
• ChannelARN	string	Diperlukan	ARN dari saluran yang digunakan acara tersebut.

Bidang berikut disediakan oleh acara pelanggan:

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
EventData	-	Diperlukan	Data audit dikirim ke CloudTrail dalam `PutAuditEvents` panggilan.
• versi	string	Diperlukan	Versi acara dari sumbernya. Kendala panjang: Panjang maksimum 256.
• userIdentity	-	Diperlukan	Informasi tentang pengguna yang mengajukan permintaan.
• • jenis	string	Diperlukan	Jenis identitas pengguna. Kendala panjang: Panjang maksimum 128.
• • principalId	string	Diperlukan	Pengenal unik untuk aktor acara tersebut. Kendala panjang: Panjang maksimum 1024.
• • detail	Objek JSON	Opsional	Informasi tambahan tentang identitas.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• UserAgent	string	Opsional	Agen yang melaluinya permintaan itu dibuat. Kendala panjang: Panjang maksimum 1024.
• EventSource	string	Diperlukan	Ini adalah sumber acara mitra, atau aplikasi khusus tentang peristiwa mana yang dicatat. Kendala panjang: Panjang maksimum 1024.
• eventName	string	Diperlukan	Tindakan yang diminta, salah satu tindakan dalam API untuk layanan sumber atau aplikasi. Kendala panjang: Panjang maksimum 1024.
• eventTime	string	Diperlukan	Stempel waktu acara, dalam `yyyy-MM-DDTHH:mm:ss s` format, dalam Waktu Terkoordinasi Universal (UTC).

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• UID	string	Diperlukan	Nilai UID yang mengidentifikasi permintaan. Layanan atau aplikasi yang disebut menghasilkan nilai ini. Kendala panjang: Panjang maksimum 1024.
• requestParameters	Objek JSON	Opsional	Parameter, jika ada, yang dikirim dengan permintaan. Bidang ini memiliki ukuran maksimum 100 kB, dan konten yang melebihi batas ditolak.
• ResponseElements	Objek JSON	Opsional	Elemen respons untuk tindakan yang membuat perubahan (membuat, memperbarui, atau menghapus tindakan) . Bidang ini memiliki ukuran maksimum 100 kB, dan konten yang melebihi batas ditolak.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• errorCode	string	Opsional	Sebuah string yang mewakili kesalahan untuk acara tersebut. Kendala panjang: Panjang maksimum 256.
• errorMessage	string	Opsional	Deskripsi kesalahan. Kendala panjang: Panjang maksimum 256.
• sourceIPAddress	string	Opsional	Alamat IP dari mana permintaan dibuat. Alamat IPv4 dan IPv6 diterima.
• penerima AccountId	string	Diperlukan	Merupakan ID akun yang menerima acara ini. ID akun harus sama dengan ID AWS akun yang memiliki saluran.
• tambahan EventData	Objek JSON	Opsional	Data tambahan tentang peristiwa yang bukan bagian dari permintaan atau tanggapan. Bidang ini memiliki ukuran maksimum 28 kB, dan konten yang melebihi batas tersebut ditolak.

Contoh berikut menunjukkan hierarki elemen skema yang cocok dengan yang ada dalam catatan CloudTrail peristiwa.

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
       "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
             JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
```

```
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

CloudTrail Dasbor danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Anda dapat menggunakan dasbor CloudTrail Danau untuk melihat tren acara untuk penyimpanan data acara di akun Anda. CloudTrail Lake menawarkan jenis dasbor berikut:

- Dasbor terkelola — Anda dapat melihat dasbor terkelola untuk melihat tren acara untuk penyimpanan data acara yang mengumpulkan peristiwa manajemen, peristiwa data, atau peristiwa Wawasan. Dasbor ini secara otomatis tersedia untuk Anda dan dikelola oleh CloudTrail Lake. CloudTrail menawarkan 14 dasbor terkelola untuk dipilih. Anda dapat menyegarkan dasbor terkelola secara manual. Anda tidak dapat memodifikasi, menambah, atau menghapus widget untuk dasbor ini, namun, Anda dapat menyimpan dasbor terkelola sebagai dasbor khusus jika Anda ingin memodifikasi widget atau mengatur jadwal penyegaran.
- Dasbor khusus - Dasbor khusus memungkinkan Anda untuk menanyakan peristiwa dalam jenis penyimpanan data acara apa pun. Anda dapat menambahkan hingga 10 widget ke dasbor kustom. Anda dapat menyegarkan dasbor kustom secara manual, atau Anda dapat mengatur jadwal penyegaran.
- Dasbor Sorotan — Aktifkan dasbor Sorotan untuk melihat ikhtisar sekilas tentang AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Dasbor Sorotan dikelola oleh CloudTrail dan menyertakan widget yang relevan dengan akun Anda. Widget yang ditampilkan di dasbor Sorotan unik untuk setiap akun. Widget ini dapat muncul aktivitas abnormal atau anomali yang terdeteksi. Misalnya, dasbor Sorotan Anda dapat menyertakan widget akses lintas

akun Total, yang menunjukkan jika ada peningkatan aktivitas lintas akun yang tidak normal. CloudTrail memperbarui dasbor Sorotan setiap 6 jam. Dasbor menunjukkan 24 jam terakhir data dari pembaruan terakhir.

Setiap dasbor terdiri dari satu atau lebih widget dan setiap widget menyediakan representasi grafis dari hasil query SQL. Untuk melihat kueri widget, pilih Lihat dan edit kueri untuk membuka editor kueri.

Saat dasbor disegarkan, CloudTrail Lake menjalankan kueri untuk mengisi widget dasbor. Karena menjalankan kueri menimbulkan biaya, CloudTrail meminta Anda untuk mengetahui biaya yang terkait dengan menjalankan kueri. Untuk informasi selengkapnya tentang CloudTrail harga, lihat CloudTrail Harga.

Topik

- Prasyarat
- Batasan
- Dukungan Wilayah
- Izin yang diperlukan
- Lihat dasbor terkelola dengan CloudTrail konsol
- Aktifkan dasbor Sorotan dengan CloudTrail konsol
- Nonaktifkan dasbor Sorotan dengan CloudTrail konsol
- Buat dasbor khusus dengan CloudTrail konsol
- Tetapkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol
- Nonaktifkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol
- Ubah perlindungan terminasi dengan CloudTrail konsol
- Hapus dasbor khusus dengan CloudTrail konsol
- Buat, perbarui, dan kelola dasbor dengan AWS CLI

Prasyarat

Prasyarat berikut berlaku untuk dasbor Danau: CloudTrail

- Untuk melihat dan menggunakan dasbor Danau, Anda harus membuat setidaknya satu penyimpanan data acara CloudTrail Danau. Anda dapat membuat penyimpanan data acara

menggunakan konsol, AWS CLI, atau SDK. Untuk informasi tentang membuat penyimpanan data acara menggunakan konsol, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol. Untuk informasi tentang membuat penyimpanan data acara menggunakan AWS CLI, lihatBuat toko data acara dengan AWS CLI.

- Anda harus memiliki izin yang memadai untuk melihat, membuat, memperbarui, dan menyegarkan dasbor. Untuk informasi selengkapnya, lihat Izin yang diperlukan.

Batasan

Batasan berikut berlaku untuk dasbor CloudTrail Danau:

- Anda hanya dapat mengaktifkan dasbor Sorotan untuk penyimpanan data acara yang ada di akun Anda.
- Anda hanya dapat melihat dasbor terkelola untuk penyimpanan data peristiwa yang ada di akun Anda.
- Untuk dasbor kustom, Anda hanya dapat menambahkan widget sampel atau membuat widget baru yang menyimpan data peristiwa kueri yang ada di akun Anda.
- Administrator yang didelegasikan untuk AWS Organizations organisasi tidak dapat melihat atau mengelola dasbor yang dimiliki oleh akun manajemen.

Dukungan Wilayah

Dasbor CloudTrail Danau didukung di semua Wilayah AWS tempat CloudTrail Danau didukung.

Widget ringkasan Aktivitas di dasbor Sorotan didukung di Wilayah berikut:

- Wilayah Asia Pasifik (Tokyo) (ap-northeast-1)
- AS Timur (Virginia Utara) (us-east-1)
- Wilayah AS Barat (Oregon) (us-west-1)

Semua widget lainnya didukung di semua Wilayah AWS tempat CloudTrail Lake didukung.

Untuk informasi tentang Wilayah yang didukung CloudTrail Danau, lihatCloudTrail Daerah yang didukung Danau.

Izin yang diperlukan

Bagian ini menjelaskan izin yang diperlukan untuk dasbor CloudTrail Lake dan membahas dua jenis kebijakan IAM:

- Identity-based kebijakan yang memungkinkan Anda melakukan tindakan untuk membuat, mengelola, dan menghapus dasbor.
- Resource-based kebijakan yang memungkinkan CloudTrail untuk menjalankan kueri di penyimpanan data acara Anda saat dasbor di-refresh dan melakukan penyegaran terjadwal dasbor kustom dan dasbor Sorotan atas nama Anda. Saat membuat dasbor menggunakan CloudTrail konsol, Anda diberi opsi untuk melampirkan kebijakan berbasis sumber daya. Anda juga dapat menjalankan AWS CLI `put-resource-policy`perintah untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara atau dasbor Anda.

Identity-based persyaratan kebijakan

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

Untuk melihat dan mengelola dasbor CloudTrail Danau, Anda memerlukan salah satu kebijakan berikut:

- Kebijakan yang `CloudTrailFullAccess`dikelola.
- Kebijakan yang `AdministratorAccess`dikelola.
- Kebijakan khusus yang menyertakan satu atau beberapa izin khusus yang dijelaskan di bagian berikut.

Topik

- Izin yang diperlukan untuk membuat dasbor
- Izin yang diperlukan untuk memperbarui dasbor
- Izin yang diperlukan untuk menyegarkan dasbor

Izin yang diperlukan untuk membuat dasbor

Kebijakan contoh berikut memberikan izin minimum yang diperlukan untuk membuat dasbor. Ganti *partitionregion*,*account-id*,, dan *eds-id* dengan nilai untuk konfigurasi Anda.

- `StartQuery`izin diperlukan hanya jika permintaan berisi widget. Berikan `StartQuery` izin untuk semua penyimpanan data acara yang disertakan dalam kueri widget.
- `StartDashboardRefresh`izin hanya diperlukan jika dasbor memiliki jadwal penyegaran.
- Untuk dasbor Sorotan, penelepon harus memiliki `StartQuery` izin pada semua penyimpanan data acara di akun.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Izin yang diperlukan untuk memperbarui dasbor

Kebijakan contoh berikut memberikan izin minimum yang diperlukan untuk memperbarui dasbor. Ganti *partitionregion*,*account-id*,, dan *eds-id* dengan nilai untuk konfigurasi Anda.

- `StartQuery`izin diperlukan hanya jika permintaan berisi widget. Berikan `StartQuery` izin untuk semua penyimpanan data acara yang disertakan dalam kueri widget.

- `StartDashboardRefresh`izin hanya diperlukan jika dasbor memiliki jadwal penyegaran.
- Untuk dasbor Sorotan, penelepon harus memiliki `StartQuery` izin pada semua penyimpanan data acara di akun.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:UpdateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Izin yang diperlukan untuk menyegarkan dasbor

Kebijakan contoh berikut memberikan izin minimum yang diperlukan untuk menyegarkan dasbor. Ganti *partitionregion*,*account-id*,*dashboard-name*,,, dan *eds-id* dengan nilai untuk konfigurasi Anda.

- Untuk dasbor khusus dan dasbor Sorotan, pemanggil harus memilikinya. `cloudtrail:StartDashboardRefresh permissions`
- Untuk dasbor terkelola, pemanggil harus memiliki `cloudtrail:StartDashboardRefresh` izin dan `cloudtrail:StartQuery` izin untuk penyimpanan data peristiwa yang terlibat dalam penyegaran.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/dashboard-
name",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

Resource-based kebijakan untuk dasbor dan penyimpanan data acara

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Untuk menjalankan kueri di dasbor selama penyegaran manual atau terjadwal, Anda harus melampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa yang terkait dengan widget di dasbor. Hal ini memungkinkan CloudTrail Lake untuk menjalankan kueri atas nama Anda. Saat Anda membuat dasbor khusus, atau mengaktifkan dasbor Sorotan menggunakan CloudTrail konsol, CloudTrail memberi Anda opsi untuk memilih penyimpanan data acara mana yang ingin Anda terapkan izin. Untuk informasi selengkapnya tentang kebijakan berbasis sumber daya, lihat. Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor

Untuk mengatur jadwal penyegaran dasbor, Anda harus melampirkan kebijakan berbasis sumber daya ke dasbor untuk memungkinkan CloudTrail Lake menyegarkan dasbor atas nama Anda. Saat

Anda menetapkan jadwal penyegaran untuk dasbor kustom, atau mengaktifkan dasbor Sorotan menggunakan CloudTrail konsol, CloudTrail memberi Anda opsi untuk melampirkan kebijakan berbasis sumber daya ke dasbor Anda. Untuk contoh kebijakan, lihat Resource-based contoh kebijakan untuk dasbor.

Anda dapat melampirkan kebijakan berbasis sumber daya menggunakan CloudTrail konsol, operasi AWS CLI, atau API. PutResourcePolicy

Izin kunci KMS untuk mendekripsi data di penyimpanan data acara

Jika penyimpanan data peristiwa yang ditanyakan dienkripsi dengan kunci KMS, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data di penyimpanan data peristiwa. Contoh pernyataan kebijakan berikut memungkinkan prinsipal CloudTrail layanan untuk mendekripsi penyimpanan data peristiwa.

```
{
      "Sid": "AllowCloudTrailDecryptAccess",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Lihat dasbor terkelola dengan CloudTrail konsol

CloudTrail Lake menyediakan dasbor terkelola yang menunjukkan tren acara untuk penyimpanan data acara yang mengumpulkan peristiwa manajemen, peristiwa data, dan peristiwa Wawasan. Dasbor ini dikelola oleh CloudTrail Lake. Anda tidak dapat memodifikasi, menambah, atau menghapus widget untuk dasbor ini, namun, Anda dapat menyimpan dasbor terkelola sebagai dasbor khusus jika Anda ingin memodifikasi widget atau mengatur jadwal penyegaran.

> **Note**
>
> Anda hanya dapat melihat dasbor terkelola untuk penyimpanan data peristiwa yang ada di akun Anda.

Untuk melihat dasbor terkelola

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Dari dasbor Terkelola, pilih dasbor yang ingin Anda lihat. Untuk informasi selengkapnya, lihat Dasbor terkelola yang tersedia.

   > **Note**
   >
   > Dropdown hanya menampilkan penyimpanan data peristiwa yang relevan untuk dasbor yang dipilih. Misalnya, jika Anda memilih dasbor yang berfokus pada peristiwa data, seperti peristiwa data S3, tarik-turun hanya akan menampilkan penyimpanan data peristiwa yang dikonfigurasi untuk mengumpulkan peristiwa data.

5. Pilih penyimpanan data acara untuk dasbor. CloudTrail akan menjalankan kueri di dasbor ini saat dasbor disegarkan.
6. Untuk melihat kueri widget, pilih Lihat dan edit kueri di bagian bawah widget.
7. Pilih untuk memfilter data dasbor dengan rentang Absolute atau Rentang relatif. Pilih Rentang absolut untuk memilih tanggal dan rentang waktu tertentu. Pilih Rentang relatif untuk memilih rentang waktu yang telah ditentukan atau rentang khusus. Secara default, dasbor menampilkan data acara selama 24 jam terakhir.

   > **Note**
   >
   > CloudTrail Kueri danau menimbulkan biaya berdasarkan jumlah data yang dipindai. Untuk membantu mengontrol biaya, Anda dapat memfilter pada rentang waktu yang lebih sempit. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

8. Pilih ikon penyegaran untuk mengisi grafik untuk widget dasbor. Setiap widget menunjukkan status penyegaran.

Simpan dasbor terkelola sebagai dasbor khusus

Anda tidak dapat mengubah dasbor terkelola, tetapi Anda dapat menyimpan salinan sebagai dasbor khusus. Ini memungkinkan Anda untuk mengatur jadwal penyegaran untuk dasbor dan memodifikasi widget.

Untuk menyimpan dasbor terkelola sebagai dasbor khusus

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Pilih dasbor terkelola yang ingin Anda buat salinannya.
5. Pilih Simpan sebagai dasbor baru.
6. Berikan nama untuk mengidentifikasi dasbor.
7. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi dan mengurutkan dasbor Anda. Untuk informasi selengkapnya tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya di Panduan Pengguna AWS Sumber Daya Penandaan.
8. Untuk Izin, pilih penyimpanan data acara yang ingin Anda terapkan izin. Karena CloudTrail menjalankan kueri untuk mengisi data untuk widget di dasbor, CloudTrail memerlukan izin untuk menjalankan kueri di penyimpanan data acara yang terkait dengan widget dasbor. Untuk setiap penyimpanan data peristiwa yang dipilih dalam langkah ini, CloudTrail melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa yang memungkinkan untuk menjalankan kueri. CloudTrail Anda dapat membatalkan pilihan penyimpanan data acara jika Anda tidak ingin mengizinkan izin.
9. Pilih Buat dasbor.

Setelah Anda membuat dasbor khusus, Anda dapat menambahkan widget, menghapus widget, dan mengatur jadwal penyegaran untuk dasbor.

Dasbor terkelola yang tersedia

Bagian ini memberikan informasi tentang dasbor terkelola yang tersedia dan memberikan informasi tentang widget yang ditampilkan di setiap dasbor.

Dasbor terkelola yang tersedia:

- Dasbor pemantauan keamanan
- Dasbor aktivitas IAM
- Dasbor aktivitas pengguna
- Dasbor acara yang diperkaya
- Dasbor analisis kesalahan
- Dasbor aktivitas EC2
- Dasbor aktivitas Organizations
- Dasbor perubahan sumber daya
- Dasbor ikhtisar peristiwa data
- Dasbor peristiwa data Lambda
- Dasbor peristiwa data DynamoDB
- Dasbor peristiwa data S3
- Dasbor acara wawasan
- Dasbor acara manajemen
- Dasbor ikhtisar

Dasbor pemantauan keamanan

Dasbor ini memberikan tampilan terpusat dari widget yang berfokus pada keamanan kritis, seperti peristiwa yang ditolak akses teratas, upaya login konsol yang gagal dan alamat IP terkait, upaya login konsol pengguna root, tindakan destruktif, akses lintas akun, dan widget fokus keamanan kritis lainnya. Ini memberikan deteksi dan respons insiden cepat untuk meningkatkan postur keamanan Anda secara keseluruhan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Akses teratas ditolak acara

Melacak peristiwa yang ditolak akses yang paling sering terjadi, dikelompokkan berdasarkan API.

Upaya yang ConsoleLogin gagal

Melacak tren upaya login konsol yang gagal dari waktu ke waktu, dengan kerusakan pada MFA vs penelepon yang diautentikasi. Non-MFA

ConsoleLogin Upaya gagal dengan alamat IP

Melacak alamat IP yang terkait dengan upaya login konsol yang gagal dan menampilkan alamat IP yang menyinggung teratas dengan jumlah login yang gagal.

ConsoleLogin Upaya pengguna root

Melacak frekuensi upaya login konsol yang dilakukan oleh pengguna root dari waktu ke waktu.

Tindakan destruktif

Melacak frekuensi operasi hapus dari waktu ke waktu.

Akses lintas akun teratas

Melacak aktivitas lintas akun teratas berdasarkan ID dan tindakan akun pemanggil.

Pengguna yang menonaktifkan MFA

Melacak pengguna terbaru yang menonaktifkan MFA.

EC2 terbaru SecurityGroup dan perubahan NetworkAcl

Melacak EC2 terbaru SecurityGroup dan NetworkAcl perubahan.

SecurityGroup Perubahan EC2 terbaru yang memungkinkan akses publik

Melacak grup keamanan EC2 terbaru yang memiliki aturan yang memungkinkan publik (0.0.0.0/0) akses.

Potensi CloudTrail tindakan penonaktifan

Melacak tindakan terbaru yang berisiko mengganggu CloudTrail logging.

Dasbor aktivitas IAM

Dasbor ini memberikan visibilitas ke API IAM yang umum digunakan, kesalahan API, perubahan entitas IAM, dan alamat IP pemanggil teratas, memungkinkan identifikasi tindakan IAM yang tidak diinginkan dan masalah kepatuhan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

API IAM Teratas

Melacak API IAM yang paling sering digunakan.

Penelepon IAM teratas

Melacak penelepon API IAM yang paling sering.

Kesuksesan IAM vs tren kegagalan

Melacak tren kesuksesan dan panggilan API IAM yang gagal dari waktu ke waktu.

Kesalahan API IAM teratas

Melacak kesalahan yang paling sering terjadi dalam memanggil API IAM.

API AccessDenied IAM Teratas

Melacak panggilan API IAM paling sering yang gagal dengan kesalahan akses ditolak.

Alamat IP teratas panggilan IAM

Melacak alamat IP sumber teratas dari mana panggilan API IAM dibuat.

Perubahan kebijakan IAM terbaru

Melacak perubahan terbaru pada kebijakan IAM, dikategorikan berdasarkan operasi IAM API spesifik yang memfasilitasi perubahan, sumber daya IAM (pengguna, peran, atau grup) yang terkait dengan perubahan kebijakan, dan nama kebijakan atau ARN yang digunakan.

Perubahan pengguna IAM terbaru

Melacak perubahan terbaru pada pengguna IAM, dikategorikan berdasarkan API IAM spesifik yang memfasilitasi manajemen pengguna, pengguna IAM yang terpengaruh oleh perubahan, dan waktu acara.

Peran IAM yang diasumsikan teratas

Melacak peran IAM yang paling sering diasumsikan.

Dasbor aktivitas pengguna

Dasbor ini memberikan visibilitas ke tren aktivitas pengguna, wawasan tentang area utama seperti pengguna aktif teratas, pola lalu lintas pengguna, pengguna dengan kesalahan akses yang ditolak, operasi pengguna baru-baru ini, pengguna yang melakukan aktivitas destruktif dan perubahan kebijakan IAM, serta tindakan pengguna istimewa. Ini membantu mendeteksi tindakan pengguna yang tidak diinginkan dan risiko keamanan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Tren aktivitas pengguna menurut ARN pengguna

Melacak tren aktivitas pengguna dari waktu ke waktu oleh ARN pengguna.

Tren aktivitas pengguna berdasarkan API

Melacak tren aktivitas pengguna dari waktu ke waktu dengan API.

Aktivitas pengguna terbaru

Melacak tindakan pengguna terbaru.

Pengguna teratas dengan kesalahan

Melacak pengguna yang memiliki jumlah kesalahan tertinggi.

Pengguna teratas dengan AccessDenied kesalahan

Melacak pengguna yang memiliki jumlah AccessDenied kesalahan tertinggi.

Pengguna teratas melakukan tindakan destruktif

Melacak pengguna yang membuat jumlah tindakan destruktif tertinggi.

Pengguna teratas mengubah kebijakan IAM

Melacak pengguna IAM yang sering melakukan perubahan pada kebijakan IAM.

Tindakan teratas yang dilakukan oleh calon pengguna istimewa IAM

Melacak tindakan yang paling sering dilakukan oleh pengguna IAM yang sangat istimewa, seperti administrator.

Dasbor acara yang diperkaya

Dasbor acara yang diperkaya ini memberikan wawasan tentang tren di seluruh sumber daya yang ditandai, aktivitas utama, dan AWS kunci kondisi global. Wawasan ini membantu Anda menganalisis distribusi sumber daya dan tag utama yang paling sering digunakan serta kunci kondisi global yang sering digunakan dalam sesi peran, permintaan, dan prinsip dalam konteks permintaan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Acara yang diperkaya dari waktu ke waktu

Melacak hitungan peristiwa yang diperkaya dari waktu ke waktu.

Pasangan nilai kunci tag sumber daya yang paling sering

Menampilkan pasangan nilai kunci tag sumber daya yang paling sering digunakan di seluruh peristiwa yang diperkaya.

Pasangan nilai kunci tag sumber daya yang paling sering dengan sumber daya dan pengguna terkait

Menampilkan pasangan nilai kunci tag sumber daya yang paling sering digunakan, menunjukkan sumber daya mana yang menggunakan tag ini dan pengguna mana yang terkait dengannya.

Pasangan nilai kunci tag utama yang paling sering

Menampilkan pasangan nilai kunci tag utama yang paling sering digunakan di seluruh peristiwa yang diperkaya.

Akses yang paling sering ditolak tindakan yang dikelompokkan berdasarkan pasangan nilai kunci tag utama

Menampilkan tindakan penolakan akses yang paling sering dikelompokkan berdasarkan pasangan nilai kunci tag utama di seluruh peristiwa yang diperkaya.

Properti utama paling sering dalam kunci kondisi global IAM

Menampilkan kunci kondisi global IAM yang paling sering digunakan untuk properti utama, menunjukkan pasangan nilai kunci dan jumlah di semua peristiwa.

Properti permintaan paling sering di kunci kondisi global IAM

Menampilkan kunci kondisi global IAM yang paling sering digunakan untuk properti permintaan, menunjukkan pasangan nilai kunci dan jumlah di semua peristiwa.

Properti sesi peran paling sering dalam kunci kondisi global IAM

Menampilkan kunci kondisi global IAM yang paling sering digunakan untuk properti sesi peran, menampilkan pasangan nilai kunci dan jumlah mereka di semua peristiwa.

Dasbor analisis kesalahan

Dasbor ini memberikan wawasan komprehensif tentang tren kesalahan di seluruh layanan, API, pengguna, kode kesalahan, dan API yang dibatasi. Visibilitas memungkinkan identifikasi cepat dan pemecahan masalah potensi masalah ketersediaan untuk kinerja sistem yang optimal.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Jumlah kesalahan berdasarkan layanan

Melacak jumlah kesalahan aktivitas berdasarkan layanan.

Hitungan kesalahan berdasarkan API

Melacak jumlah kesalahan aktivitas berdasarkan API.

Kesalahan teratas dengan kode kesalahan

Melacak kesalahan yang paling sering dengan kode kesalahan.

Kesalahan teratas dengan pesan kesalahan

Melacak kesalahan yang paling sering dengan pesan kesalahan.

AccessDenied Kesalahan teratas berdasarkan API

Melacak API dengan kesalahan ditolak akses yang paling sering dilaporkan.

Kesalahan terhambat teratas oleh API

Melacak API dengan kesalahan terhambat yang paling sering dilaporkan.

Pengguna teratas dengan kesalahan

Melacak pengguna dengan kesalahan yang paling sering dilaporkan.

Dasbor aktivitas EC2

Dasbor ini memberikan visibilitas komprehensif ke dalam aktivitas manajemen EC2, seperti tren API, kesalahan akses, peluncur instans teratas, perubahan keamanan, dan modifikasi jaringan. Wawasan membantu mengidentifikasi risiko keamanan dan masalah operasional.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Ikhtisar aktivitas manajemen instans EC2

Memantau ikhtisar aktivitas manajemen instans EC2 selama waktu tertentu, menyoroti operasi utama seperti peluncuran, penghentian, dan penghentian.

Keberhasilan API EC2 vs tren kegagalan

Melacak tren kesuksesan dan panggilan API EC2 yang gagal dari waktu ke waktu.

Kesalahan EC2 teratas

Melacak kode kesalahan paling sering yang terjadi selama panggilan API EC2.

Acara EC2 AccessDenied teratas

Melacak API EC2 dengan kesalahan paling banyak ditolak akses.

Pengguna teratas meluncurkan instans EC2

Melacak pengguna yang paling aktif dalam meluncurkan instans EC2 baru.

EC2 terbaru SecurityGroup dan perubahan NetworkInterface

Melacak grup keamanan EC2 terbaru dan perubahan antarmuka jaringan.

Manajemen VPC terbaru dan perubahan tabel rute

Melacak aktivitas manajemen VPC terbaru dan perubahan tabel rute.

Tindakan EC2 terbaru oleh pengguna root

Melacak tindakan EC2 terbaru yang dilakukan oleh pengguna root dengan izin yang sangat istimewa.

Dasbor aktivitas Organizations

Dirancang untuk penyimpanan data acara organisasi, dasbor ini menawarkan visibilitas ke dalam aktivitas dan tren organisasi, termasuk wawasan tentang anggota aktif, manajemen akun, pola akses, perubahan kebijakan, dan layanan dan API teratas yang digunakan.

Dasbor ini tersedia untuk penyimpanan data acara organisasi dan mencakup widget berikut:

Tren aktivitas dalam organisasi

Melacak tren aktivitas keseluruhan di seluruh AWS Organizations organisasi dari waktu ke waktu, memberikan visibilitas ke periode tingkat aktivitas tinggi atau rendah.

Ringkasan manajemen akun anggota

Melacak distribusi aktivitas manajemen akun anggota dalam organisasi, dikategorikan berdasarkan jumlah setiap jenis aktivitas.

Layanan yang paling banyak digunakan di seluruh organisasi

Melacak Layanan AWS yang paling banyak digunakan di seluruh organisasi.

Akun paling aktif berdasarkan layanan

Melacak akun yang paling aktif menggunakan Layanan AWS di seluruh organisasi.

API yang paling banyak digunakan di seluruh organisasi

Menyoroti AWS API yang paling sering dipanggil di seluruh organisasi.

Akun anggota paling aktif

Melacak akun anggota dalam organisasi yang telah menunjukkan jumlah aktivitas tertinggi.

Akses tren kesalahan ditolak di seluruh organisasi

Melacak pola kesalahan akses yang ditolak yang terjadi dalam organisasi dari waktu ke waktu.

Akun dengan sebagian besar kesalahan akses ditolak

Melacak akun dalam organisasi yang telah mengalami jumlah kesalahan akses ditolak tertinggi.

Perubahan kebijakan kontrol layanan terbaru

Melacak perubahan terbaru yang dilakukan pada kebijakan kontrol layanan (SCP) dalam organisasi.

Dasbor perubahan sumber daya

Dasbor ini memberikan pandangan komprehensif tentang aktivitas manajemen sumber daya, memantau tren dalam penyediaan, penghapusan, dan modifikasi di seluruh layanan. Ini menyoroti perubahan penting, termasuk yang dilakukan melalui CloudFormation, secara manual, dan kebijakan seperti bucket S3 dan akses KMS.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Tren pembuatan dan penghapusan sumber daya

Melacak pembuatan dan penghapusan sumber daya dalam akun dari waktu ke waktu.

Pengguna teratas yang melakukan pembuatan sumber daya

Melacak pengguna yang paling aktif membuat sumber daya baru.

API teratas yang digunakan untuk pembuatan sumber daya

Melacak API yang paling sering digunakan untuk membuat sumber daya baru di dalam akun.

API teratas yang digunakan untuk penghapusan sumber daya

Melacak API yang paling sering digunakan untuk menghapus sumber daya dalam akun.

Sumber daya terbaru dibuat di luar CloudFormation

Melacak sumber daya baru yang dibuat di luar CloudFormation tata kelola, menekankan perubahan yang tidak dikelola melalui CloudFormation templat.

Perubahan sumber daya terbaru yang dilakukan menggunakan konsol

Melacak perubahan terbaru yang dilakukan pada sumber daya melalui file Konsol Manajemen AWS.

Perubahan akses bucket S3 terbaru

Melacak perubahan akses bucket S3 terbaru.

Perubahan akses kunci KMS terbaru

Melacak perubahan kebijakan utama KMS terbaru.

Dasbor ikhtisar peristiwa data

Dasbor ini menawarkan tampilan terpusat peristiwa data di penyimpanan data acara, termasuk tren aktivitas keseluruhan, layanan teratas, API, wilayah, API bidang data terbatas, dan pengguna pesawat data terkemuka. Dasbor ini membantu Anda memantau aktivitas API bidang data untuk audit dan pemecahan masalah.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data dan menyertakan widget berikut:

Tren peristiwa data keseluruhan

Melacak tren dalam peristiwa data keseluruhan yang terjadi dalam akun dari waktu ke waktu.

Layanan teratas yang menghasilkan peristiwa data

Melacak layanan yang menghasilkan volume aktivitas data tertinggi dalam akun.

API teratas yang menghasilkan peristiwa data

Melacak API yang menghasilkan volume aktivitas data tertinggi dalam akun.

Wilayah teratas yang menghasilkan peristiwa data

Melacak wilayah yang menghasilkan volume aktivitas data tertinggi dalam akun.

API bidang data terhambat teratas

Melacak API bidang data yang sering mengalami pelambatan di dalam akun.

Pengguna teratas API bidang data

Melacak pengguna teratas yang paling banyak menggunakan API bidang data di seluruh akun.

Dasbor peristiwa data Lambda

Dasbor ini menyediakan visibilitas ke aktivitas API bidang data Lambda, termasuk pengguna teratas, fungsi yang sering dipanggil, kesalahan API umum. Wawasan ini membantu Anda mengaudit penggunaan Lambda, mendeteksi kelainan, dan mengurangi risiko operasional atau keamanan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data Lambda dan menyertakan widget berikut:

Aktivitas API bidang data Lambda

Melacak tren aktivitas API bidang data Lambda dalam akun dari waktu ke waktu.

Lambda memanggil tren kesuksesan vs kegagalan

Melacak tren kesuksesan dan doa Lambda yang gagal dari waktu ke waktu.

Pengguna teratas pemanggilan Lambda

Melacak pengguna yang paling banyak menggunakan fungsi Lambda di seluruh akun.

Fungsi Lambda yang dipanggil teratas

Melacak fungsi Lambda yang paling sering dipanggil di dalam akun.

10 kesalahan API Lambda Invoke teratas

Melacak 10 kesalahan teratas yang ditemui selama panggilan API Lambda Invoke.

Sebagian besar pengguna pemanggilan Lambda yang terhambat

Melacak pengguna yang mengalami jumlah peristiwa pelambatan tertinggi untuk pemanggilan Lambda.

Dasbor peristiwa data DynamoDB

Dasbor ini menyediakan visibilitas ke aktivitas API bidang data DynamoDB, termasuk tren penggunaan, API teratas, dan pola pelambatan yang melibatkan pengguna dan tabel. Wawasan ini

membantu Anda mengaudit penggunaan DynamoDB, mendeteksi kelainan, dan mengurangi risiko operasional atau keamanan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data DynamoDB dan menyertakan widget berikut:

Aktivitas data akun DynamoDB

Melacak tren dalam peristiwa data DynamoDB yang terjadi dalam akun dari waktu ke waktu.

DynamoDB data plane API sukses vs tren kegagalan

Melacak tren keberhasilan dan kegagalan panggilan API pesawat data DynamoDB dari waktu ke waktu.

10 API bidang data DynamoDB teratas

Daftar 10 panggilan API bidang data DynamoDB teratas.

Pengguna teratas API bidang data DynamoDB

Melacak pengguna yang melakukan jumlah panggilan tertinggi ke DynamoDB data plane API dalam akun.

10 kesalahan API bidang data DynamoDB teratas

Melacak 10 kesalahan teratas dalam memanggil DynamoDB data plane API.

Sebagian besar pengguna API bidang data DynamoDB yang dibatasi

Melacak pengguna dengan throttling paling sering saat memanggil DynamoDB data plane API.

API bidang data DynamoDB yang dibatasi teratas

Melacak API bidang data DynamoDB yang sering mengalami pelambatan di dalam akun.

Tabel DynamoDB yang dibatasi atas

Melacak tabel DynamoDB yang mengalami tingkat pelambatan tertinggi dalam akun.

Dasbor peristiwa data S3

Dasbor ini memberikan visibilitas ke aktivitas API bidang data S3, termasuk tren penggunaan, objek S3 yang paling banyak diakses, pengguna S3 teratas, dan tindakan S3 teratas. Wawasan ini membantu Anda mengaudit penggunaan S3, mendeteksi kelainan, dan mengurangi risiko operasional atau keamanan.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data Amazon S3 dan menyertakan widget berikut:

Aktivitas akun S3

Melacak aktivitas akun S3.

Objek yang paling banyak diakses

Daftar objek S3 yang paling banyak diakses.

Pengguna teratas S3

Melacak pengguna S3 teratas.

Tindakan S3 teratas

Melacak tindakan S3 teratas.

Dasbor acara wawasan

Dasbor ini memberikan visibilitas ke dalam rincian keseluruhan peristiwa Wawasan berdasarkan jenis, serta pengguna dan layanan teratas yang menghasilkan jenis acara ini. Selain itu, ini menunjukkan hitungan harian peristiwa Wawasan dan pandangan historis 30 hari dari metrik Wawasan.

> **Note**
>
> - Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data peristiwa sumber, diperlukan waktu hingga 7 hari CloudTrail untuk menyampaikan acara Insights pertama, jika aktivitas yang tidak biasa terdeteksi.
> - Dasbor Insights Events hanya menampilkan informasi tentang peristiwa Wawasan yang dikumpulkan oleh penyimpanan data peristiwa yang dipilih, yang ditentukan oleh konfigurasi penyimpanan data peristiwa sumber. Misalnya, jika Anda mengonfigurasi penyimpanan data peristiwa sumber untuk mengaktifkan peristiwa Wawasan `ApiCallRateInsight` tetapi tidak`ApiErrorRateInsight`, Anda tidak akan melihat informasi tentang peristiwa Insights. `ApiErrorRateInsight`

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa Wawasan dan menyertakan widget berikut:

Jenis wawasan

Melacak peristiwa menurut jenis Wawasan.

Wawasan berdasarkan tanggal

Melacak acara Wawasan berdasarkan tanggal.

Tingkat panggilan API Wawasan berdasarkan sumber acara

Melacak Insights rate panggilan API menurut sumber peristiwa. Untuk melihat data widget ini, penyimpanan data peristiwa Insights Anda harus dikonfigurasi untuk mengumpulkan Wawasan tentang tingkat panggilan API.

Tingkat kesalahan API Wawasan berdasarkan sumber peristiwa

Melacak tingkat kesalahan API Wawasan menurut sumber peristiwa. Untuk melihat widget ini, penyimpanan data peristiwa Insights Anda harus dikonfigurasi untuk mengumpulkan Insights pada tingkat kesalahan API.

Wawasan oleh pengguna teratas

Daftar pengguna teratas dengan permintaan yang menghasilkan peristiwa Wawasan.

Insights acara

Daftar acara Wawasan terbaru.

Dasbor acara manajemen

Dasbor ini menyoroti wawasan tentang peristiwa yang ditolak akses, tindakan destruktif, peristiwa login konsol, kesalahan teratas menurut pengguna, penggunaan versi TLS, dan panggilan TLS yang sudah ketinggalan zaman oleh pengguna.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Akses teratas ditolak acara

Melacak peristiwa teratas yang mengakibatkan kesalahan akses ditolak.

Kesalahan teratas oleh pengguna

Melacak kesalahan teratas oleh pengguna.

Acara masuk konsol

Menampilkan acara login konsol.

Tindakan destruktif

Melacak tindakan yang menghasilkan tindakan destruktif.

Versi TLS

Menampilkan versi TLS.

Panggilan TLS usang oleh pengguna

Melacak panggilan menggunakan versi TLS yang sudah ketinggalan zaman oleh pengguna.

Dasbor ikhtisar

Dasbor ini menyoroti wawasan tentang peristiwa yang ditolak akses, tindakan destruktif, peristiwa login konsol, kesalahan teratas menurut pengguna, penggunaan versi TLS, dan panggilan TLS yang sudah ketinggalan zaman oleh pengguna.

Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen dan menyertakan widget berikut:

Aktivitas akun

Melacak aktivitas baca dan tulis untuk akun Anda.

Kesalahan teratas

Daftar kesalahan yang paling sering.

Wilayah paling aktif

Menunjukkan yang paling aktif Wilayah AWS.

Layanan teratas

Menunjukkan layanan teratas.

Sebagian besar peristiwa yang dibatasi

Daftar peristiwa yang paling dibatasi.

Pengguna teratas

Daftar pengguna teratas.

Aktifkan dasbor Sorotan dengan CloudTrail konsol

Aktifkan dasbor Sorotan untuk melihat ikhtisar sekilas tentang AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Dasbor Sorotan dikelola oleh CloudTrail dan menyertakan widget yang relevan dengan akun Anda. Widget yang ditampilkan di dasbor Sorotan unik untuk setiap akun. Widget ini dapat muncul aktivitas abnormal atau anomali yang terdeteksi. Misalnya, dasbor Sorotan Anda dapat menyertakan widget akses lintas akun Total, yang menunjukkan jika ada peningkatan aktivitas lintas akun yang tidak normal.

CloudTrail memperbarui dasbor Sorotan setiap 6 jam. Dasbor menunjukkan 24 jam terakhir data dari pembaruan terakhir.

> **Note**
>
> Anda hanya dapat mengaktifkan dasbor Sorotan untuk penyimpanan data acara yang ada di akun Anda.
> Anda tidak dapat mengatur jadwal penyegaran untuk dasbor Sorotan, atau menambah atau menghapus widget.

Untuk mengaktifkan dasbor Sorotan

Gunakan prosedur berikut untuk mengaktifkan dasbor Sorotan.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Sorotan.
4. Karena menjalankan kueri menimbulkan CloudTrail biaya, CloudTrail meminta Anda untuk meninjau informasi biaya sebelum mengaktifkan dasbor Sorotan. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

   Pilih Setuju dan aktifkan Sorotan untuk mengaktifkan dasbor Sorotan.
5. Untuk Izin, pilih penyimpanan data acara yang ingin Anda terapkan izin. CloudTrail memerlukan izin untuk menjalankan kueri di penyimpanan data acara Anda dan menyegarkan dasbor atas nama Anda. Untuk memberikan izin, CloudTrail melampirkan kebijakan berbasis sumber daya default ke setiap penyimpanan data peristiwa yang dipilih dalam langkah ini CloudTrail untuk memungkinkan menjalankan kueri di penyimpanan data peristiwa. CloudTrail melampirkan

kebijakan berbasis sumber daya ke dasbor untuk memungkinkan penyegaran dasbor setiap CloudTrail 6 jam.

Anda dapat mengubah kebijakan berbasis sumber daya untuk penyimpanan data peristiwa dari halaman detailnya. Anda dapat mengubah kebijakan berbasis sumber daya untuk dasbor dengan memilih Edit kebijakan dari menu Tindakan untuk dasbor.

6. Pilih Konfirmasi.

Saat Anda mengaktifkan dasbor Sorotan, perlindungan penghentian diaktifkan secara otomatis. Perlindungan penghentian melindungi dasbor agar tidak terhapus secara tidak sengaja. Anda harus menonaktifkan perlindungan terminasi, jika Anda ingin menonaktifkan dasbor.

Nonaktifkan dasbor Sorotan dengan CloudTrail konsol

Bagian ini menjelaskan cara menonaktifkan dasbor Sorotan. Karena perlindungan penghentian diaktifkan secara otomatis untuk dasbor Sorotan, Anda harus menonaktifkan perlindungan penghentian terlebih dahulu dan kemudian menonaktifkan dasbor Sorotan.

Untuk menonaktifkan dasbor Sorotan

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Sorotan.
4. Dari Tindakan, pilih Ubah perlindungan penghentian.
5. Pilih Dinonaktifkan.
6. Pilih Simpan.
7. Dari Tindakan, pilih Nonaktifkan Sorotan.

Buat dasbor khusus dengan CloudTrail konsol

Anda dapat membuat dasbor khusus dan menambahkan hingga 10 widget ke setiap dasbor khusus. Anda dapat memilih untuk menambahkan widget sampel atau membuat widget baru dari kueri SQL.

Setelah selesai menambahkan widget, Anda dapat menyegarkan dasbor secara manual atau mengatur jadwal penyegaran.

Untuk membuat dasbor khusus

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Pilih Bangun dasbor saya sendiri.
5. Berikan nama dasbor untuk mengidentifikasi dasbor Anda.
6. Untuk Izin, pilih penyimpanan data acara yang ingin Anda terapkan izin. Karena CloudTrail menjalankan kueri untuk mengisi data untuk widget di dasbor, CloudTrail memerlukan izin untuk menjalankan kueri pada penyimpanan data acara yang terkait dengan widget dasbor. Untuk setiap penyimpanan data peristiwa yang dipilih dalam langkah ini, CloudTrail melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa yang memungkinkan untuk menjalankan kueri pada penyimpanan data peristiwa CloudTrail untuk dasbor ini.
7. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi dan mengurutkan dasbor Anda. Untuk informasi selengkapnya tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya di Panduan Pengguna AWS Sumber Daya Penandaan.
8. Pilih Buat dasbor.

   Selanjutnya, Anda dapat menambahkan widget dan mengatur jadwal penyegaran.

Topik

- Tambahkan widget sampel dengan CloudTrail konsol
- Buat widget baru dari kueri SQL dengan konsol CloudTrail
- Hapus widget dari dasbor dengan CloudTrail konsol

Tambahkan widget sampel dengan CloudTrail konsol

Bagian ini menjelaskan cara menambahkan widget sampel ke dasbor Anda. Anda dapat menambahkan maksimal 10 widget ke dasbor khusus.

> **Note**
>
> Widget sampel terbatas pada penyimpanan data peristiwa tunggal yang ada di akun Anda. Untuk melakukan kueri di beberapa penyimpanan data acara di akun Anda, buat widget baru.

Untuk menambahkan widget sampel ke dasbor

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Di dasbor Kustom, pilih dasbor yang ingin Anda tambahkan widget.
5. Dari Tindakan, pilih Edit dasbor.
6. Dari Tindakan, pilih Tambahkan widget sampel.
7. Pilih penyimpanan data peristiwa tempat Anda ingin menjalankan kueri. Anda hanya dapat memilih penyimpanan data acara yang ada di akun Anda.
8. Pilih widget sampel yang ingin Anda tambahkan. Secara default, semua widget sampel ditampilkan. Anda dapat memfilter berdasarkan jenis widget (misalnya, widget IAM).
9. Pilih Lihat kueri untuk melihat kueri untuk widget yang dipilih.
10. Pilih Tambahkan ke dasbor untuk menambahkan widget ke dasbor.
11. Pilih Simpan untuk menyimpan dasbor.

Buat widget baru dari kueri SQL dengan konsol CloudTrail

Bagian ini menjelaskan cara membuat widget baru dengan menulis atau menempelkan kueri SQL dan memilih jenis bagan. Anda dapat menambahkan maksimal 10 widget ke dasbor khusus.

Untuk membuat widget baru dari kueri SQL

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Di dasbor Kustom, pilih dasbor yang ingin Anda buat widget.

5. Dari Tindakan, pilih Edit dasbor.
6. Dari Tindakan, pilih Buat widget baru.
7. Pilih penyimpanan data peristiwa tempat Anda ingin menjalankan kueri. Anda dapat melakukan kueri di beberapa penyimpanan data peristiwa selama penyimpanan data acara ada di akun Anda.
8. Tulis atau salin kueri SQL.

   Anda juga dapat memberikan prompt bahasa alami dalam bahasa Inggris dan memilih Hasilkan kueri untuk menghasilkan kueri SQL dari prompt Anda. Untuk informasi selengkapnya, lihat Buat kueri CloudTrail Danau dari petunjuk bahasa alami.
9. Pilih Jalankan untuk menjalankan kueri dan melakukan pratinjau hasil kueri.

   > **Note**
   >
   > Saat menjalankan kueri, Anda dikenakan biaya berdasarkan jumlah data yang dioptimalkan dan dikompresi yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan `eventTime` stempel waktu awal dan akhir ke kueri.
10. Pilih tab Visualizer untuk memilih jenis bagan untuk widget. Anda dapat memilih dari jenis bagan ini: tabel, bagan batang, bagan garis, dan diagram lingkaran.
11. Pilih Tambahkan ke dasbor untuk menambahkan widget ke dasbor.
12. Pilih Simpan untuk menyimpan dasbor.

Hapus widget dari dasbor dengan CloudTrail konsol

Bagian ini menjelaskan untuk menghapus widget dari dasbor khusus.

Untuk menghapus widget dari dasbor

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Di dasbor khusus, pilih dasbor yang ingin Anda hapus widgetnya.
5. Dari Tindakan, pilih Edit dasbor.

6. Pada widget yang ingin Anda hapus, pilih ikon hapus
   ( )
   dan kemudian pilih Hapus.
7. Pilih Simpan untuk menyimpan dasbor.

Tetapkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol

Bagian ini menjelaskan cara mengatur jadwal penyegaran dasbor. Anda dapat mengatur jadwal penyegaran agar CloudTrail Lake menyegarkan dasbor setiap 1 jam, 6 jam, 12 jam, atau 24 jam (1 hari).

Saat Anda menetapkan jadwal penyegaran menggunakan CloudTrail konsol, CloudTrail lampirkan kebijakan berbasis sumber daya ke dasbor yang memungkinkan CloudTrail untuk menyegarkan dasbor atas nama Anda.

Untuk mengatur jadwal penyegaran

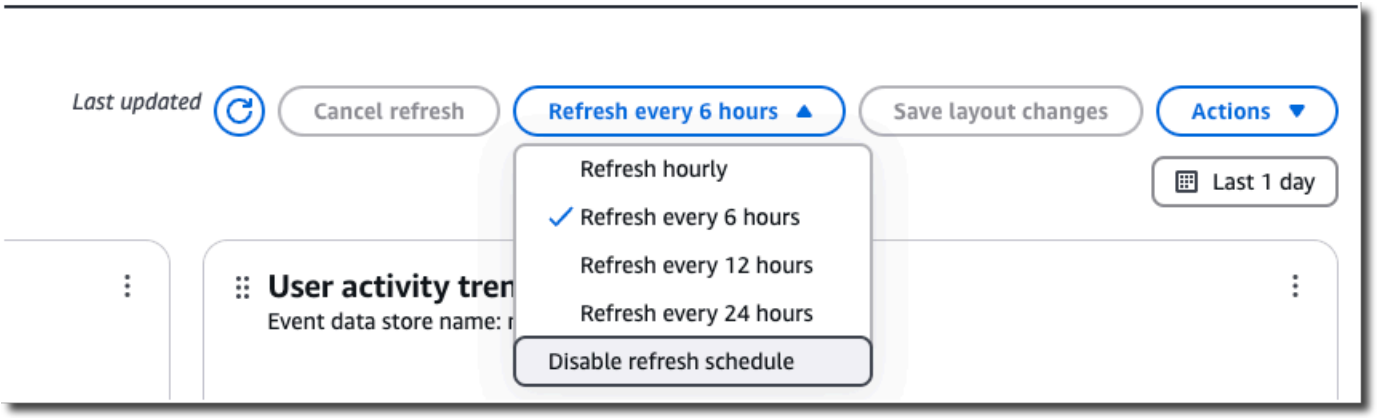
1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Di dasbor khusus, pilih dasbor yang ingin Anda atur jadwal penyegaran.
5. Pilih frekuensi refresh dari daftar dropdown.
6. Untuk membuat jadwal penyegaran, CloudTrail lampirkan kebijakan berbasis sumber daya ke dasbor CloudTrail untuk memungkinkan menyegarkan dasbor atas nama Anda. Perluas kebijakan sumber daya Dasbor untuk melihat kebijakan berbasis sumber daya yang CloudTrail akan dilampirkan ke dasbor.
7. Karena menjalankan kueri menimbulkan biaya, CloudTrail meminta Anda untuk mengonfirmasi bahwa Anda ingin menjalankan kueri CloudTrail untuk frekuensi yang dijadwalkan. Pilih Konfirmasi untuk mengatur jadwal penyegaran.

Nonaktifkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol

Anda dapat menonaktifkan jadwal penyegaran jika Anda tidak lagi CloudTrail ingin menyegarkan dasbor secara otomatis, dan sebagai gantinya ingin menyegarkan dasbor Anda secara manual.

Untuk menonaktifkan jadwal penyegaran

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Di dasbor khusus, pilih dasbor yang ingin Anda nonaktifkan jadwal penyegaran.
5. Pilih Nonaktifkan jadwal penyegaran dari daftar dropdown.



Ubah perlindungan terminasi dengan CloudTrail konsol

Perlindungan penghentian mencegah dasbor dari penghapusan yang tidak disengaja. Jika Anda ingin menghapus dasbor khusus, atau menonaktifkan dasbor Sorotan, Anda harus menonaktifkan perlindungan penghentian.

Untuk mematikan perlindungan terminasi

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Danau, pilih Dasbor.
3. Pilih dasbor yang ingin Anda nonaktifkan perlindungan terminasi.

4. Dari Tindakan, pilih Ubah perlindungan penghentian.
5. Pilih Dinonaktifkan.
6. Pilih Simpan.

Untuk mengaktifkan perlindungan terminasi

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Danau, pilih Dasbor.
3. Pilih dasbor yang ingin Anda aktifkan perlindungan terminasi.
4. Dari Tindakan, pilih Ubah perlindungan penghentian.
5. Untuk mengaktifkan perlindungan penghentian, pilih Diaktifkan.
6. Pilih Simpan.

Hapus dasbor khusus dengan CloudTrail konsol

Bagian ini menjelaskan cara menghapus dasbor menggunakan CloudTrail.

> **Note**
>
> Anda tidak dapat menghapus penyimpanan data peristiwa jika perlindungan penghentian diaktifkan.

Untuk menghapus dasbor

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, di bawah Danau, pilih Dasbor.
3. Pilih tab Dasbor Terkelola dan kustom.
4. Pilih dasbor khusus yang ingin Anda hapus.
5. Dari Tindakan, pilih Hapus.
6. Pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus dasbor.

Buat, perbarui, dan kelola dasbor dengan AWS CLI

Bagian ini menjelaskan AWS CLI perintah yang dapat Anda gunakan untuk membuat, memperbarui, dan mengelola dasbor CloudTrail Danau Anda.

Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter `--region` bersama perintah tersebut.

Perintah yang tersedia untuk dasbor

Perintah untuk membuat dan memperbarui dasbor di CloudTrail Lake meliputi:

- `create-dashboard`untuk membuat dasbor khusus atau mengaktifkan dasbor Sorotan.
- `update-dashboard`untuk memperbarui dasbor khusus atau dasbor Sorotan.
- `delete-dashboard`untuk menghapus dasbor khusus atau dasbor Sorotan.
- `get-dashboard`mengembalikan informasi tentang dasbor yang ditentukan.
- `list-dashboards`daftar semua dasbor untuk Anda Akun AWS, atau untuk filter yang ditentukan.
- `start-dashboard-refresh`memulai penyegaran dasbor.
- `get-resource-policy`mendapatkan kebijakan berbasis sumber daya yang dilampirkan ke dasbor.
- `put-resource-policy`melampirkan kebijakan berbasis sumber daya ke dasbor untuk memungkinkan CloudTrail penyegaran dasbor secara asinkron atas nama Anda. Anda juga melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa untuk memungkinkan menjalankan kueri di penyimpanan data acara CloudTrail untuk mengisi data untuk widget dasbor.
- `delete-resource-policy`menghapus kebijakan berbasis sumber daya yang dilampirkan ke dasbor.
- `add-tags`menambahkan tag untuk mengidentifikasi dasbor.
- `remove-tags`menghapus tag dari dasbor.
- `list-tags`daftar tag untuk dasbor.

Untuk daftar perintah yang tersedia untuk penyimpanan data acara CloudTrail Lake, lihatPerintah yang tersedia untuk penyimpanan data acara.

Untuk daftar perintah yang tersedia untuk kueri CloudTrail Lake, lihatPerintah yang tersedia untuk kueri CloudTrail Lake.

Untuk daftar perintah yang tersedia untuk integrasi CloudTrail Lake, lihatPerintah yang tersedia untuk integrasi CloudTrail Lake.

Topik:

- Buat dasbor dengan AWS CLI
- Kelola dasbor dengan AWS CLI
- Hapus dasbor dengan AWS CLI

Buat dasbor dengan AWS CLI

Bagian ini menjelaskan cara menggunakan `create-dashboard` perintah untuk membuat dasbor kustom atau dasbor Sorotan.

Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter `--region` bersama perintah tersebut.

CloudTrail menjalankan kueri untuk mengisi widget dasbor selama penyegaran manual atau terjadwal. CloudTrail harus diberikan izin untuk menjalankan `StartQuery` operasi pada setiap penyimpanan data peristiwa yang terkait dengan widget dasbor. Untuk memberikan izin, jalankan `put-resource-policy` perintah untuk melampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa, atau edit kebijakan penyimpanan data peristiwa di konsol. CloudTrail Untuk contoh kebijakan, lihat Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor.

Untuk mengatur jadwal penyegaran, CloudTrail harus diberikan izin untuk menjalankan `StartDashboardRefresh` operasi untuk menyegarkan dasbor atas nama Anda. Untuk memberikan izin, jalankan `put-resource-policy` operasi untuk melampirkan kebijakan berbasis sumber daya ke dasbor, atau edit kebijakan dasbor di konsol. CloudTrail Untuk contoh kebijakan, lihat Resource-based contoh kebijakan untuk dasbor.

Contoh:

- Buat dasbor khusus dengan AWS CLI
- Aktifkan dasbor Sorotan dengan AWS CLI

- Lihat properti untuk widget

Buat dasbor khusus dengan AWS CLI

Prosedur berikut menunjukkan cara membuat dasbor khusus, melampirkan kebijakan berbasis sumber daya yang diperlukan ke penyimpanan data peristiwa dan dasbor, dan memperbarui dasbor untuk mengatur dan mengaktifkan jadwal penyegaran.

1. Jalankan `create-dashboard` untuk membuat dasbor.

   Saat Anda membuat dasbor khusus, Anda dapat meneruskan array dengan hingga 10 widget. Widget menyediakan representasi grafis dari hasil untuk kueri. Setiap widget terdiri dari`ViewProperties`,`QueryStatement`, dan`QueryParameters`.

   - `ViewProperties`- Menentukan properti untuk jenis tampilan. Untuk informasi selengkapnya, lihat Lihat properti untuk widget.
   - `QueryStatement`— Kueri CloudTrail berjalan saat dasbor di-refresh. Anda dapat melakukan kueri di beberapa penyimpanan data peristiwa selama penyimpanan data acara ada di akun Anda.
   - `QueryParameters`— `QueryParameters` Nilai-nilai berikut didukung untuk dasbor kustom:`$Period$`,`$StartTime$`, dan`$EndTime$`. Untuk menggunakan `QueryParameters` place a `?` di `QueryStatement` mana Anda ingin mengganti parameter. CloudTrail akan mengisi parameter saat kueri dijalankan.

   Contoh berikut membuat dashboard dengan empat widget, salah satu dari setiap jenis tampilan.

   > **Note**
   >
   > Dalam contoh ini, `?` dikelilingi dengan tanda kutip tunggal karena digunakan dengan`eventTime`. Bergantung pada sistem operasi yang Anda jalankan, Anda mungkin perlu mengelilingi tanda kutip tunggal dengan tanda kutip melarikan diri. Untuk informasi selengkapnya, lihat Menggunakan tanda kutip dan literal dengan string di. AWS CLI

```
aws cloudtrail create-dashboard --name AccountActivityDashboard \
--widgets '[
```

```
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT
100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "AccountActivity",
        "View": "LineChart",
        "YAxisColumn": "eventCount",
        "XAxisColumn": "eventDate",
        "FilterColumn": "readOnly"
      },
      "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate,
IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly
ORDER BY DATE_TRUNC('?', eventTime), readOnly",
      "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$",
"$Period$"]
    },
```

```
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Horizontal"
      },
      "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
 ]'
```

2. Buat file terpisah dengan kebijakan sumber daya yang diperlukan untuk setiap penyimpanan data peristiwa yang disertakan dalam widget`QueryStatement`. Beri nama file*`policy.json`*, dengan contoh pernyataan kebijakan berikut:

   Ganti *`123456789012`* dengan ID akun Anda, *`arn:aws:cloudtrail:us-east-1:123456789012:dashboard/exampleDashboard`* dengan ARN dasbor.

   Untuk informasi selengkapnya tentang kebijakan berbasis sumber daya untuk dasbor, lihat. Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor

3. Jalankan `put-resource-policy` perintah untuk melampirkan kebijakan. Anda juga dapat memperbarui kebijakan berbasis sumber daya penyimpanan data peristiwa di konsol. CloudTrail

   Contoh berikut melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa.

   ```
   aws cloudtrail put-resource-policy \
   --resource-arn eds-arn \
   --resource-policy file://policy.json
   ```

4. Jalankan `put-resource-policy` perintah untuk melampirkan kebijakan berbasis sumber daya ke dasbor. Untuk contoh kebijakan, lihat Resource-based contoh kebijakan untuk dasbor.

   Contoh berikut melampirkan kebijakan berbasis sumber daya ke dasbor. Ganti *`account-id`* dengan ID akun Anda dan *`dashboard-arn`* dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

5. Jalankan `update-dashboard` perintah untuk mengatur dan mengaktifkan jadwal penyegaran dengan mengonfigurasi `--refresh-schedule` parameter.

   `--refresh-schedule`Terdiri dari parameter opsional berikut:

   - `Frequency`— `Value` Untuk `Unit` dan untuk jadwal.

     Untuk dasbor khusus, unit dapat berupa `HOURS` atau`DAYS`.

     Untuk dasbor kustom, nilai berikut valid ketika unit adalah`HOURS`:`1`,,`6`, `12` `24`

     Untuk dasbor khusus, satu-satunya nilai yang valid saat unit `DAYS` adalah`1`.
   - `Status`- Menentukan apakah jadwal refresh diaktifkan. Tetapkan nilainya `ENABLED` untuk mengaktifkan jadwal penyegaran, atau `DISABLED` untuk mematikan jadwal penyegaran.
   - `TimeOfDay` — Waktu hari di UTC untuk menjalankan jadwal; untuk per jam hanya mengacu pada menit; default adalah 00:00.

   Contoh berikut menetapkan jadwal refresh untuk setiap enam jam dan memungkinkan jadwal.

   ```
   aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
   --refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
    "ENABLED"}'
   ```

Aktifkan dasbor Sorotan dengan AWS CLI

Prosedur berikut menunjukkan cara membuat dasbor Sorotan, melampirkan kebijakan berbasis sumber daya yang diperlukan ke penyimpanan data acara dan dasbor, dan memperbarui dasbor untuk mengatur dan mengaktifkan jadwal penyegaran.

1. Jalankan `create-dashboard` perintah untuk membuat dasbor Sorotan. Untuk membuat dasbor ini, `--name` harus`AWSCloudTrail-Highlights`.

```
aws cloudtrail create-dashboard --name AWSCloudTrail-Highlights
```

2. Untuk setiap penyimpanan data peristiwa di akun Anda, jalankan `put-resource-policy` perintah untuk melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa. Anda juga dapat memperbarui kebijakan berbasis sumber daya penyimpanan data peristiwa di konsol. CloudTrail Untuk contoh kebijakan, lihat Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor.

   Contoh berikut melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa. Ganti *`account-id`* dengan ID akun Anda, *`eds-arn`* dengan ARN penyimpanan data acara, dan *`dashboard-arn`* dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "EDSPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartQuery", "Condition":
 { "StringEquals": { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount":
 "account-id"}}} ]}'
```

3. Jalankan `put-resource-policy` perintah untuk melampirkan kebijakan berbasis sumber daya ke dasbor. Untuk contoh kebijakan, lihat Resource-based contoh kebijakan untuk dasbor.

   Contoh berikut melampirkan kebijakan berbasis sumber daya ke dasbor. Ganti *`account-id`* dengan ID akun Anda dan *`dashboard-arn`* dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. Jalankan `update-dashboard` perintah untuk mengatur dan mengaktifkan jadwal penyegaran dengan mengonfigurasi `--refresh-schedule` parameter. Untuk dasbor Sorotan, satu-satunya yang valid `UNIT` adalah `HOURS` dan satu-satunya yang valid `Value` adalah`6`.

```
aws cloudtrail update-dashboard --dashboard-id AWSCloudTrail-Highlights \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

Lihat properti untuk widget

Bagian ini menjelaskan properti tampilan yang dapat dikonfigurasi untuk 4 jenis tampilan: tabel, bagan garis, diagram lingkaran, dan bagan batang.

Lihat jenis:

- Tabel
- Bagan garis
- Bagan pai
- Bagan batang

Tabel

Contoh berikut menunjukkan widget dikonfigurasi sebagai tabel.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopErrors",
       "View": "Table"
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

Tabel berikut menjelaskan properti tampilan dikonfigurasi untuk tabel.

Parameter	Diperlukan	Nilai
`Height`	Ya	Ketinggian meja dalam inci.

Parameter	Diperlukan	Nilai
`Width`	Ya	Lebar meja dalam inci.
`Title`	Ya	Judul tabel.
`View`	Ya	Jenis tampilan widget. Untuk tabel, nilainya adalah`Table`.

Bagan garis

Contoh berikut menunjukkan widget dikonfigurasi sebagai grafik garis.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "AccountActivity",
       "View": "LineChart",
       "YAxisColumn": "eventCount",
       "XAxisColumn": "eventDate",
       "FilterColumn": "readOnly"
    },
    "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate, IF(readOnly,
 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE eventTime >
 '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly ORDER BY
 DATE_TRUNC('?', eventTime), readOnly",
    "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$", "$Period$"]
}
```

Tabel berikut menjelaskan properti tampilan dikonfigurasi untuk bagan garis.

Parameter	Diperlukan	Nilai
`Height`	Ya	Ketinggian grafik garis dalam inci.
`Width`	Ya	Lebar grafik garis dalam inci.
`Title`	Ya	Judul grafik garis.

Parameter	Diperlukan	Nilai
`View`	Ya	Jenis tampilan widget. Untuk grafik garis, nilainya adalah`LineChart` .
`YAxisColumn`	Ya	Bidang dari hasil kueri yang ingin Anda gunakan untuk kolom sumbu Y. Misalnya, `eventCount` .
`XAxisColumn`	Ya	Bidang dari hasil kueri yang ingin Anda gunakan untuk kolom sumbu X. Misalnya, `eventDate` .
`FilterColumn`	Tidak	Bidang dari hasil kueri yang ingin Anda filter. Misalnya, `readOnly`.

Bagan pai

Contoh berikut menunjukkan widget dikonfigurasi sebagai diagram lingkaran.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "MostActiveRegions",
       "View": "PieChart",
       "LabelColumn": "awsRegion",
       "ValueColumn": "eventCount",
       "FilterColumn": "awsRegion"
    },
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

Tabel berikut menjelaskan properti tampilan dikonfigurasi untuk diagram lingkaran.

Parameter	Diperlukan	Nilai
`Height`	Ya	Ketinggian diagram lingkaran dalam inci.
`Width`	Ya	Lebar diagram lingkaran dalam inci.
`Title`	Ya	Judul diagram lingkaran.
`View`	Ya	Jenis tampilan widget. Untuk diagram lingkaran, nilainya adalah`PieChart`.
`LabelColumn`	Ya	Label untuk segmen dalam diagram lingkaran. Misalnya, `awsRegion` .
`ValueColumn`	Ya	Nilai untuk segmen dalam diagram lingkaran. Misalnya, `ValueColumn` .
`FilterColumn`	Tidak	Bidang dari hasil kueri yang ingin Anda filter. Misalnya, `awsRegion` .

Bagan batang

Contoh berikut menunjukkan widget dikonfigurasi sebagai bar chart.

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Horizontal"
```

```
    },
    "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
 COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

Tabel berikut menjelaskan properti tampilan dikonfigurasi untuk diagram batang.

Parameter	Diperlukan	Nilai
`Height`	Ya	Ketinggian grafik batang dalam inci.
`Width`	Ya	Lebar bar chart dalam inci.
`Title`	Ya	Judul bar chart.
`View`	Ya	Jenis tampilan widget. Untuk diagram batang, nilainya adalah`BarChart`.
`LabelColumn`	Ya	Label untuk bar di bar chart. Misalnya, `service`.
`ValueColumn`	Ya	Nilai untuk bar di bar chart. Misalnya, `eventCount` .
`FilterColumn`	Tidak	Bidang dari hasil kueri yang ingin Anda filter. Misalnya, `service`.
`Orientation`	Tidak	Orientasi diagram batang, salah satu `Horizontal` atau`Vertical`.

Kelola dasbor dengan AWS CLI

Bagian ini menjelaskan beberapa perintah lain yang dapat Anda jalankan untuk mengelola dasbor Anda, termasuk mendapatkan dasbor, mencantumkan dasbor Anda, menyegarkan dasbor, dan memperbarui dasbor.

Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter `--region` bersama perintah tersebut.

Contoh:

- Dapatkan dasbor dengan AWS CLI
- Daftar dasbor dengan AWS CLI
- Lampirkan kebijakan berbasis sumber daya ke penyimpanan data acara atau dasbor dengan AWS CLI
- Segarkan dasbor secara manual dengan AWS CLI
- Perbarui dasbor dengan AWS CLI

Dapatkan dasbor dengan AWS CLI

Jalankan `get-dashboard` perintah untuk mengembalikan dasbor. Tentukan `--dashboard-id` dengan memberikan dasbor ARN, atau nama dasbor.

```
aws cloudtrail get-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

Daftar dasbor dengan AWS CLI

Jalankan `list-dashboards` perintah untuk membuat daftar dasbor untuk akun Anda.

- Sertakan `--type` parameter, untuk melihat hanya `MANAGED` dasbor `CUSTOM` atau.
- Sertakan `--max-results` parameter untuk membatasi jumlah hasil. Nilai yang valid adalah 1-100.
- Sertakan dasbor `--name-prefix` untuk mengembalikan yang cocok dengan awalan yang ditentukan.

Contoh berikut mencantumkan semua dasbor.

```
aws cloudtrail list-dashboards
```

Contoh ini hanya mencantumkan `CUSTOM` dasbor.

```
aws cloudtrail list-dashboards --type CUSTOM
```

Contoh berikutnya hanya mencantumkan `MANAGED` dasbor.

```
aws cloudtrail list-dashboards --type MANAGED
```

Contoh terakhir mencantumkan dasbor yang cocok dengan awalan yang ditentukan.

```
aws cloudtrail list-dashboards --name-prefix ExamplePrefix
```

Lampirkan kebijakan berbasis sumber daya ke penyimpanan data acara atau dasbor dengan AWS CLI

Jalankan `put-resource-policy` perintah untuk menerapkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa atau dasbor.

Lampirkan kebijakan berbasis sumber daya ke penyimpanan data acara

Untuk menjalankan kueri di dasbor selama penyegaran manual atau terjadwal, Anda perlu melampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa yang terkait dengan widget di dasbor. Hal ini memungkinkan CloudTrail Lake untuk menjalankan kueri atas nama Anda. Untuk informasi selengkapnya tentang kebijakan berbasis sumber daya, lihat. Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor

Contoh berikut melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa. Ganti *account-id* dengan ID akun Anda, *eds-arn* dengan ARN penyimpanan data acara yang CloudTrail akan menjalankan kueri, dan *dashboard-arn* dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartQuery", "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-
arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

Lampirkan kebijakan berbasis sumber daya ke dasbor

Untuk mengatur jadwal penyegaran dasbor, Anda perlu melampirkan kebijakan berbasis sumber daya ke dasbor untuk memungkinkan CloudTrail Lake menyegarkan dasbor atas nama Anda. Untuk informasi selengkapnya tentang kebijakan berbasis sumber daya, lihat. Resource-based contoh kebijakan untuk dasbor

Contoh berikut melampirkan kebijakan berbasis sumber daya ke dasbor. Ganti *account-id* dengan ID akun Anda dan *dashboard-arn* dengan ARN dasbor.

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

Segarkan dasbor secara manual dengan AWS CLI

Jalankan `start-dashboard-refresh` perintah untuk menyegarkan dasbor secara manual. Sebelum Anda dapat menjalankan perintah ini, Anda harus melampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa yang terkait dengan widget dasbor.

Contoh berikut menunjukkan cara menyegarkan dasbor kustom secara manual.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id  dashboard-id \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z"}'
```

Contoh berikutnya menunjukkan cara menyegarkan dasbor terkelola secara manual. Karena dasbor terkelola dikonfigurasi oleh CloudTrail, permintaan penyegaran harus menyertakan ID penyimpanan data peristiwa tempat kueri akan dijalankan.

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id dashboard-id  \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z", "$EventDataStoreId
$": "eds-id"}'
```

Perbarui dasbor dengan AWS CLI

Jalankan `update-dashboard` perintah untuk memperbarui dasbor. Anda dapat memperbarui dasbor untuk mengatur jadwal penyegaran, mengaktifkan atau menonaktifkan jadwal penyegaran, memodifikasi widget, dan mengaktifkan atau menonaktifkan perlindungan penghentian.

Perbarui jadwal penyegaran dengan AWS CLI

Contoh berikut memperbarui jadwal penyegaran untuk dasbor kustom bernama`AccountActivityDashboard`.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status": "ENABLED"}'
```

Nonaktifkan perlindungan penghentian dan jadwal penyegaran di dasbor khusus dengan AWS CLI

Contoh berikut menonaktifkan perlindungan terminasi untuk dasbor khusus bernama `AccountActivityDashboard` untuk memungkinkan dasbor dihapus. Ini juga mematikan jadwal penyegaran.

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{ "Status": "DISABLED"}' \
--no-termination-protection-enabled
```

Tambahkan widget ke dasbor khusus

Contoh berikut menambahkan widget baru bernama `TopServices` ke dashboard kustom bernama`AccountActivityDashboard`. Array widget mencakup dua widget yang sudah dibuat untuk dasbor dan widget baru.

> **Note**
>
> Dalam contoh ini, ? dikelilingi dengan tanda kutip tunggal karena digunakan dengan`eventTime`. Bergantung pada sistem operasi yang Anda jalankan, Anda mungkin perlu mengelilingi tanda kutip tunggal dengan tanda kutip melarikan diri. Untuk informasi selengkapnya, lihat Menggunakan tanda kutip dan literal dengan string di. AWS CLI

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--widgets '[
```

```
   {
     "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopErrors",
       "View": "Table"
     },
     "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
ORDER BY eventCount DESC LIMIT 100",
     "QueryParameters": ["$StartTime$", "$EndTime$"]
   },
   {
     "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "MostActiveRegions",
       "View": "PieChart",
       "LabelColumn": "awsRegion",
       "ValueColumn": "eventCount",
       "FilterColumn": "awsRegion"
     },
     "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
     "QueryParameters": ["$StartTime$", "$EndTime$"]
   },
   {
     "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Vertical"
     },
     "QueryStatement": "SELECT replace(eventSource, '.amazonaws.com') AS service,
COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
     "QueryParameters": ["$StartTime$", "$EndTime$"]
   }
 ]'
```

Hapus dasbor dengan AWS CLI

Bagian ini menjelaskan cara menggunakan AWS CLI `delete-dashboard` perintah untuk menghapus dasbor CloudTrail Lake.

Untuk menghapus dasbor, tentukan `--dashboard-id` dengan memberikan dasbor ARN, atau nama dasbor.

```
aws cloudtrail delete-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

Tidak ada respon jika operasi berhasil.

> **Note**
>
> Anda tidak dapat menghapus dasbor jika `--termination-protection-enabled` disetel.

CloudTrail Pertanyaan danau

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Pertanyaan di CloudTrail Lake ditulis dalam SQL. Anda dapat membuat kueri di tab CloudTrail Lake Editor dengan menulis kueri di SQL dari awal, dengan membuka kueri yang disimpan atau sampel dan mengeditnya, atau dengan menggunakan generator kueri untuk menghasilkan kueri dari prompt bahasa Inggris. Anda tidak dapat menimpa kueri sampel yang disertakan dengan perubahan Anda, tetapi Anda dapat menyimpannya sebagai kueri baru. Untuk informasi selengkapnya tentang bahasa kueri SQL yang diizinkan, lihatCloudTrail Kendala Lake SQL.

Kueri tak terbatas (seperti`SELECT * FROM edsID`) memindai semua data di penyimpanan data acara Anda. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan

menambahkan stempel `eventTime` waktu mulai dan berakhir ke kueri. Berikut ini adalah contoh yang mencari semua peristiwa di penyimpanan data acara tertentu di mana waktu acara setelah (>) 5 Januari 2023 pukul 13:51 dan sebelum (<) 19 Januari 2023 pukul 1:51 siang. Karena penyimpanan data peristiwa memiliki periode retensi minimum tujuh hari, rentang waktu minimum antara `eventTime` nilai awal dan akhir juga tujuh hari.

```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

Untuk informasi tentang cara mengoptimalkan kueri Anda, lihatOptimalkan kueri CloudTrail Danau.

Topik

- Alat editor kueri
- Buat kueri CloudTrail Danau dari petunjuk bahasa alami
- Lihat contoh kueri dengan konsol CloudTrail
- Membuat atau mengedit kueri dengan CloudTrail konsol
- Jalankan kueri dan simpan hasil kueri dengan konsol
- Lihat hasil kueri dengan konsol
- Meringkas hasil kueri dalam bahasa alami
- Unduh hasil kueri yang disimpan
- Validasi hasil kueri yang disimpan CloudTrail Lake
- Optimalkan kueri CloudTrail Danau
- Jalankan dan kelola kueri CloudTrail Lake dengan AWS CLI

Alat editor kueri

Toolbar di kanan atas editor kueri menawarkan perintah untuk membantu penulis dan memformat kueri SQL Anda.



Daftar berikut menjelaskan perintah pada toolbar.

- Undo - Mengembalikan perubahan konten terakhir yang dibuat di editor kueri.
- Redo — Mengulangi perubahan konten terakhir yang dibuat di editor kueri.
- Format yang dipilih - Mengatur konten editor kueri sesuai dengan pemformatan SQL dan konvensi spasi.
- Comment/uncomment selected - Komentar bagian yang dipilih dari query jika belum dikomentari. Jika bagian yang dipilih sudah dikomentari, memilih opsi ini akan menghapus komentar.

Buat kueri CloudTrail Danau dari petunjuk bahasa alami

Anda dapat menggunakan generator kueri CloudTrail Lake untuk menghasilkan kueri dari prompt bahasa Inggris yang Anda berikan. Generator kueri menggunakan kecerdasan buatan generatif (AI generatif) untuk menghasilkan kueri SQL siap pakai dari prompt Anda, yang kemudian dapat Anda pilih untuk dijalankan di editor kueri Lake, atau selengkapnya. Anda tidak perlu memiliki pengetahuan luas tentang SQL atau bidang CloudTrail acara untuk menggunakan generator kueri.

Prompt dapat berupa pertanyaan atau pernyataan tentang data acara di penyimpanan data acara CloudTrail Lake Anda. Misalnya, Anda dapat memasukkan petunjuk seperti "What are my top errors in the past month?" dan “Give me a list of users that used SNS.”

Prompt dapat memiliki minimal 3 karakter dan maksimal 500 karakter.

Tidak ada biaya untuk menghasilkan kueri; Namun, ketika Anda menjalankan kueri, Anda dikenakan biaya berdasarkan jumlah data yang dioptimalkan dan dikompresi yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan `eventTime` stempel waktu awal dan akhir ke kueri.

> **Note**
>
> Anda dapat memberikan umpan balik tentang kueri yang dihasilkan dengan memilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah kueri yang dihasilkan. Saat Anda memberikan umpan balik, CloudTrail menyimpan prompt Anda dan kueri yang dihasilkan. Jangan sertakan informasi identitas pribadi, rahasia, atau sensitif apa pun dalam permintaan Anda.
> Fitur ini menggunakan model bahasa besar AI generatif (LLM); kami merekomendasikan untuk memeriksa ulang respons LLM.

> **Note**
>
> CloudTrail akan secara otomatis memilih wilayah optimal dalam geografi Anda untuk memproses permintaan inferensi sambil menghasilkan kueri. Ini memaksimalkan sumber daya komputasi yang tersedia, ketersediaan model, dan memberikan pengalaman pelanggan terbaik. Data Anda akan tetap disimpan hanya di wilayah tempat permintaan berasal, namun, permintaan input dan hasil keluaran dapat diproses di luar wilayah tersebut. Semua data akan dikirimkan dienkripsi di seluruh jaringan aman Amazon.
> CloudTrail akan dengan aman merutekan permintaan inferensi Anda ke sumber daya komputasi yang tersedia dalam wilayah geografis tempat permintaan tersebut berasal, sebagai berikut:
>
> - Permintaan inferensi yang berasal dari Amerika Serikat akan diproses di Amerika Serikat
> - Permintaan inferensi yang berasal dari Jepang akan diproses di Jepang
> - Permintaan inferensi yang berasal dari Australia akan diproses di Australia.
> - Permintaan inferensi yang berasal dari Uni Eropa akan diproses di dalam Uni Eropa
> - Permintaan inferensi yang berasal dari India akan diproses di India
>
> Untuk memilih keluar dari fitur pembuatan kueri, Anda dapat secara eksplisit menolak atau menghapus `cloudtrail:GenerateQuery` tindakan dari kebijakan iam yang Anda gunakan.

Anda dapat mengakses generator kueri menggunakan CloudTrail konsol dan AWS CLI.

CloudTrail console

Untuk menggunakan generator kueri di CloudTrail konsol

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.
3. Pada halaman Query, pilih tab Editor.
4. Pilih penyimpanan data acara yang ingin Anda buat kueri.
5. Di area generator Query, masukkan prompt dalam bahasa Inggris biasa. Sebagai contoh, lihat Contoh petunjuk.

6. Pilih Hasilkan kueri. Generator kueri akan mencoba menghasilkan kueri dari prompt Anda. Jika berhasil, generator kueri menyediakan kueri SQL di editor. Jika prompt tidak berhasil, ulangi prompt Anda dan coba lagi.
7. (Opsional) Anda dapat memberikan umpan balik tentang kueri yang dihasilkan. Untuk memberikan umpan balik, pilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah prompt. Saat Anda memberikan umpan balik, CloudTrail menyimpan prompt Anda dan kueri yang dihasilkan.
8. (Opsional) Pilih Jalankan untuk menjalankan kueri.

> **Note**
>
> Saat menjalankan kueri, Anda dikenakan biaya berdasarkan jumlah data yang dioptimalkan dan dikompresi yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan `eventTime` stempel waktu awal dan akhir ke kueri.

9. (Opsional) Jika Anda menjalankan kueri dan ada hasil, Anda dapat memilih Ringkas hasil untuk menghasilkan ringkasan bahasa alami dalam bahasa Inggris dari hasil kueri. Opsi ini menggunakan kecerdasan buatan generatif (AI generatif) untuk menghasilkan ringkasan. Untuk informasi selengkapnya tentang metrik ini, lihat Meringkas hasil kueri dalam bahasa alami.

   Anda dapat memberikan umpan balik tentang ringkasan dengan memilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah ringkasan yang dihasilkan.

> **Note**
>
> Fitur ringkasan kueri ada dalam rilis pratinjau untuk CloudTrail Lake dan dapat berubah sewaktu-waktu. Fitur ini tersedia di wilayah berikut: Asia Pasifik (Tokyo), AS Timur (Virginia N.), dan AS Barat (Oregon).

AWS CLI

Untuk menghasilkan kueri dengan AWS CLI

Jalankan `generate-query` perintah untuk menghasilkan kueri dari prompt bahasa Inggris. Untuk`--event-data-stores`, berikan ARN (atau akhiran ID ARN) dari penyimpanan data

acara yang ingin Anda kueri. Anda hanya dapat menentukan satu penyimpanan data acara. Untuk`--prompt`, berikan prompt dalam bahasa Inggris.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

Jika berhasil, perintah mengeluarkan pernyataan SQL dan memberikan `QueryAlias` yang akan Anda gunakan dengan `start-query` perintah untuk menjalankan kueri terhadap penyimpanan data acara Anda.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

Untuk menjalankan kueri dengan AWS CLI

Jalankan `start-query` perintah dengan `QueryAlias` output oleh `generate-query` perintah pada contoh sebelumnya. Anda juga memiliki opsi untuk menjalankan `start-query` perintah dengan menyediakan file`QueryStatement`.

```
aws cloudtrail start-query --query-alias AWSCloudTrail-UUID
```

Responsnya adalah `QueryId` string. Untuk mendapatkan status kueri, jalankan `describe-query` menggunakan `QueryId` nilai yang dikembalikan oleh`start-query`. Jika kueri berhasil, Anda dapat menjalankan `get-query-results` untuk mendapatkan hasil.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Kueri yang berjalan lebih dari satu jam mungkin habis. Anda masih bisa mendapatkan sebagian hasil yang diproses sebelum waktu kueri habis.

Jika Anda mengirimkan hasil kueri ke bucket S3 menggunakan `--delivery-s3uri` parameter opsional, kebijakan bucket harus memberikan CloudTrail izin untuk mengirimkan hasil kueri ke bucket. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake.

Izin yang diperlukan

Kebijakan `AWSCloudTrail_FullAccess`dan kebijakan `AdministratorAccess`terkelola keduanya memberikan izin yang diperlukan untuk menggunakan fitur ini.

Anda juga dapat menyertakan tindakan `cloudtrail:GenerateQuery` dalam kebijakan terkelola atau inline pelanggan baru atau yang sudah ada.

Dukungan Wilayah

Fitur ini didukung sebagai berikut Wilayah AWS:

- Wilayah Asia Pasifik (Mumbai) (ap-south-1)
- Wilayah Asia Pasifik (Sydney) (ap-southeast-2)
- Wilayah Asia Pasifik (Tokyo) (ap-northeast-1)
- Wilayah Kanada (Tengah) (ca-central-1)
- Wilayah Eropa (London) (eu-west-2)
- Wilayah AS Timur (Virginia N.) (us-east-1)
- Wilayah AS Barat (Oregon) (us-west-2)

Batasan

Berikut ini adalah batasan generator kueri:

- Generator kueri hanya dapat menerima petunjuk dalam bahasa Inggris.
- Generator kueri hanya dapat menghasilkan kueri untuk penyimpanan data peristiwa yang mengumpulkan CloudTrail peristiwa (peristiwa manajemen, peristiwa data, peristiwa aktivitas jaringan).
- Generator kueri tidak dapat menghasilkan kueri untuk prompt yang tidak berkaitan dengan data peristiwa CloudTrail Lake.

Contoh petunjuk

Bagian ini memberikan contoh prompt dan query SQL yang dihasilkan dari prompt.

Jika Anda memilih untuk menjalankan contoh kueri di bagian ini, ganti *eds-id* dengan ID penyimpanan data peristiwa yang ingin Anda kueri dan ganti stempel waktu dengan stempel waktu yang sesuai untuk kasus penggunaan Anda. Stempel waktu memiliki format sebagai berikut:. YYYY-MM-DD HH:MM:SS

Prompt: What are my top errors in the past month?

Kueri SQL:

```
SELECT
    errorMessage,
    COUNT(*) as eventCount
FROM
    eds-id
WHERE
    errorMessage IS NOT NULL
AND eventTime >= timestamp '2024-05-01 00:00:00'
AND eventTime <= timestamp '2024-05-31 23:59:59'
GROUP BY 1
ORDER BY 2 DESC
LIMIT 2;
```

Prompt: Give me a list of users that used Amazon SNS.

Kueri SQL:

```
SELECT
    DISTINCT userIdentity.arn AS user
FROM
    eds-id
WHERE
    eventSource = 'sns.amazonaws.com'
```

Prompt: What are my API counts each day for read and write events in the past month?

Kueri SQL:

```
SELECT date(eventTime) AS event_date,
    SUM(
```

```
        CASE
            WHEN readonly = true THEN 1
            ELSE 0
        END
    ) AS read_events,
    SUM(
        CASE
            WHEN readonly = false THEN 1
            ELSE 0
        END
    ) AS write_events
FROM
    eds-id
WHERE
    eventTime >= timestamp '2024-05-04 00:00:00'
AND eventTime <= timestamp '2024-06-04 23:59:59'
GROUP BY 1
ORDER BY 1 ASC;
```

Prompt: Show any events with access denied errors for the past three weeks.

Kueri SQL:

```
SELECT *
FROM
  eds-id
WHERE
  WHERE (errorCode = 'AccessDenied' OR errorMessage = 'Access Denied')
AND eventTime >= timestamp '2024-05-16 01:00:00'
AND eventTime <= timestamp '2024-06-06 01:00:00'
```

Prompt: Query the number of calls each operator performed on the date 2024-05-01. The operator is a principal tag.

Kueri SQL:

```
SELECT element_at(
        eventContext.tagContext.principalTags,
        'operator'
    ) AS operator,
    COUNT(*) AS eventCount
FROM
    eds-id
```

```
WHERE eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
GROUP BY 1
ORDER BY 2 DESC;
```

Prompt: Give me all event IDs that touched resources within the CloudFormation stack with name myStack on the date 2024-05-01.

Kueri SQL:

```
SELECT eventID
FROM
    eds-id
WHERE any_match(
        eventContext.tagcontext.resourcetags,
        rt->element_at(rt.tags, 'aws:cloudformation:stack-name') = 'myStack'
    )
    AND eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
```

Prompt: Count the number of events grouped by resource tag 'solution' values, listing them in descending order of count.

Kueri SQL:

```
SELECT element_at(rt.tags, 'solution'),
    count(*) as event_count
FROM
    eds-id,
    unnest(eventContext.tagContext.resourceTags) as rt
WHERE eventtime < '2025-05-14 19:00:00'
GROUP BY 1
ORDER BY 2 DESC;
```

Prompt: Find all Amazon S3 data events where resource tag Environment has value prod.

Kueri SQL:

```
SELECT *
FROM
    eds-id
WHERE eventCategory = 'Data'
```

```
    AND eventSource = 's3.amazonaws.com'
    AND eventtime >= '2025-05-14 00:00:00'
    AND eventtime < '2025-05-14 20:00:00'
    AND any_match(
        eventContext.tagContext.resourceTags,
        rt->element_at(rt.tags, 'Environment') = 'prod'
    )
```

Lihat contoh kueri dengan konsol CloudTrail

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri.

CloudTrail kueri dikenakan biaya berdasarkan jumlah data yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan stempel `eventTime` waktu mulai dan berakhir ke kueri. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

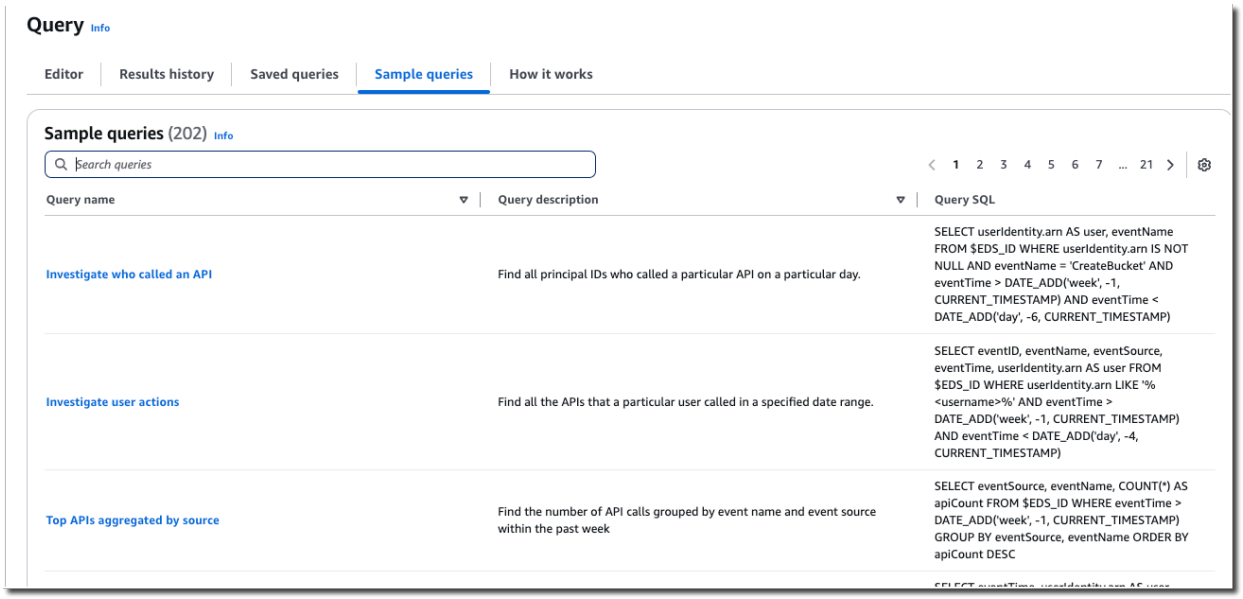
> **Note**
>
> Anda juga dapat melihat kueri yang dibuat oleh GitHub komunitas. Untuk informasi lebih lanjut, lihat pertanyaan sampel CloudTrail Danau di GitHub situs web. AWS CloudTrail belum mengevaluasi kueri di. GitHub

Untuk melihat dan menjalankan kueri sampel

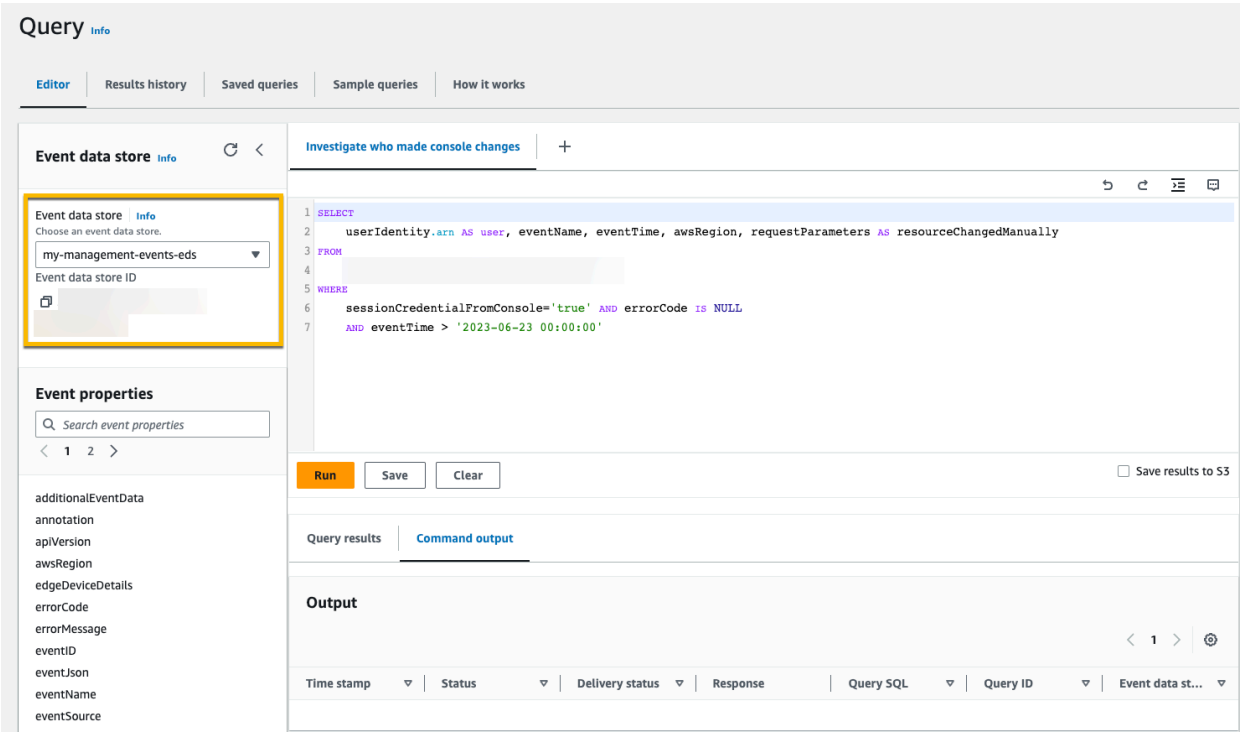
1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.
3. Pada halaman Query, pilih tab Contoh query.
4. Pilih contoh kueri dari daftar atau masukkan frasa untuk dicari. Dalam contoh ini, kita akan membuka kueri Selidiki siapa yang membuat perubahan konsol dengan memilih nama Query. Ini membuka kueri di tab Editor.

   > **Note**
   >
   > Secara default, halaman ini menggunakan fungsionalitas pencarian dasar. Anda dapat meningkatkan fungsionalitas pencarian dengan menambahkan izin untuk

`cloudtrail:SearchSampleQueries` tindakan, jika belum disediakan oleh kebijakan izin Anda. Kebijakan [AWSCloudTrail_FullAccess](#)terkelola memberikan izin untuk melakukan `cloudtrail:SearchSampleQueries` tindakan.

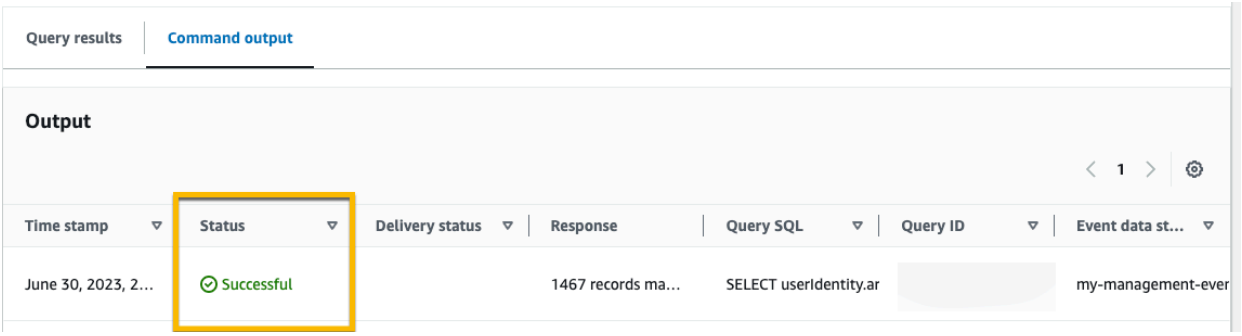


5. Pada tab Editor, pilih penyimpanan data acara yang ingin Anda jalankan kueri. Saat Anda memilih penyimpanan data acara dari daftar, CloudTrail secara otomatis mengisi ID penyimpanan data acara di `FROM` baris editor kueri.

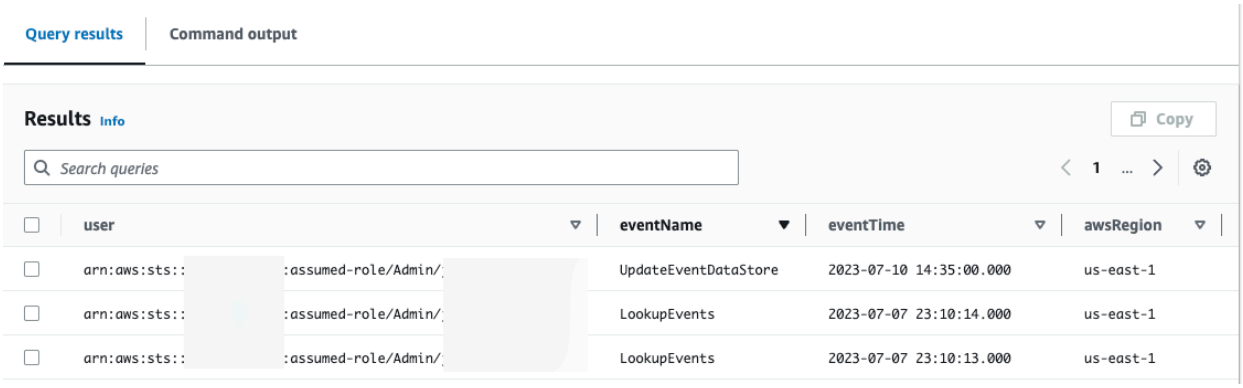


6. Pilih Jalankan untuk menjalankan kueri.

   Tab Output perintah menunjukkan metadata tentang kueri Anda, seperti apakah kueri berhasil, jumlah catatan yang cocok, dan waktu menjalankan kueri.



   Tab Hasil kueri menampilkan data peristiwa di penyimpanan data peristiwa terpilih yang cocok dengan kueri Anda.



Untuk informasi selengkapnya tentang mengedit kueri, lihatMembuat atau mengedit kueri dengan CloudTrail konsol. Untuk informasi selengkapnya tentang menjalankan kueri dan menyimpan hasil kueri, lihatJalankan kueri dan simpan hasil kueri dengan konsol.

Membuat atau mengedit kueri dengan CloudTrail konsol

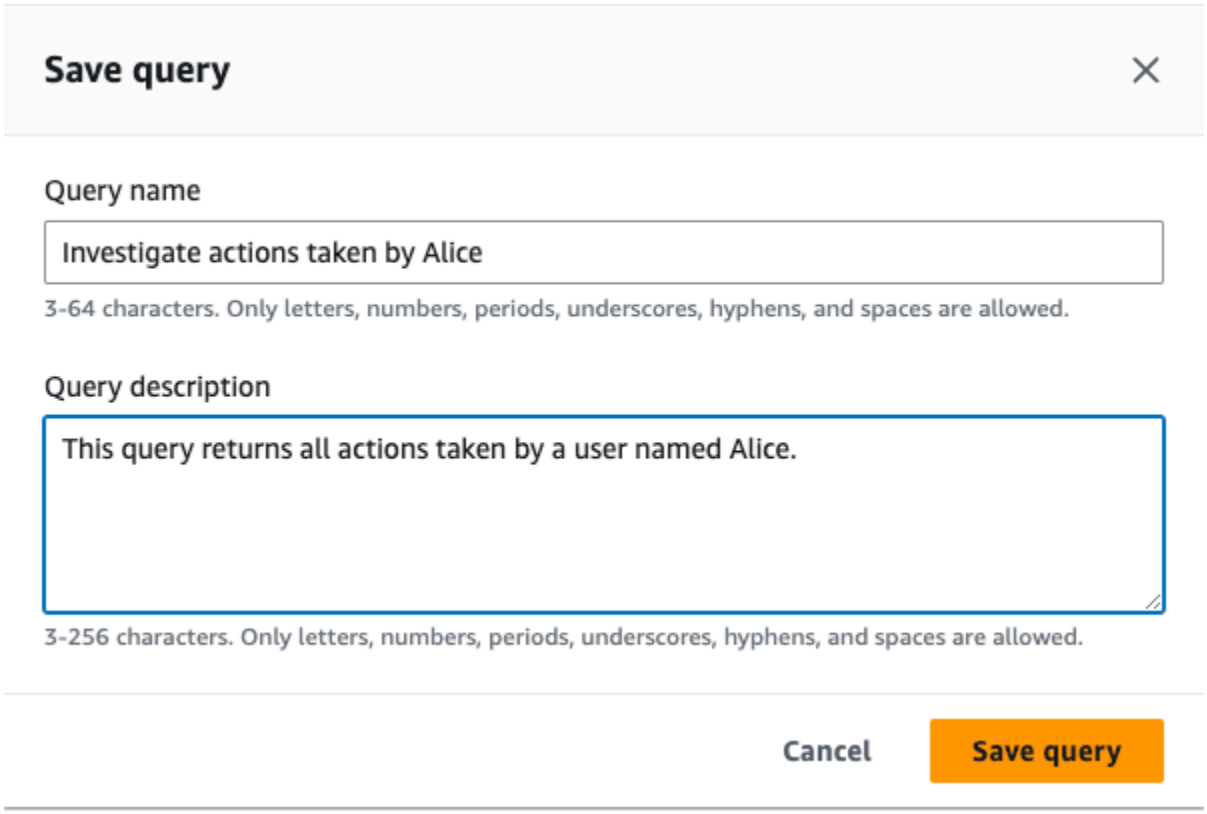
Dalam panduan ini, kami membuka salah satu contoh kueri, mengeditnya untuk menemukan tindakan yang diambil oleh pengguna tertentu bernama`Alice`, dan menyimpannya sebagai kueri baru. Anda juga dapat mengedit kueri tersimpan di tab Kueri tersimpan, jika Anda telah menyimpan kueri. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan stempel `eventTime` waktu mulai dan berakhir ke kueri.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.

2. Dari panel navigasi, di bawah Danau, pilih Kueri.
3. Pada halaman Query, pilih tab Contoh query.
4. Buka kueri sampel dengan memilih nama Query. Ini membuka kueri di tab Editor. Dalam contoh ini, kita akan memilih kueri bernama Selidiki tindakan pengguna dan mengedit kueri untuk menemukan tindakan untuk pengguna tertentu bernama`Alice`.
5. Di tab Editor, edit `WHERE` baris untuk menentukan pengguna yang ingin Anda selidiki dan perbarui `eventTime` nilai sesuai kebutuhan. Nilai `FROM` adalah bagian ID dari ARN penyimpanan data acara dan secara otomatis diisi oleh CloudTrail ketika Anda memilih penyimpanan data acara.

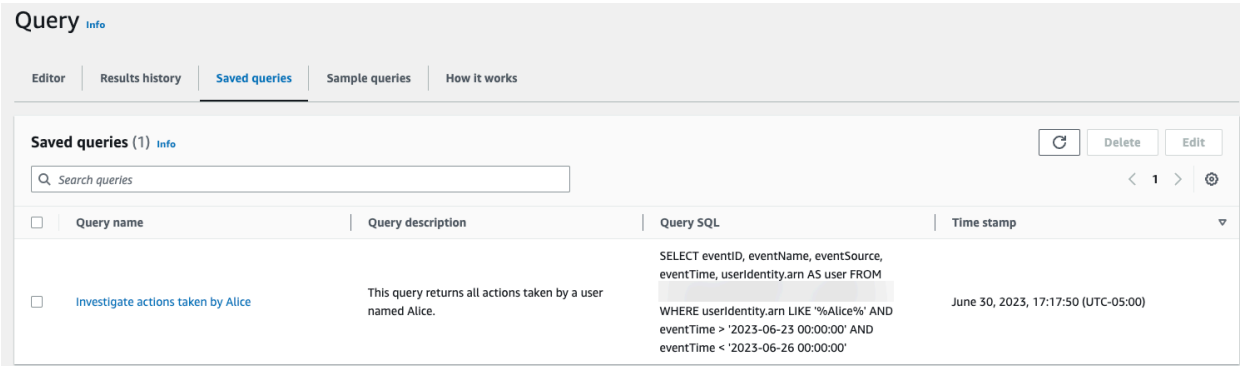
```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. Anda dapat menjalankan kueri sebelum menyimpannya, untuk memverifikasi bahwa kueri berfungsi. Untuk menjalankan kueri, pilih penyimpanan data peristiwa dari daftar drop-down penyimpanan data peristiwa, lalu pilih Jalankan. Lihat kolom Status pada tab keluaran Perintah untuk kueri aktif guna memverifikasi bahwa kueri berhasil dijalankan.
7. Ketika Anda telah memperbarui kueri sampel, pilih Simpan.
8. Di Simpan kueri, masukkan nama dan deskripsi untuk kueri. Pilih Simpan kueri untuk menyimpan perubahan Anda sebagai kueri baru. Untuk membuang perubahan pada kueri, pilih Batalkan, atau tutup jendela Simpan kueri.



> **Note**
>
> Kueri tersimpan terkait dengan browser Anda; jika Anda menggunakan browser lain atau perangkat lain untuk mengakses CloudTrail konsol, kueri yang disimpan tidak tersedia.

9. Buka tab Kueri tersimpan untuk melihat kueri baru di tabel.



Jalankan kueri dan simpan hasil kueri dengan konsol

Setelah memilih atau menyimpan kueri, Anda dapat menjalankan kueri di penyimpanan data acara.

Saat menjalankan kueri, Anda memiliki opsi untuk menyimpan hasil kueri ke bucket Amazon S3. Saat menjalankan kueri di CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data yang dipindai oleh kueri. Tidak ada biaya CloudTrail Danau tambahan untuk menyimpan hasil kueri ke ember S3, namun, ada biaya penyimpanan S3. Untuk informasi selengkapnya tentang harga S3, lihat harga Amazon S3.

Saat Anda menyimpan hasil kueri, hasil kueri mungkin ditampilkan di CloudTrail konsol sebelum dapat dilihat di bucket S3 karena CloudTrail memberikan hasil kueri setelah pemindaian kueri selesai. Meskipun sebagian besar kueri selesai dalam beberapa menit, tergantung pada ukuran penyimpanan data acara Anda, dapat memakan waktu lebih lama untuk mengirimkan hasil kueri CloudTrail ke bucket S3 Anda. CloudTrail mengirimkan hasil kueri ke bucket S3 dalam format gzip terkompresi. Rata-rata, setelah pemindaian kueri selesai, Anda dapat mengharapkan latensi 60 hingga 90 detik untuk setiap GB data yang dikirim ke bucket S3.

Untuk menjalankan kueri menggunakan CloudTrail Lake

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.
3. Pada tab Kueri tersimpan atau Kueri sampel, pilih kueri yang akan dijalankan dengan memilih nama Kueri.
4. Pada tab Editor, untuk penyimpanan data acara, pilih penyimpanan data acara dari daftar drop-down.
5. (Opsional) Pada tab Editor, pilih Simpan hasil ke S3 untuk menyimpan hasil kueri ke bucket S3. Saat Anda memilih bucket S3 default, CloudTrail buat dan terapkan kebijakan bucket yang diperlukan. Jika Anda memilih bucket S3 default, kebijakan IAM Anda harus menyertakan izin untuk `s3:PutEncryptionConfiguration` tindakan karena enkripsi sisi server secara default diaktifkan untuk bucket. Untuk informasi selengkapnya tentang menyimpan hasil kueri, lihatInformasi tambahan tentang hasil kueri yang disimpan.

> **Note**
>
> Untuk menggunakan bucket yang berbeda, tentukan nama bucket, atau pilih Browse S3 untuk memilih bucket. Kebijakan bucket harus memberikan CloudTrail izin untuk mengirimkan hasil kueri ke bucket. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake.

6. Pada tab Editor, pilih Jalankan.

   Bergantung pada ukuran penyimpanan data acara Anda, dan jumlah hari data yang disertakan, kueri dapat memakan waktu beberapa menit untuk dijalankan. Tab keluaran Perintah menunjukkan status kueri, dan apakah kueri selesai dijalankan. Ketika kueri selesai berjalan, buka tab Hasil kueri untuk melihat tabel hasil untuk kueri aktif (kueri saat ini ditampilkan di editor).

> **Note**
>
> Kueri yang berjalan lebih dari satu jam mungkin habis. Anda masih bisa mendapatkan sebagian hasil yang diproses sebelum waktu kueri habis. CloudTrail tidak memberikan hasil kueri sebagian ke bucket S3. Untuk menghindari waktu habis, Anda dapat memperbaiki kueri untuk membatasi jumlah data yang dipindai dengan menentukan rentang waktu yang lebih sempit.

Informasi tambahan tentang hasil kueri yang disimpan

Setelah menyimpan hasil kueri, Anda dapat mengunduh hasil kueri yang disimpan dari bucket S3. Untuk informasi selengkapnya tentang menemukan dan mengunduh hasil kueri yang disimpan, lihatUnduh hasil kueri yang disimpan.

Anda juga dapat memvalidasi hasil kueri yang disimpan untuk menentukan apakah hasil kueri diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan hasil kueri. Untuk informasi selengkapnya tentang memvalidasi hasil kueri yang disimpan, lihatValidasi hasil kueri yang disimpan CloudTrail Lake.

Contoh: Menyimpan hasil kueri ke bucket Amazon S3

Panduan ini menunjukkan bagaimana Anda dapat menyimpan hasil kueri ke bucket S3 dan kemudian mengunduh hasil kueri tersebut.

Untuk menyimpan hasil kueri ke bucket Amazon S3

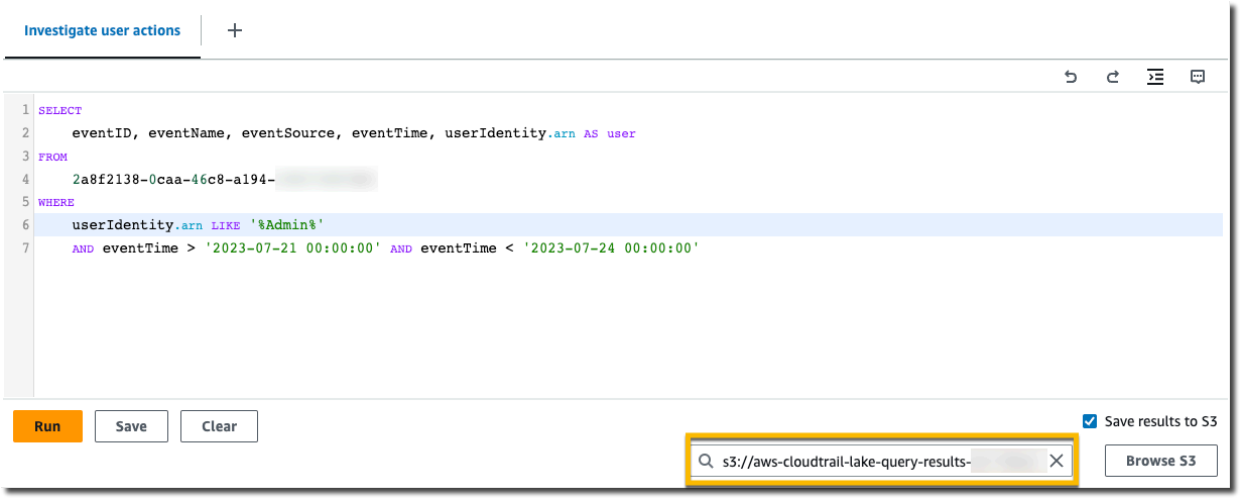
1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.

3. Pada tab Kueri sampel atau Kueri tersimpan, pilih kueri yang akan dijalankan dengan memilih nama Kueri. Dalam contoh ini, kita akan memilih query sampel bernama Selidiki tindakan pengguna.
4. Pada tab Editor, untuk penyimpanan data acara, pilih penyimpanan data acara dari daftar drop-down. Saat Anda memilih penyimpanan data acara dari daftar, CloudTrail secara otomatis mengisi ID penyimpanan data acara di `From` baris.
5. Dalam contoh query ini, kita akan mengedit `userIdentity.ARN` nilai untuk menentukan nama penggunaAdmin, dan kita akan meninggalkan nilai default untuk`eventTime`. Saat menjalankan kueri, Anda dikenakan biaya untuk jumlah data yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan stempel `eventTime` waktu mulai dan berakhir ke kueri.



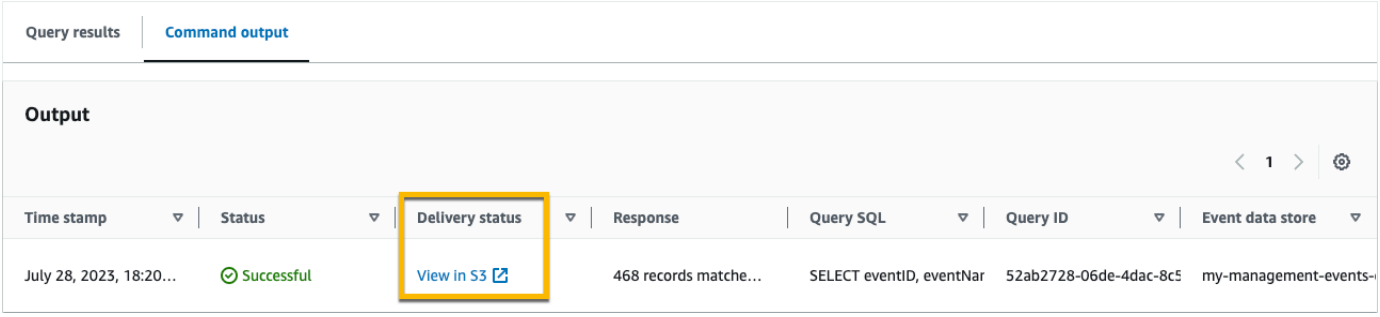
6. Pilih Simpan hasil ke S3 untuk menyimpan hasil kueri ke bucket S3. Saat Anda memilih bucket S3 default, CloudTrail buat dan terapkan kebijakan bucket yang diperlukan. Jika Anda memilih bucket S3 default, kebijakan IAM Anda harus menyertakan izin untuk `s3:PutEncryptionConfiguration` tindakan karena enkripsi sisi server secara default diaktifkan untuk bucket. Dalam contoh ini, kita akan menggunakan bucket S3 default.

> **Note**
>
> Untuk menggunakan bucket yang berbeda, tentukan nama bucket, atau pilih Browse S3 untuk memilih bucket. Kebijakan bucket harus memberikan CloudTrail izin untuk mengirimkan hasil kueri ke bucket. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake.

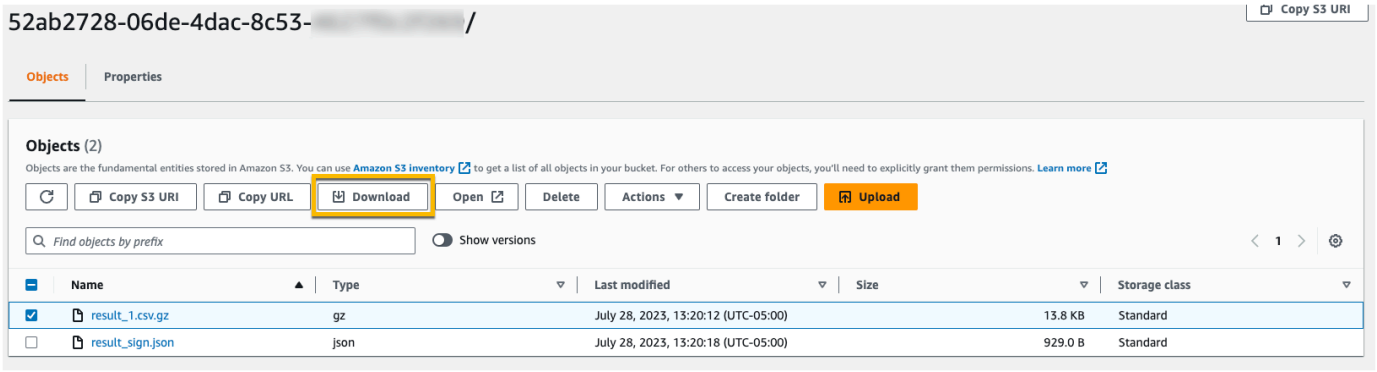


7. Pilih Jalankan. Bergantung pada ukuran penyimpanan data acara Anda, dan jumlah hari data yang disertakan, kueri dapat memakan waktu beberapa menit untuk dijalankan. Tab keluaran Perintah menunjukkan status kueri, dan apakah kueri selesai dijalankan. Ketika kueri selesai berjalan, buka tab Hasil kueri untuk melihat tabel hasil untuk kueri aktif (kueri saat ini ditampilkan di editor).
8. Saat CloudTrail menyelesaikan pengiriman hasil kueri yang disimpan ke bucket S3 Anda, kolom Status pengiriman menyediakan tautan ke bucket S3 yang berisi file hasil kueri tersimpan serta file tanda yang dapat Anda gunakan untuk memverifikasi hasil kueri yang disimpan. Pilih Lihat di S3 untuk melihat file hasil kueri dan menandatangani file di bucket S3.

> **Note**
>
> Saat Anda menyimpan hasil kueri, hasil kueri dapat ditampilkan di CloudTrail konsol sebelum dapat dilihat di bucket S3 karena CloudTrail memberikan hasil kueri setelah pemindaian kueri selesai. Meskipun sebagian besar kueri selesai dalam beberapa menit, tergantung pada ukuran penyimpanan data acara Anda, dapat memakan waktu lebih lama untuk mengirimkan hasil kueri CloudTrail ke bucket S3 Anda. CloudTrail mengirimkan hasil kueri ke bucket S3 dalam format gzip terkompresi. Rata-rata, setelah pemindaian kueri selesai, Anda dapat mengharapkan latensi 60 hingga 90 detik untuk setiap GB data yang dikirim ke bucket S3.



9. Untuk mengunduh hasil kueri Anda, pilih file hasil kueri (dalam contoh ini,`result_1.csv.gz`) lalu pilih Unduh.



Untuk informasi tentang memvalidasi hasil kueri yang disimpan, lihatValidasi hasil kueri yang disimpan CloudTrail Lake.

Lihat hasil kueri dengan konsol

Setelah kueri selesai, Anda dapat melihat hasilnya. Hasil kueri tersedia selama tujuh hari setelah kueri selesai. Anda dapat melihat hasil untuk kueri aktif di tab Hasil kueri, atau Anda dapat mengakses hasil untuk semua kueri terbaru di tab Riwayat hasil di halaman beranda Lake.

Hasil kueri dapat berubah dari proses kueri yang lebih lama ke yang lebih baru, karena peristiwa selanjutnya dalam periode kueri dapat dicatat di antara kueri.

Saat Anda menyimpan hasil kueri, hasil kueri mungkin ditampilkan di CloudTrail konsol sebelum dapat dilihat di bucket S3 karena CloudTrail memberikan hasil kueri setelah pemindaian kueri selesai. Meskipun sebagian besar kueri selesai dalam beberapa menit, tergantung pada ukuran penyimpanan data acara Anda, dapat memakan waktu lebih lama untuk mengirimkan hasil kueri CloudTrail ke bucket S3 Anda. CloudTrail mengirimkan hasil kueri ke bucket S3 dalam format gzip terkompresi. Rata-rata, setelah pemindaian kueri selesai, Anda dapat mengharapkan latensi 60 hingga 90 detik

untuk setiap GB data yang dikirim ke bucket S3. Untuk informasi selengkapnya tentang menemukan dan mengunduh hasil kueri yang disimpan, lihatUnduh hasil kueri yang disimpan.

> **Note**
>
> Kueri yang berjalan lebih dari satu jam mungkin habis. Anda masih bisa mendapatkan sebagian hasil yang diproses sebelum waktu kueri habis. CloudTrail tidak memberikan hasil kueri sebagian ke bucket S3. Untuk menghindari waktu habis, Anda dapat memperbaiki kueri untuk membatasi jumlah data yang dipindai dengan menentukan rentang waktu yang lebih sempit.

Untuk melihat hasil kueri

1. Pilih tab Hasil kueri pada editor kueri jika belum dipilih. Pada tab Hasil kueri untuk kueri aktif, setiap baris mewakili hasil peristiwa yang cocok dengan kueri. Filter hasil dengan memasukkan semua atau sebagian dari nilai bidang peristiwa di bilah pencarian. Untuk menyalin acara, pilih acara yang ingin Anda salin lalu pilih Salin.
2. (Opsional) Pilih Ringkas hasil untuk menghasilkan ringkasan bahasa alami dari hasil kueri. Ringkasan disediakan dalam bahasa Inggris. Opsi ini menggunakan kecerdasan buatan generatif (AI generatif) untuk menghasilkan ringkasan. Untuk informasi selengkapnya tentang metrik ini, lihat Meringkas hasil kueri dalam bahasa alami.

   Anda dapat memberikan umpan balik tentang ringkasan dengan memilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah ringkasan yang dihasilkan.

   > **Note**
   >
   > Fitur ringkasan kueri ada dalam rilis pratinjau untuk CloudTrail Lake dan dapat berubah sewaktu-waktu. Fitur ini tersedia di wilayah berikut: Asia Pasifik (Tokyo), AS Timur (Virginia N.), dan AS Barat (Oregon).
3. Pada tab keluaran Perintah, lihat metadata tentang kueri yang dijalankan, seperti ID penyimpanan data peristiwa, waktu berjalan, jumlah hasil yang dipindai, dan apakah kueri berhasil atau tidak. Jika Anda menyimpan hasil kueri ke bucket Amazon S3, metadata juga menyertakan tautan ke bucket S3 yang berisi hasil kueri yang disimpan.

Meringkas hasil kueri dalam bahasa alami

> **Note**
>
> Fitur ringkasan kueri ada dalam rilis pratinjau untuk CloudTrail Lake dan dapat berubah sewaktu-waktu.

> **Note**
>
> CloudTrail akan secara otomatis memilih wilayah optimal dalam geografi Anda untuk memproses permintaan inferensi sambil meringkas kueri. Ini memaksimalkan sumber daya komputasi yang tersedia, ketersediaan model, dan memberikan pengalaman pelanggan terbaik. Data Anda akan tetap disimpan hanya di wilayah tempat permintaan berasal, namun, permintaan input dan hasil keluaran dapat diproses di luar wilayah tersebut. Semua data akan dikirimkan dienkripsi di seluruh jaringan aman Amazon.
> CloudTrail akan dengan aman merutekan permintaan inferensi Anda ke sumber daya komputasi yang tersedia dalam wilayah geografis tempat permintaan tersebut berasal, sebagai berikut:
>
> - Permintaan inferensi yang berasal dari Amerika Serikat akan diproses di Amerika Serikat
> - Permintaan inferensi yang berasal dari Jepang akan diproses di Jepang
>
> Untuk memilih keluar dari fitur ringkasan kueri, Anda dapat secara eksplisit menolak atau menghapus `cloudtrail:GenerateQueryResultsSummary` tindakan dari kebijakan iam yang Anda gunakan.

Setelah kueri selesai, Anda bisa mendapatkan ringkasan hasil kueri dalam bahasa alami dari tab Hasil kueri di editor kueri. Opsi ini menggunakan kecerdasan buatan generatif (AI generatif) untuk menghasilkan ringkasan.

Untuk meringkas hasil kueri

1. Dari tab Hasil kueri editor kueri, pilih Ringkas hasil untuk menghasilkan ringkasan bahasa alami dari hasil kueri. Ringkasan disediakan dalam bahasa Inggris.

2. (Opsional) Berikan umpan balik tentang ringkasan dengan memilih tombol jempol ke atas atau jempol ke bawah yang muncul di bawah ringkasan yang dihasilkan.

Jika penyimpanan data peristiwa terkait dienkripsi menggunakan kunci KMS, Anda tidak dapat menggunakan kunci KMS untuk mengenkripsi hasil kueri dan ringkasan. Hasil kueri dan ringkasan malah dienkripsi oleh. CloudTrail

Akses ke ringkasan yang dihasilkan diotorisasi terhadap`GetQueryResults`,`GenerateQueryResultsSummary`, dan izin KMS (jika penyimpanan tanggal acara terkait dienkripsi dengan kunci KMS). Saat ringkasan dibuat, CloudTrail merekam peristiwa yang dinamai `GenerateQueryResultsSummary` untuk visibilitas.

Izin yang diperlukan

Kebijakan `AWSCloudTrail_FullAccess`dan kebijakan `AdministratorAccess`terkelola keduanya memberikan izin yang diperlukan untuk menggunakan fitur ini.

Anda juga dapat menyertakan `cloudtrail:GenerateQueryResultsSummary` dan `cloudtrail:GetQueryResults` tindakan dalam kebijakan terkelola atau inline pelanggan baru atau yang sudah ada.

Jika penyimpanan data peristiwa yang terkait dengan hasil kueri yang diringkas dienkripsi dengan kunci KMS, Anda juga memerlukan izin untuk kunci KMS.

Dukungan Wilayah

Fitur ini tersedia sebagai berikut Wilayah AWS:

- Wilayah Asia Pasifik (Tokyo) (ap-northeast-1)
- Wilayah AS Timur (Virginia N.) (us-east-1)
- Wilayah AS Barat (Oregon) (us-west-2)

Batasan

Berikut ini adalah batasan fitur ini:

- Ringkasan hanya dalam bahasa Inggris.
- Ringkasan terbatas pada penyimpanan data acara yang mengumpulkan CloudTrail peristiwa (peristiwa manajemen, peristiwa data, peristiwa aktivitas jaringan).

- Setiap ringkasan adalah untuk hasil dari satu kueri.
- Ukuran hasil kueri harus kurang dari 250 KB.
- Kuota bulanan hasil kueri yang dapat diringkas adalah 3 MB.

Unduh hasil kueri yang disimpan

Setelah Anda menyimpan hasil kueri, Anda harus dapat menemukan file yang berisi hasil kueri. CloudTrail mengirimkan hasil kueri ke bucket Amazon S3 yang ditentukan saat menyimpan hasil kueri.

> **Note**
>
> Saat Anda menyimpan hasil kueri, hasil kueri mungkin ditampilkan di konsol sebelum dapat dilihat di bucket S3 karena CloudTrail memberikan hasil kueri setelah pemindaian kueri selesai. Meskipun sebagian besar kueri selesai dalam beberapa menit, tergantung pada ukuran penyimpanan data acara Anda, dapat memakan waktu lebih lama untuk mengirimkan hasil kueri CloudTrail ke bucket S3 Anda. CloudTrail mengirimkan hasil kueri ke bucket S3 dalam format gzip terkompresi. Rata-rata, setelah pemindaian kueri selesai, Anda dapat mengharapkan latensi 60 hingga 90 detik untuk setiap GB data yang dikirim ke bucket S3.

Topik

- Temukan hasil kueri tersimpan CloudTrail Lake Anda
- Unduh hasil kueri tersimpan CloudTrail Lake Anda

Temukan hasil kueri tersimpan CloudTrail Lake Anda

CloudTrail menerbitkan hasil kueri dan menandatangani file ke bucket S3 Anda. File hasil kueri berisi output dari kueri yang disimpan dan file tanda memberikan tanda tangan dan nilai hash untuk hasil kueri. Anda dapat menggunakan file tanda untuk memvalidasi hasil kueri. Untuk informasi selengkapnya tentang memvalidasi hasil kueri, lihatValidasi hasil kueri yang disimpan CloudTrail Lake.

Untuk mengambil hasil kueri atau file tanda tangan, Anda dapat menggunakan konsol Amazon S3, antarmuka baris perintah Amazon S3 (CLI), atau API.

Untuk menemukan hasil kueri dan menandatangani file dengan konsol Amazon S3

1. Buka konsol Amazon S3.
2. Pilih ember yang Anda tentukan.
3. Arahkan melalui hierarki objek hingga Anda menemukan hasil kueri dan menandatangani file. File hasil kueri memiliki ekstensi.csv.gz dan file tanda memiliki ekstensi.json.

Anda akan menavigasi hierarki objek yang mirip dengan contoh berikut, tetapi dengan nama bucket, ID akun, tanggal, dan ID kueri yang berbeda.

```
All Buckets
    amzn-s3-demo-bucket
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Unduh hasil kueri tersimpan CloudTrail Lake Anda

Saat Anda menyimpan hasil kueri, CloudTrail kirimkan dua jenis file ke bucket Amazon S3 Anda.

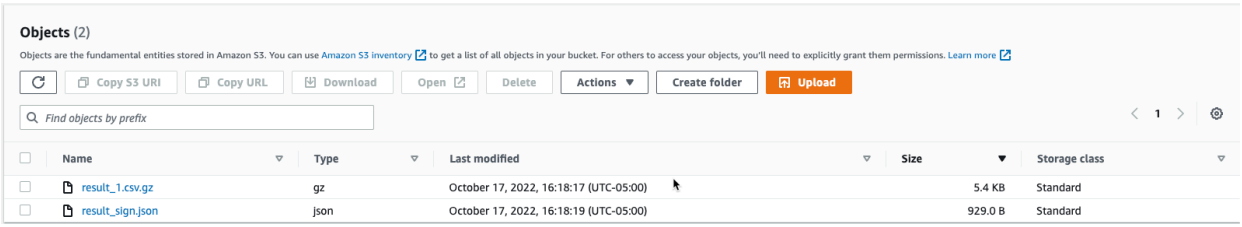
- File tanda dalam format JSON yang dapat Anda gunakan untuk memvalidasi file hasil kueri. Berkas tanda bernama result_sign.json. Untuk informasi selengkapnya tentang file tanda, lihatCloudTrail struktur file tanda tangan.
- Satu atau lebih file hasil kueri dalam format CSV, yang berisi hasil dari kueri. Jumlah file hasil kueri yang dikirimkan tergantung pada ukuran total hasil kueri. Ukuran file maksimum untuk file hasil kueri adalah 1 TB. Setiap file hasil kueri diberi nama result_ *number* .csv.gz. Misalnya, jika ukuran total hasil kueri adalah 2 TB, Anda akan memiliki dua file hasil kueri, result_1.csv.gz dan result_2.csv.gz.

CloudTrail hasil kueri dan file tanda adalah objek Amazon S3. Anda dapat menggunakan konsol S3, AWS Command Line Interface (CLI), atau S3 API untuk mengambil hasil kueri dan menandatangani file.

Prosedur berikut menjelaskan cara mengunduh hasil kueri dan menandatangani file dengan konsol Amazon S3.

Untuk mengunduh hasil kueri atau menandatangani file dengan konsol Amazon S3

1. Buka konsol Amazon S3.
2. Pilih bucket dan pilih file yang ingin Anda unduh.



3. Pilih Unduh dan ikuti petunjuk apa pun untuk menyimpan file.

> **Note**
>
> Beberapa browser, seperti Chrome, secara otomatis mengekstrak file hasil kueri untuk Anda. Jika browser Anda melakukan ini untuk Anda, lewati ke langkah 5.

4. Gunakan produk seperti 7-Zip untuk mengekstrak file hasil kueri.
5. Buka hasil kueri atau tandatangani file.

Validasi hasil kueri yang disimpan CloudTrail Lake

Untuk menentukan apakah hasil kueri diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan hasil kueri, Anda dapat menggunakan validasi integritas hasil CloudTrail kueri. Fitur ini dibangun menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan file hasil CloudTrail kueri tanpa deteksi. Anda dapat menggunakan baris perintah untuk memvalidasi file hasil kueri.

Mengapa menggunakannya?

File hasil kueri yang divalidasi sangat berharga dalam penyelidikan keamanan dan forensik. Misalnya, file hasil kueri yang divalidasi memungkinkan Anda untuk menegaskan secara positif bahwa file hasil kueri itu sendiri tidak berubah. Proses validasi integritas file hasil CloudTrail kueri juga memungkinkan Anda mengetahui apakah file hasil kueri telah dihapus atau diubah.

Topik

- Validasi hasil kueri yang disimpan dengan AWS CLI
- CloudTrail struktur file tanda tangan
- Implementasi kustom validasi integritas file hasil CloudTrail kueri

Validasi hasil kueri yang disimpan dengan AWS CLI

Anda dapat memvalidasi integritas file hasil kueri dan menandatangani file dengan menggunakan aws cloudtrail verify-query-resultsperintah.

Prasyarat

Untuk memvalidasi integritas hasil kueri dengan baris perintah, kondisi berikut harus dipenuhi:

- Anda harus memiliki konektivitas online untuk AWS.
- Anda harus menggunakan AWS CLI versi 2.
- Untuk memvalidasi file hasil kueri dan menandatangani file secara lokal, ketentuan berikut berlaku:
  - Anda harus meletakkan file hasil kueri dan menandatangani file di jalur file yang ditentukan. Tentukan jalur file sebagai nilai untuk --local-export-path parameter.
  - Anda tidak boleh mengganti nama file hasil kueri dan file tanda tangan.
- Untuk memvalidasi file hasil kueri dan menandatangani file di bucket S3, ketentuan berikut berlaku:
  - Anda tidak boleh mengganti nama file hasil kueri dan file tanda tangan.
  - Anda harus memiliki akses baca ke bucket Amazon S3 yang berisi file hasil kueri dan file tanda tangan.
  - Awalan S3 yang ditentukan harus berisi file hasil kueri dan file tanda. Tentukan awalan S3 sebagai nilai untuk parameter. --s3-prefix

verify-query-results

verify-query-resultsPerintah memverifikasi nilai hash dari setiap file hasil kueri dengan membandingkan nilai dengan `fileHashValue` dalam file tanda, dan kemudian memvalidasi `hashSignature` dalam file tanda.

Saat memverifikasi hasil kueri, Anda dapat menggunakan opsi baris --s3-prefix perintah --s3-bucket dan untuk memvalidasi file hasil kueri dan menandatangani file yang disimpan dalam bucket S3, atau

Anda dapat menggunakan opsi baris --local-export-path perintah untuk melakukan validasi lokal dari file hasil kueri yang diunduh dan file tanda tangan.

> **Note**
>
> verify-query-resultsPerintahnya spesifik Wilayah. Anda harus menentukan opsi --region global untuk memvalidasi hasil kueri untuk spesifik Wilayah AWS.

Berikut ini adalah opsi untuk verify-query-results perintah.

--s3-bucket *<string>*

Menentukan nama bucket S3 yang menyimpan file hasil kueri dan file tanda tangan. Anda tidak dapat menggunakan parameter ini dengan--local-export-path.

--s3-prefix *<string>*

Menentukan jalur S3 dari folder S3 yang berisi file hasil query dan file tanda (misalnya,). `s3/path/` Anda tidak dapat menggunakan parameter ini dengan--local-export-path. Anda tidak perlu memberikan parameter ini jika file berada di direktori root bucket S3.

--local-export-path *<string>*

Menentukan direktori lokal yang berisi file hasil query dan file tanda (misalnya,`/local/path/to/export/file/`). Anda tidak dapat menggunakan parameter ini dengan --s3-bucket atau--s3-prefix.

Contoh

Contoh berikut memvalidasi hasil kueri menggunakan opsi baris --s3-prefix perintah --s3-bucket dan untuk menentukan nama bucket S3 dan awalan yang berisi file hasil kueri dan file tanda.

```
aws cloudtrail verify-query-results --s3-bucket amzn-s3-demo-bucket --s3-prefix prefix
 --region region
```

Contoh berikut memvalidasi hasil kueri yang diunduh menggunakan opsi baris --local-export-path perintah untuk menentukan jalur lokal untuk file hasil kueri dan file tanda tangan. Untuk informasi

selengkapnya tentang mengunduh file hasil kueri, lihatUnduh hasil kueri tersimpan CloudTrail Lake Anda.

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

Hasil validasi

Tabel berikut menjelaskan kemungkinan pesan validasi untuk file hasil kueri dan file tanda.

Jenis File	Pesan Validasi	Deskripsi
`Sign file`	`Successfully validated sign and query result files`	Tanda tangan file tanda tangan valid. File hasil kueri yang direferensikannya dapat diperiksa.
`Query result file`	`ValidationError: "File` *`file_name`* `has inconsistent hash value with hash value recorded in sign file, hash value in sign file is` *`expected_hash`* `, but get` *`computed_hash`*	Validasi gagal karena nilai hash untuk file hasil kueri tidak cocok dengan `fileHashValue` dalam file tanda.
`Sign file`	`ValidationError: Invalid signature in sign file`	Validasi untuk file tanda gagal karena tanda tangan tidak valid.

CloudTrail struktur file tanda tangan

File tanda berisi nama setiap file hasil kueri yang dikirimkan ke bucket Amazon S3 saat Anda menyimpan hasil kueri, nilai hash untuk setiap file hasil kueri, dan tanda tangan digital file. Tanda tangan digital dan nilai hash digunakan untuk memvalidasi integritas file hasil kueri dan file tanda itu sendiri.

Menandatangani lokasi berkas

File tanda dikirim ke lokasi bucket Amazon S3 yang mengikuti sintaks ini.

```
s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Contoh isi file tanda tangan

File tanda contoh berikut berisi informasi untuk hasil kueri CloudTrail Lake.

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

Menandatangani deskripsi bidang file

Berikut ini adalah deskripsi untuk setiap bidang dalam file tanda:

`version`

Versi file tanda.

`region`

Wilayah untuk AWS akun yang digunakan untuk menyimpan hasil kueri.

`files.fileHashValue`

Nilai hash yang dikodekan heksadesimal dari konten file hasil kueri terkompresi.

`files.fileName`

Nama file hasil query.

`hashAlgorithm`

Algoritma hash digunakan untuk hash file hasil query.

`signatureAlgorithm`

Algoritma yang digunakan untuk menandatangani file.

`queryCompleteTime`

Menunjukkan saat CloudTrail mengirimkan hasil kueri ke bucket S3. Anda dapat menggunakan nilai ini untuk menemukan kunci publik.

`hashSignature`

Tanda tangan hash untuk file tersebut.

`publicKeyFingerprint`

Sidik jari heksadesimal yang dikodekan dari kunci publik yang digunakan untuk menandatangani file.

Implementasi kustom validasi integritas file hasil CloudTrail kueri

Karena CloudTrail menggunakan standar industri, algoritma kriptografi yang tersedia secara terbuka dan fungsi hash, Anda dapat membuat alat Anda sendiri untuk memvalidasi integritas file hasil kueri. CloudTrail Saat Anda menyimpan hasil kueri ke bucket Amazon S3, kirimkan CloudTrail file tanda ke bucket S3 Anda. Anda dapat menerapkan solusi validasi Anda sendiri untuk memvalidasi tanda tangan dan file hasil kueri. Untuk informasi selengkapnya tentang file tanda, lihatCloudTrail struktur file tanda tangan.

Topik ini menjelaskan bagaimana file tanda ditandatangani, dan kemudian merinci langkah-langkah yang perlu Anda ambil untuk menerapkan solusi yang memvalidasi file tanda dan file hasil kueri yang direferensikan oleh file tanda tangan.

Memahami bagaimana file CloudTrail tanda ditandatangani

CloudTrail file tanda ditandatangani dengan tanda tangan digital RSA. Untuk setiap file tanda, CloudTrail lakukan hal berikut:

1. Membuat daftar hash yang berisi nilai hash untuk setiap file hasil query.
2. Mendapat kunci pribadi yang unik untuk Wilayah.
3. Melewati hash SHA-256 dari string dan kunci pribadi ke algoritma penandatanganan RSA, yang menghasilkan tanda tangan digital.
4. Mengkodekan kode byte tanda tangan ke dalam format heksadesimal.
5. Menempatkan tanda tangan digital ke dalam file tanda.

Isi string penandatanganan data

String penandatanganan data terdiri dari nilai hash untuk setiap file hasil kueri yang dipisahkan oleh spasi. File tanda mencantumkan `fileHashValue` untuk setiap file hasil kueri.

Langkah-langkah implementasi validasi kustom

Saat menerapkan solusi validasi kustom, Anda perlu memvalidasi file tanda dan file hasil kueri yang dirujuk.

Validasi file tanda

Untuk memvalidasi file tanda tangan, Anda memerlukan tanda tangannya, kunci publik yang kunci pribadinya digunakan untuk menandatanganinya, dan string penandatanganan data yang Anda hitung.

1. Dapatkan file tanda.
2. Verifikasi bahwa file tanda telah diambil dari lokasi aslinya.
3. Dapatkan tanda tangan heksadesimal yang dikodekan dari file tanda.
4. Dapatkan sidik jari yang dikodekan heksadesimal dari kunci publik yang kunci pribadinya digunakan untuk menandatangani file tanda.
5. Ambil kunci publik untuk rentang waktu yang sesuai dengan `queryCompleteTime` dalam file tanda. Untuk rentang waktu, pilih yang `StartTime` lebih awal dari `queryCompleteTime` dan yang lebih `EndTime` lambat dari`queryCompleteTime`.
6. Dari antara kunci publik yang diambil, pilih kunci publik yang sidik jarinya cocok dengan `publicKeyFingerprint` nilai dalam file tanda.

7. Menggunakan daftar hash yang berisi nilai hash untuk setiap file hasil kueri yang dipisahkan oleh spasi, buat ulang string penandatanganan data yang digunakan untuk memverifikasi tanda tangan file. File tanda mencantumkan `fileHashValue` untuk setiap file hasil kueri.

   Misalnya, jika `files` array file tanda Anda berisi tiga file hasil kueri berikut, daftar hash Anda adalah “aaa bbb ccc”.

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

   },
   {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

   },
   {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

   }
],
```

8. Validasi tanda tangan dengan meneruskan hash SHA-256 dari string, kunci publik, dan tanda tangan sebagai parameter ke algoritma verifikasi tanda tangan RSA. Jika hasilnya benar, file tanda valid.

Validasi file hasil kueri

Jika file tanda valid, validasi file hasil kueri yang menjadi referensi file tanda. Untuk memvalidasi integritas file hasil kueri, hitung nilai hash SHA-256 pada konten terkompresi dan bandingkan

hasilnya dengan file hasil kueri yang `fileHashValue` direkam dalam file tanda. Jika hash cocok, file hasil kueri valid.

Bagian berikut menjelaskan proses validasi secara rinci.

A. Dapatkan berkas tanda

Langkah pertama adalah mendapatkan file tanda dan mendapatkan sidik jari kunci publik.

1. Dapatkan file tanda dari bucket Amazon S3 Anda untuk hasil kueri yang ingin Anda validasi.
2. Selanjutnya, dapatkan `hashSignature` nilai dari file tanda.
3. Dalam file tanda, dapatkan sidik jari kunci publik yang kunci pribadinya digunakan untuk menandatangani file dari `publicKeyFingerprint` bidang.

B. Ambil kunci publik untuk memvalidasi file tanda

Untuk mendapatkan kunci publik untuk memvalidasi file tanda, Anda dapat menggunakan salah satu AWS CLI atau CloudTrail API. Dalam kedua kasus, Anda menentukan rentang waktu (yaitu, waktu mulai dan waktu akhir) untuk file tanda yang ingin Anda validasi. Gunakan rentang waktu yang sesuai dengan `queryCompleteTime` dalam file tanda. Satu atau beberapa kunci publik dapat dikembalikan untuk rentang waktu yang Anda tentukan. Kunci yang dikembalikan mungkin memiliki rentang waktu validitas yang tumpang tindih.

> **Note**
>
> Karena CloudTrail menggunakan pasangan private/public kunci yang berbeda per Wilayah, setiap file tanda ditandatangani dengan kunci pribadi yang unik untuk Wilayahnya. Oleh karena itu, ketika Anda memvalidasi file tanda dari Wilayah tertentu, Anda harus mengambil kunci publiknya dari Wilayah yang sama.

Gunakan tombol AWS CLI untuk mengambil kunci publik

Untuk mengambil kunci publik untuk file tanda dengan menggunakan AWS CLI, gunakan `cloudtrail list-public-keys` perintah. Perintah memiliki format berikut:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time
<end-time>]
```

Parameter waktu mulai dan akhir waktu adalah stempel waktu UTC dan bersifat opsional. Jika tidak ditentukan, waktu saat ini digunakan, dan kunci publik atau kunci yang saat ini aktif dikembalikan.

Sampel Respon

Responsnya akan berupa daftar objek JSON yang mewakili kunci (atau kunci) yang dikembalikan:

Gunakan CloudTrail API untuk mengambil kunci publik

Untuk mengambil kunci publik untuk file tanda menggunakan CloudTrail API, teruskan nilai waktu mulai dan waktu akhir ke `ListPublicKeys` API. `ListPublicKeys`API mengembalikan kunci publik yang kunci pribadinya digunakan untuk menandatangani file dalam rentang waktu yang ditentukan. Untuk setiap kunci publik, API juga mengembalikan sidik jari yang sesuai.

`ListPublicKeys`

Bagian ini menjelaskan parameter permintaan dan elemen respons untuk `ListPublicKeys` API.

> **Note**
>
> Pengkodean untuk bidang biner `ListPublicKeys` untuk dapat berubah.

Parameter Permintaan

Nama	Deskripsi
`StartTime`	Secara opsional menentukan, di UTC, awal rentang waktu untuk mencari kunci publik untuk CloudTrail file tanda. Jika tidak StartTime ditentukan, waktu saat ini digunakan, dan kunci publik saat ini dikembalikan. Jenis: DateTime
`EndTime`	Secara opsional menentukan, di UTC, akhir rentang waktu untuk mencari kunci publik untuk file tanda tangan. CloudTrail Jika tidak EndTime ditentukan, waktu saat ini digunakan. Jenis: DateTime

Elemen Respon

`PublicKeyList`, array `PublicKey` objek yang berisi:

Nama	Deskripsi
`Value`	DER menyandikan nilai kunci publik dalam format PKCS #1. Jenis: Gumpalan
`ValidityStartTime`	Waktu mulai validitas kunci publik. Jenis: DateTime
`ValidityEndTime`	Waktu berakhirnya validitas kunci publik. Jenis: DateTime
`Fingerprint`	Sidik jari kunci publik. Sidik jari dapat digunakan untuk mengidentifikasi kunci publik yang harus Anda gunakan untuk memvalidasi file tanda. Tipe: String

C. Pilih kunci publik yang akan digunakan untuk validasi

Dari antara kunci publik yang diambil oleh `list-public-keys` atau`ListPublicKeys`, pilih kunci publik yang sidik jarinya cocok dengan sidik jari yang direkam di `publicKeyFingerprint` bidang file tanda. Ini adalah kunci publik yang akan Anda gunakan untuk memvalidasi file tanda.

D. Buat ulang string penandatanganan data

Sekarang setelah Anda memiliki tanda tangan dari file tanda dan kunci publik terkait, Anda perlu menghitung string penandatanganan data. Setelah menghitung string penandatanganan data, Anda akan memiliki input yang diperlukan untuk memverifikasi tanda tangan.

String penandatanganan data terdiri dari nilai hash untuk setiap file hasil kueri yang dipisahkan oleh spasi. Setelah Anda membuat ulang string ini, Anda dapat memvalidasi file tanda.

E. Validasi file tanda

Teruskan string penandatanganan data yang dibuat ulang, tanda tangan digital, dan kunci publik ke algoritma verifikasi tanda tangan RSA. Jika output benar, tanda tangan dari file tanda diverifikasi dan file tanda valid.

F. Validasi file hasil query

Setelah Anda memvalidasi file tanda, Anda dapat memvalidasi file hasil kueri yang direferensikan. File tanda berisi hash SHA-256 dari file hasil kueri. Jika salah satu file hasil kueri diubah setelah CloudTrail dikirimkan, hash SHA-256 akan berubah, dan tanda tangan file tanda tidak akan cocok.

Gunakan prosedur berikut untuk memvalidasi file hasil kueri yang tercantum dalam `files` array file tanda.

1. Ambil hash asli file dari `files.fileHashValue` bidang di file tanda.
2. Hash konten terkompresi dari file hasil kueri dengan algoritma hashing yang ditentukan dalam. `hashAlgorithm`
3. Bandingkan nilai hash yang Anda buat untuk setiap file hasil kueri dengan file tanda `files.fileHashValue` di. Jika hash cocok, file hasil kueri valid.

Memvalidasi tanda tangan dan file hasil kueri secara offline

Saat memvalidasi file hasil tanda dan kueri secara offline, Anda biasanya dapat mengikuti prosedur yang dijelaskan di bagian sebelumnya. Namun, Anda harus mempertimbangkan informasi berikut tentang kunci publik.

Kunci publik

Untuk memvalidasi offline, kunci publik yang Anda butuhkan untuk memvalidasi file hasil kueri dalam rentang waktu tertentu harus diperoleh terlebih dahulu secara online (dengan meneleponListPublicKeys, misalnya) dan kemudian disimpan secara offline. Langkah ini harus diulang setiap kali Anda ingin memvalidasi file tambahan di luar rentang waktu awal yang Anda tentukan.

Contoh cuplikan validasi

Cuplikan sampel berikut menyediakan kode kerangka untuk memvalidasi file hasil CloudTrail tanda dan kueri. Kode kerangka online/offline agnostik; artinya, terserah Anda untuk memutuskan apakah akan menerapkannya dengan atau tanpa konektivitas online ke. AWS Implementasi yang disarankan menggunakan Java Cryptography Extension (JCE) dan Bouncy Castle sebagai penyedia keamanan.

Cuplikan sampel menunjukkan:

- Cara membuat string penandatanganan data yang digunakan untuk memvalidasi tanda tangan file.

- Cara memverifikasi tanda tangan file tanda tangan.
- Cara menghitung nilai hash untuk file hasil kueri dan membandingkannya dengan yang `fileHashValue` tercantum dalam file tanda untuk memverifikasi keaslian file hasil kueri.

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");
```

```
       for (int i = 0; i < jsonArray.length(); i++) {
           JSONObject file = jsonArray.getJSONObject(i);
           String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

           // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
           byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3ObjectKey);
           messageDigest.update(exportFileContent);
           byte[] exportFileHash = messageDigest.digest();
           messageDigest.reset();
           byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

           boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
           if (!signaturesMatch) {
               System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                       s3Bucket, fileS3ObjectKey,
                       Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
           } else {
               System.out.println(String.format("Export file: %s/%s hash match",
                       s3Bucket, fileS3ObjectKey));
           }

           hashList.add(file.getString("fileHashValue"));
       }
       String hashListString = hashList.stream().collect(Collectors.joining(" "));

       /*
           NOTE:
           To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
           of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
           returned from ListPublicKey API are DER encoded in PKCS#1 format:

           PublicKeyInfo ::= SEQUENCE {
               algorithm       AlgorithmIdentifier,
               PublicKey       BIT STRING
           }
```

```
            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
 getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
 AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
 rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

Optimalkan kueri CloudTrail Danau

Halaman ini memberikan panduan tentang cara mengoptimalkan kueri CloudTrail Danau untuk meningkatkan kinerja dan keandalan. Ini mencakup teknik pengoptimalan khusus serta solusi untuk kegagalan kueri umum.

Topik

- Rekomendasi untuk mengoptimalkan kueri
- Solusi untuk kegagalan kueri

Rekomendasi untuk mengoptimalkan kueri

Ikuti rekomendasi di bagian ini untuk mengoptimalkan kueri Anda.

Rekomendasi:

- Optimalkan agregasi
- Gunakan teknik aproksimasi
- Batasi hasil kueri
- Optimalkan kueri LIKE
- Gunakan UNION ALL sebagai pengganti UNION
- Sertakan hanya kolom yang diperlukan
- Kurangi ruang lingkup fungsi jendela

Optimalkan agregasi

Mengecualikan kolom redundan dalam GROUP BY klausa dapat meningkatkan kinerja karena lebih sedikit kolom membutuhkan lebih sedikit memori. Misalnya, dalam query berikut, kita dapat menggunakan `arbitrary` fungsi pada kolom redundan seperti `eventType` untuk meningkatkan kinerja. `arbitrary`Fungsi pada `eventType` digunakan untuk memilih nilai bidang secara acak dari grup karena nilainya sama dan tidak perlu disertakan dalam GROUP BY klausa.

```
SELECT eventName, eventSource, arbitrary(eventType), count(*)
FROM $EDS_ID
GROUP BY eventName, eventSource
```

Dimungkinkan untuk meningkatkan kinerja GROUP BY fungsi dengan mengurutkan daftar bidang dalam urutan penurunan jumlah nilai uniknya (kardinalitas). GROUP BY Misalnya, saat mendapatkan jumlah peristiwa dari suatu tipe di masing-masing Wilayah AWS, kinerja dapat ditingkatkan dengan menggunakan `awsRegion` urutan`eventName`, dalam GROUP BY fungsi alih-alih`awsRegion`, `eventName` karena ada nilai yang lebih unik `eventName` daripada yang ada`awsRegion`.

```
SELECT eventName, awsRegion, count(*)
```

```
FROM $EDS_ID
GROUP BY eventName, awsRegion
```

Gunakan teknik aproksimasi

Setiap kali nilai yang tepat tidak diperlukan untuk menghitung nilai yang berbeda, gunakan fungsi agregat perkiraan untuk menemukan nilai yang paling sering. Misalnya, `approx_distinct`menggunakan memori jauh lebih sedikit dan berjalan lebih cepat daripada `COUNT(DISTINCT fieldName)` operasi.

Batasi hasil kueri

Jika hanya respons sampel yang diperlukan untuk kueri, batasi hasilnya ke sejumlah kecil baris dengan menggunakan `LIMIT` kondisi. Jika tidak, kueri akan mengembalikan hasil yang besar dan membutuhkan lebih banyak waktu untuk eksekusi kueri.

Menggunakan `LIMIT` bersama dengan `ORDER BY` dapat memberikan hasil untuk catatan N atas atau bawah lebih cepat karena mengurangi jumlah memori yang dibutuhkan dan waktu yang dibutuhkan untuk mengurutkan.

```
SELECT * FROM $EDS_ID
ORDER BY eventTime
LIMIT 100;
```

Optimalkan kueri LIKE

Anda dapat menggunakan `LIKE` untuk menemukan string yang cocok, tetapi dengan string panjang, ini adalah komputasi intensif. `regexp_like`Fungsi ini dalam banyak kasus merupakan alternatif yang lebih cepat.

Seringkali, Anda dapat mengoptimalkan pencarian dengan menambatkan substring yang Anda cari. Misalnya, jika Anda mencari awalan, lebih baik menggunakan '`substr`%' daripada '% `substr` %' dengan `LIKE` operator dan '^`substr`' dengan fungsinya. `regexp_like`

Gunakan **`UNION ALL`** sebagai pengganti **`UNION`**

`UNION ALL`dan `UNION` dua cara untuk menggabungkan hasil dari dua kueri menjadi satu hasil tetapi `UNION` menghapus duplikat. `UNION`perlu memproses semua catatan dan menemukan duplikat, yang merupakan memori dan komputasi intensif, tetapi `UNION ALL` merupakan operasi yang relatif cepat. Kecuali Anda perlu menghapus duplikat catatan, gunakan `UNION ALL` untuk kinerja terbaik.

Sertakan hanya kolom yang diperlukan

Jika Anda tidak memerlukan kolom, jangan sertakan dalam kueri Anda. Semakin sedikit data yang harus diproses oleh kueri, semakin cepat ia akan berjalan. Jika Anda memiliki kueri yang dilakukan `SELECT *` di kueri terluar, Anda harus mengubah `*` ke daftar kolom yang Anda butuhkan.

`ORDER BY`Klausa mengembalikan hasil query dalam urutan diurutkan. Saat menyortir jumlah data yang lebih besar, jika memori yang diperlukan tidak tersedia, hasil yang diurutkan menengah ditulis ke disk yang dapat memperlambat eksekusi kueri. Jika Anda tidak benar-benar membutuhkan hasil Anda untuk diurutkan, hindari menambahkan `ORDER BY` klausa. Selain itu, hindari `ORDER BY` menambahkan kueri batin jika tidak benar-benar diperlukan.

Kurangi ruang lingkup fungsi jendela

Fungsi jendela menyimpan semua catatan yang mereka operasikan dalam memori untuk menghitung hasilnya. Ketika jendela sangat besar, fungsi jendela bisa kehabisan memori. Untuk memastikan bahwa kueri berjalan dalam batas memori yang tersedia, kurangi ukuran jendela tempat fungsi jendela Anda beroperasi dengan menambahkan `PARTITION BY` klausa.

Terkadang kueri dengan fungsi jendela dapat ditulis ulang tanpa fungsi jendela. Misalnya, alih-alih menggunakan `row_number` atau`rank`, Anda dapat menggunakan fungsi agregat seperti `max_by`atau `min_by`.

Kueri berikut menemukan alias yang terakhir ditugaskan ke setiap kunci KMS menggunakan. `max_by`

```
SELECT element_at(requestParameters, 'targetKeyId') as keyId,
max_by(element_at(requestParameters, 'aliasName'), eventTime) as mostRecentAlias
FROM $EDS_ID
WHERE eventsource = 'kms.amazonaws.com'
AND eventName in ('CreateAlias', 'UpdateAlias')
AND eventTime > DATE_ADD('week', -1, CURRENT_TIMESTAMP)
GROUP BY element_at(requestParameters, 'targetKeyId')
```

Dalam hal ini, `max_by` fungsi mengembalikan alias untuk catatan dengan waktu acara terbaru dalam grup. Kueri ini berjalan lebih cepat dan menggunakan lebih sedikit memori daripada kueri setara dengan fungsi jendela.

Solusi untuk kegagalan kueri

Bagian ini menyediakan solusi untuk kegagalan kueri umum.

Kegagalan kueri:

- Kueri gagal karena responsnya terlalu besar
- Kueri gagal karena kehabisan sumber daya

Kueri gagal karena responsnya terlalu besar

Kueri dapat gagal jika responsnya terlalu besar sehingga menghasilkan pesan**`Query response is too large`**. Jika ini terjadi, Anda dapat mengurangi ruang lingkup agregasi.

Fungsi agregasi seperti `array_agg` dapat menyebabkan setidaknya satu baris dalam respons kueri menjadi sangat besar menyebabkan kueri gagal. Misalnya, menggunakan `array_agg(eventName)` instead of `array_agg(DISTINCT eventName)` akan meningkatkan ukuran respons banyak karena nama acara yang digandakan dari CloudTrail peristiwa yang dipilih.

Kueri gagal karena kehabisan sumber daya

Jika memori yang cukup tidak tersedia selama pelaksanaan operasi intensif memori seperti gabungan, agregasi dan fungsi jendela, hasil antara tumpah ke disk, tetapi tumpahan memperlambat eksekusi kueri dan tidak cukup untuk mencegah kueri gagal. **`Query exhausted resources at this scale factor`** Ini dapat diperbaiki dengan mencoba kembali kueri.

Jika kesalahan di atas tetap ada bahkan setelah mengoptimalkan kueri, Anda dapat mencatat kueri menggunakan peristiwa dan menjalankan kueri beberapa kali dalam interval yang lebih kecil dari rentang waktu kueri asli. `eventTime`

Jalankan dan kelola kueri CloudTrail Lake dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk menjalankan dan mengelola kueri CloudTrail Danau Anda. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wilayah AWS konfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Perintah yang tersedia untuk kueri CloudTrail Lake

Perintah untuk menjalankan dan mengelola kueri di CloudTrail Lake meliputi:

- `start-query`untuk menjalankan kueri.
- `describe-query`untuk mengembalikan metadata tentang kueri.

- `generate-query`untuk menghasilkan kueri dari prompt bahasa Inggris. Untuk informasi selengkapnya, lihat Buat kueri CloudTrail Danau dari petunjuk bahasa alami.
- `get-query-results`untuk mengembalikan hasil kueri untuk ID kueri yang ditentukan.
- `list-queries`untuk mendapatkan kueri daftar untuk penyimpanan data peristiwa tertentu.
- `cancel-query`untuk membatalkan kueri yang sedang berjalan.

Untuk daftar perintah yang tersedia untuk penyimpanan data acara CloudTrail Lake, lihatPerintah yang tersedia untuk penyimpanan data acara.

Untuk daftar perintah yang tersedia untuk dasbor CloudTrail Lake, lihatPerintah yang tersedia untuk dasbor.

Untuk daftar perintah yang tersedia untuk integrasi CloudTrail Lake, lihatPerintah yang tersedia untuk integrasi CloudTrail Lake.

Menghasilkan kueri dari prompt bahasa alami dengan AWS CLI

Jalankan `generate-query` perintah untuk menghasilkan kueri dari prompt bahasa Inggris. Untuk`--event-data-stores`, berikan ARN (atau akhiran ID ARN) dari penyimpanan data acara yang ingin Anda kueri. Anda hanya dapat menentukan satu penyimpanan data acara. Untuk`--prompt`, berikan prompt dalam bahasa Inggris.

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

Jika berhasil, perintah mengeluarkan pernyataan SQL dan memberikan `QueryAlias` yang akan Anda gunakan dengan `start-query` perintah untuk menjalankan kueri terhadap penyimpanan data acara Anda.

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

Mulai kueri dengan AWS CLI

AWS CLI start-queryPerintah contoh berikut menjalankan kueri pada penyimpanan data peristiwa yang ditentukan sebagai ID dalam pernyataan kueri dan mengirimkan hasil kueri ke bucket S3 tertentu. `--query-statement`Parameter menyediakan query SQL, terlampir dalam tanda kutip tunggal. Parameter opsional termasuk`--delivery-s3-uri`, untuk mengirimkan hasil kueri ke bucket S3 tertentu. Untuk informasi selengkapnya tentang bahasa kueri yang dapat Anda gunakan di CloudTrail Lake, lihatCloudTrail Kendala Lake SQL.

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3-uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

Responsnya adalah `QueryId` string. Untuk mendapatkan status kueri, jalankan describe-query menggunakan `QueryId` nilai yang dikembalikan olehstart-query. Jika kueri berhasil, Anda dapat menjalankan get-query-results untuk mendapatkan hasil.

Keluaran

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
}
```

> **Note**
>
> Kueri yang berjalan lebih dari satu jam mungkin habis. Anda masih bisa mendapatkan sebagian hasil yang diproses sebelum waktu kueri habis.
> Jika Anda mengirimkan hasil kueri ke bucket S3 menggunakan `--delivery-s3-uri` parameter opsional, kebijakan bucket harus memberikan CloudTrail izin untuk mengirimkan hasil kueri ke bucket. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake.

Dapatkan metadata tentang kueri dengan AWS CLI

Contoh AWS CLI describe-query perintah berikut mendapatkan metadata tentang kueri, termasuk waktu menjalankan kueri dalam milidetik, jumlah peristiwa yang dipindai dan dicocokkan, jumlah total byte yang dipindai, dan status kueri. `BytesScanned`Nilai cocok dengan jumlah byte yang akun Anda

ditagih untuk kueri, kecuali kueri masih berjalan. Jika hasil kueri dikirim ke bucket S3, respons juga menyediakan URI S3 dan status pengiriman.

Anda harus menentukan nilai untuk parameter `--query-id` atau `--query-alias` parameter. Menentukan `--query-alias` parameter mengembalikan informasi tentang query terakhir yang dijalankan untuk alias.

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Berikut ini adalah contoh respons.

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
    }
}
```

Dapatkan hasil kueri dengan AWS CLI

Contoh AWS CLI get-query-results perintah berikut mendapatkan hasil data peristiwa dari query. Anda harus menentukan yang `--query-id` dikembalikan oleh start-query perintah. `BytesScanned`Nilai cocok dengan jumlah byte yang akun Anda ditagih untuk kueri, kecuali kueri masih berjalan. Parameter opsional termasuk`--max-query-results`, untuk menentukan jumlah maksimum hasil yang Anda inginkan perintah untuk kembali pada satu halaman. Jika ada lebih banyak hasil daripada `--max-query-results` nilai yang Anda tentukan, jalankan perintah lagi dengan menambahkan `NextToken` nilai yang dikembalikan untuk mendapatkan halaman hasil berikutnya.

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Keluaran

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

Cantumkan semua kueri di toko data acara dengan AWS CLI

Contoh AWS CLI list-queries perintah berikut mengembalikan daftar query dan status query pada penyimpanan data peristiwa tertentu selama tujuh hari terakhir. Anda harus menentukan ARN atau akhiran ID dari nilai ARN untuk. `--event-data-store` Secara opsional, untuk mempersingkat daftar hasil, Anda dapat menentukan rentang waktu, diformat sebagai stempel waktu, dengan menambahkan `--start-time` dan `--end-time` parameter, dan nilai. `--query-status` Nilai yang valid untuk `QueryStatus` include`QUEUED`,`RUNNING`,`FINISHED`,`FAILED`, atau`CANCELLED`.

list-queriesjuga memiliki parameter pagination opsional. Gunakan `--max-results` untuk menentukan jumlah maksimum hasil yang Anda inginkan perintah untuk kembali pada satu halaman. Jika ada lebih banyak hasil daripada `--max-results` nilai yang Anda tentukan, jalankan perintah lagi dengan menambahkan `NextToken` nilai yang dikembalikan untuk mendapatkan halaman hasil berikutnya.

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

Keluaran

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

Batalkan kueri yang sedang berjalan dengan AWS CLI

Contoh AWS CLI cancel-query perintah berikut membatalkan query dengan status. `RUNNING` Anda harus menentukan nilai untuk `--query-id`. Saat Anda menjalankancancel-query, status kueri mungkin akan ditampilkan `CANCELLED` meskipun cancel-query operasi belum selesai.

> **Note**
>
> Kueri yang dibatalkan dapat dikenakan biaya. Akun Anda masih dikenakan biaya untuk jumlah data yang dipindai sebelum Anda membatalkan kueri.

Berikut ini adalah contoh CLI.

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

Keluaran

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail Kendala Lake SQL

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

CloudTrail Kueri danau adalah string SQL. Bagian ini memberikan informasi tentang fungsi, operator, dan skema yang didukung.

Hanya `SELECT` pernyataan yang diizinkan. Tidak ada string kueri yang dapat mengubah atau mengubah data.

Sintaks CloudTrail Lake untuk `SELECT` pernyataan adalah sebagai berikut. ID penyimpanan data peristiwa — bagian ID dari ARN penyimpanan data peristiwa — ditentukan untuk nilainya. `FROM`

```
SELECT [ DISTINCT ] columns [ Aggregate ]
[ FROM table event_data_store_ID]
[ WHERE columns [ Conditions ] ]
[ GROUP BY columns [ DISTINCT | Aggregate ] ]
[ HAVING columns [ Aggregate | Conditions ] ]
[ ORDER BY columns [ Aggregate | ASC | DESC | NULLS | FIRST | LAST ]
[ LIMIT [ INT ] ]
```

CloudTrail Lake mendukung semua `SELECT` pernyataan, fungsi, dan operator Trino SQL yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Trino.

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri. Untuk informasi selengkapnya, lihat Lihat contoh kueri dengan konsol CloudTrail.

Untuk informasi tentang cara mengoptimalkan kueri Anda, lihatOptimalkan kueri CloudTrail Danau.

Topik

- Fungsi, kondisi, dan bergabung dengan operator yang didukung
- Dukungan kueri multi-tabel tingkat lanjut

Fungsi, kondisi, dan bergabung dengan operator yang didukung

Fungsi yang didukung

CloudTrail Danau mendukung semua fungsi Trino. Untuk informasi selengkapnya tentang fungsi yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Trino.

Operator kondisi yang didukung

Berikut ini adalah operator kondisi yang didukung.

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

Operator bergabung yang didukung

Berikut ini adalah `JOIN` operator yang didukung. Untuk informasi selengkapnya tentang menjalankan kueri multi-tabel, lihat. Dukungan kueri multi-tabel tingkat lanjut

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

Dukungan kueri multi-tabel tingkat lanjut

CloudTrail Lake mendukung bahasa kueri tingkat lanjut di beberapa penyimpanan data acara.

- `UNION|UNION ALL|EXCEPT|INTERSECT`
- `LEFT|RIGHT|INNER JOIN`

Untuk menjalankan kueri Anda, gunakan start-query perintah di file AWS CLI. Berikut ini adalah contoh, menggunakan salah satu contoh kueri di bagian ini.

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

Responsnya adalah `QueryId` string. Untuk mendapatkan status kueri, jalankan`describe-query`, menggunakan `QueryId` nilai yang dikembalikan oleh`start-query`. Jika kueri berhasil, Anda dapat menjalankan `get-query-results` untuk mendapatkan hasil.

`UNION|UNION ALL|EXCEPT|INTERSECT`

Berikut ini adalah contoh query yang menggunakan `UNION` dan `UNION ALL` untuk menemukan peristiwa dengan ID acara dan nama acara mereka di tiga penyimpanan data acara, EDS1, EDS2, dan EDS3. Hasilnya dipilih dari setiap penyimpanan data peristiwa terlebih dahulu, kemudian hasilnya digabungkan, diurutkan berdasarkan ID peristiwa, dan dibatasi hingga sepuluh peristiwa.

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

`LEFT|RIGHT|INNER JOIN`

Berikut ini adalah contoh kueri yang digunakan `LEFT JOIN` untuk menemukan semua peristiwa dari penyimpanan data peristiwa bernama`eds2`, dipetakan ke`edsB`, yang cocok dengan yang ada

di penyimpanan data peristiwa utama (kiri),`edsA`. Peristiwa yang dikembalikan terjadi pada atau sebelum 1 Januari 2020, dan hanya nama acara yang dikembalikan.

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

Skema SQL yang didukung untuk penyimpanan data acara

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

Bagian berikut menyediakan skema SQL yang didukung untuk setiap jenis penyimpanan data peristiwa.

Topik

- Skema yang didukung untuk bidang catatan CloudTrail acara
- Skema yang didukung untuk bidang catatan acara CloudTrail Insights
- Skema yang didukung untuk AWS Config file catatan item konfigurasi
- Skema yang didukung untuk laporan catatan AWS Audit Manager bukti
- Skema yang didukung untuk bidang AWS non-acara

Skema yang didukung untuk bidang catatan CloudTrail acara

Berikut ini adalah skema SQL yang valid untuk CloudTrail bidang catatan peristiwa manajemen, data, dan aktivitas jaringan. Untuk informasi selengkapnya tentang bidang catatan CloudTrail peristiwa, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

```
[
```

```
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
"struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,

username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,

ec2issuedinvpc:string>,onbehalfof:struct<userid:string,identitystorearn:string>,

inscopeof:struct<sourcearn:string,sourceaccount:string,issuertype:string,
                credentiaisissuedto:string>,invokedby:string,identityprovider:string>"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "eventsource",
        "Type": "string"
    },
    {
        "Name": "eventname",
        "Type": "string"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "sourceipaddress",
        "Type": "string"
    },
    {
        "Name": "useragent",
```

```
        "Type": "string"
    },
    {
        "Name": "errorcode",
        "Type": "string"
    },
    {
        "Name": "errormessage",
        "Type": "string"
    },
    {
        "Name": "requestparameters",
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
```

```
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "vpcendpointaccountid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
```

```
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
    {
        "Name": "eventjsoncheckсum",
        "Type": "string"
    }
]
```

Skema yang didukung untuk bidang catatan acara CloudTrail Insights

Berikut ini adalah skema SQL yang valid untuk bidang catatan peristiwa Insights. Untuk peristiwa Wawasan, nilai `eventcategory` is`Insight`, dan nilai `eventtype` is`AwsCloudTrailInsight`. Untuk deskripsi bidang ini, lihat[CloudTrail merekam konten untuk acara Wawasan untuk penyimpanan data acara](#).

> **Note**
>
> Bidang `insightvalueinsightaverage`,`baselinevalue`, dan `baselineaverage` bidang dalam `attributions` bidang `insightContext` akan mulai tidak digunakan lagi pada 23 Juni 2025.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
```

```
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
```

```
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type": "struct<baselineaverage:double,insightaverage:double,
                 baselineduration:integer,insightduration:integer,
                 attributions:struct<attribute:string,insightvalue:string,
                 insightaverage:double,baselinevalue:string,baselineaverage:double,
                 insight:struct<value:string,average:double>,
                 baseline:struct<value:string,average:double>>>"
    }
]
```

Skema yang didukung untuk AWS Config file catatan item konfigurasi

Berikut ini adalah skema SQL yang valid untuk bidang catatan item konfigurasi. Untuk item konfigurasi, nilai `eventcategory` is`ConfigurationItem`, dan nilai `eventtype` is`AwsConfigurationItem`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
```

```
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,

 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

Skema yang didukung untuk laporan catatan AWS Audit Manager bukti

Berikut ini adalah skema SQL yang valid untuk bidang catatan bukti Audit Manager. Untuk bidang catatan bukti Audit Manager, nilai `eventcategory` is`Evidence`, dan nilai `eventtype` is`AwsAuditManagerEvidence`. Untuk informasi selengkapnya tentang mengumpulkan bukti di CloudTrail Lake menggunakan Audit Manager, lihat Pencari bukti di AWS Audit Manager Panduan Pengguna.

```
[
```

```
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
"struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

compliancecheck:string,datasource:string,eventname:string,eventsource:string,

evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,
```

```
 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                 evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

Skema yang didukung untuk bidang AWS non-acara

Berikut ini adalah skema SQL yang valid untuk AWS non-event. Untuk AWS non-peristiwa, nilai `eventcategory` is`ActivityAuditLog`, dan nilai `eventtype` is`ActivityLog`.

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
```

```
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

CloudWatch Metrik yang didukung

> **Note**
>
> AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus menggunakan layanan ini seperti biasa. Untuk informasi selengkapnya, lihat CloudTrail Perubahan ketersediaan danau.

CloudTrail Lake mendukung CloudWatch metrik Amazon. CloudWatch adalah layanan pemantauan untuk AWS sumber daya. Anda dapat menggunakannya CloudWatch untuk mengumpulkan dan melacak metrik, menyetel alarm, dan bereaksi secara otomatis terhadap perubahan sumber daya Anda AWS .

`AWS/CloudTrail`Namespace mencakup metrik berikut untuk Lake. CloudTrail

Metrik	Deskripsi	Unit
`HourlyDataIngested`	Jumlah data yang tertelan ke dalam penyimpanan data acara selama satu jam terakhir. Metrik ini diperbarui setiap jam. Metrik ini tersedia untuk semua jenis penyimpanan data peristiwa.	Byte
`TotalDataRetained`	Jumlah data yang disimpan dalam penyimpanan data peristiwa selama seluruh periode retensi. Metrik ini diperbarui setiap malam. Metrik ini tersedia untuk semua jenis penyimpanan data peristiwa.	Byte
`TotalStorageBytes`	Total byte terkompresi dalam penyimpanan data acara pada hari ini. Metrik ini tersedia untuk semua jenis penyimpanan data peristiwa.	Byte
`TotalPaidStorageBytes`	Untuk penyimpanan data peristiwa menggunakan opsi harga retensi yang dapat diperpanjang satu tahun, ini adalah total byte terkompresi setelah 366 hari hingga periode retensi maksimum	Byte

Metrik	Deskripsi	Unit
	yang dikonfigurasi untuk penyimpanan data acara. Untuk penyimpanan data acara menggunakan opsi harga retensi yang dapat diperpanjang satu tahun, penyimpanan disertakan tanpa biaya tambahan dengan harga konsumsi untuk 366 hari pertama, yang merupakan periode retensi default untuk penyimpanan data acara. Setelah 366 hari, penyimpan an. pay-as-you-go Untuk informasi tentang harga, lihat AWS CloudTrail Harga. Metrik ini hanya tersedia untuk penyimpanan data acara menggunakan opsi harga retensi yang dapat diperpanj ang satu tahun.	
`HourlyEventsAnalyzed`	Jumlah total peristiwa yang dianalisis oleh CloudTrai l Wawasan di penyimpan an data acara. Metrik ini diperbarui setiap jam. Metrik ini untuk penyimpan an data CloudTrail peristiwa yang mengaktifkan CloudTrail Wawasan.	Hitungan

Untuk informasi selengkapnya tentang CloudWatch metrik, lihat topik berikut.

- Menggunakan CloudWatch metrik Amazon
- Menggunakan CloudWatch alarm Amazon

Bekerja dengan jalan CloudTrail setapak

Trails menangkap catatan AWS aktivitas, mengirimkan dan menyimpan peristiwa ini dalam bucket Amazon S3, dengan pengiriman opsional CloudWatch ke Log dan Amazon. EventBridge

Anda dapat mengirimkan satu salinan acara manajemen yang sedang berlangsung ke bucket S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga. Untuk informasi tentang harga Amazon S3, lihat Harga Amazon S3.

Anda dapat membuat jalur Multi-wilayah dan Single-region untuk Anda. Akun AWS

Jalur Multi-Wilayah

Saat Anda membuat jejak Multi-wilayah, CloudTrail merekam peristiwa di semua peristiwa Wilayah AWS yang diaktifkan di Anda Akun AWS dan mengirimkan file log CloudTrail peristiwa ke bucket S3 yang Anda tentukan. Sebagai praktik terbaik, kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Anda dapat mengonversi jejak wilayah Tunggal menjadi jejak Multi-wilayah dengan menggunakan. AWS CLI Lihat informasi selengkapnya di Memahami jalur Multi-wilayah dan Wilayah keikutsertaan, Membuat jejak dengan konsol, dan Mengkonversi jalur satu wilayah ke jalur multi-wilayah.

Jalur Wilayah Tunggal

Saat Anda membuat jejak wilayah Tunggal, hanya CloudTrail mencatat peristiwa di Wilayah tersebut. Kemudian mengirimkan file log CloudTrail peristiwa ke bucket Amazon S3 yang Anda tentukan. Anda hanya dapat membuat jejak wilayah Tunggal dengan menggunakan. AWS CLI Jika Anda membuat jalur tunggal tambahan, Anda dapat meminta jejak tersebut mengirimkan file log CloudTrail peristiwa ke bucket S3 yang sama atau ke bucket terpisah. Ini adalah opsi default saat Anda membuat jejak menggunakan AWS CLI atau CloudTrail API. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola jalur dengan AWS CLI.

> **Note**
>
> Untuk kedua jenis jalur, Anda dapat menentukan bucket Amazon S3 dari Wilayah mana pun.

Jika Anda telah membuat organisasi AWS Organizations, Anda dapat membuat jejak organisasi yang mencatat semua peristiwa untuk semua AWS akun di organisasi tersebut. Jalur organisasi dapat berlaku untuk semua AWS Wilayah, atau Wilayah saat ini. Jejak organisasi harus dibuat menggunakan akun manajemen atau akun administrator yang didelegasikan, dan ketika ditentukan sebagai berlaku untuk organisasi, secara otomatis diterapkan ke semua akun anggota dalam organisasi. Akun anggota dapat melihat jejak organisasi, tetapi tidak dapat memodifikasi atau menghapusnya. Secara default, akun anggota tidak memiliki akses ke file log untuk jejak organisasi di bucket Amazon S3. Lihat informasi yang lebih lengkap di Membuat jejak untuk sebuah organisasi.

Topik

- Membuat jejak untuk Anda Akun AWS
- Membuat jejak untuk sebuah organisasi
- Memahami jalur Multi-wilayah dan Wilayah keikutsertaan
- Menyalin acara jejak ke Danau CloudTrail
- Mendapatkan dan melihat file CloudTrail log Anda
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menggunakan AWS CloudTrail dengan antarmuka VPC endpoint
- Persyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS
- Akun AWS penutupan dan jalan setapak

Membuat jejak untuk Anda Akun AWS

Saat membuat jejak, Anda mengaktifkan pengiriman peristiwa yang sedang berlangsung sebagai file log ke bucket Amazon S3 yang Anda tentukan. Membuat jejak memiliki banyak manfaat, termasuk:

- Catatan peristiwa yang berlangsung selama 90 hari terakhir.
- Opsi untuk secara otomatis memantau dan alarm pada peristiwa tertentu dengan mengirimkan peristiwa log ke Amazon CloudWatch Logs.
- Opsi untuk menanyakan log dan menganalisis aktivitas AWS layanan dengan Amazon Athena.

Mulai 12 April 2019, Anda hanya dapat melihat jejak di AWS Wilayah tempat mereka mencatat peristiwa. Jika Anda membuat jejak Multi-wilayah, itu akan muncul di konsol di semua Wilayah AWS yang diaktifkan di akun Anda. Jika Anda membuat jejak yang hanya mencatat peristiwa di satu Wilayah, Anda dapat melihat dan mengelolanya hanya di Wilayah tersebut. Sebagai praktik terbaik,

kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Untuk membuat jejak wilayah Tunggal, Anda harus menggunakan. AWS CLI

Jika Anda menggunakan AWS Organizations, Anda dapat membuat jejak yang akan mencatat peristiwa untuk semua AWS akun di organisasi. Jejak dengan nama yang sama akan dibuat di setiap akun anggota, dan acara dari setiap jejak akan dikirimkan ke bucket Amazon S3 yang Anda tentukan.

> **Note**
>
> Hanya akun manajemen atau akun administrator yang didelegasikan untuk organisasi yang dapat membuat jejak untuk organisasi. Membuat jejak untuk organisasi secara otomatis memungkinkan integrasi antara CloudTrail dan Organizations. Untuk informasi selengkapnya, lihat Membuat jejak untuk sebuah organisasi.
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan attempted-to-deliver peristiwa ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Topik

- Membuat dan memperbarui jejak dengan konsol
- Membuat, memperbarui, dan mengelola jalur dengan AWS CLI
- Membuat beberapa jalur

Membuat dan memperbarui jejak dengan konsol

Anda dapat menggunakan CloudTrail konsol untuk membuat, memperbarui, atau menghapus jejak Anda. Jalur yang dibuat menggunakan konsol adalah Multi-region. Untuk membuat jejak yang mencatat peristiwa hanya dalam satu Wilayah AWS, gunakan file AWS CLI.

Anda dapat membuat hingga lima jalur untuk setiap Wilayah. Setelah membuat jejak, CloudTrail secara otomatis mulai mencatat panggilan API dan peristiwa terkait di akun Anda ke bucket Amazon S3 yang Anda tentukan.

Anda dapat mengubah pengaturan berikut untuk jejak Anda menggunakan CloudTrail konsol:

- Anda dapat mengubah lokasi bucket S3 dan menentukan awalan.

- Akun manajemen untuk AWS Organizations organisasi dapat mengubah jejak tingkat akun menjadi jejak organisasi, atau dapat mengubah jejak organisasi menjadi jejak tingkat akun.
- Anda dapat mengaktifkan atau menonaktifkan enkripsi kunci KMS.
- Anda dapat mengaktifkan atau menonaktifkan validasi file log. Validasi file log memungkinkan Anda menentukan apakah file log telah dimodifikasi, dihapus, atau tidak diubah setelah CloudTrail dikirimkan. Secara default, validasi file log diaktifkan.
- Anda dapat mengonfigurasi jejak untuk mengirim pemberitahuan ke topik Amazon SNS.
- Anda dapat mengonfigurasi jejak untuk mengirim peristiwa ke grup CloudWatch log Log. Baik grup log dan peran IAM harus ada di akun Anda sendiri.
- Anda dapat memperbarui setelan untuk acara manajemen, peristiwa data, peristiwa aktivitas jaringan, dan peristiwa Wawasan.
- Anda dapat menambahkan atau menghapus tag. Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi jejak Anda.

Menggunakan CloudTrail konsol untuk membuat atau memperbarui jejak memberikan keuntungan berikut.

- Jika ini adalah pertama kalinya Anda membuat jejak, menggunakan CloudTrail konsol memungkinkan Anda untuk melihat fitur dan opsi yang tersedia.
- Jika Anda mengonfigurasi jejak untuk mencatat peristiwa data, menggunakan CloudTrail konsol memungkinkan Anda melihat tipe data yang tersedia. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data.
- Jika Anda mengonfigurasi jejak ke peristiwa aktivitas jaringan, menggunakan CloudTrail konsol memungkinkan Anda melihat sumber peristiwa yang tersedia. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.

Untuk informasi spesifik untuk membuat jejak untuk organisasi di AWS Organizations, lihatMembuat jejak untuk sebuah organisasi.

Topik

- Membuat jejak dengan CloudTrail konsol
- Memperbarui jejak dengan CloudTrail konsol
- Menghapus jejak dengan konsol CloudTrail
- Mematikan pencatatan log untuk jejak

Membuat jejak dengan CloudTrail konsol

Jejak dapat diterapkan ke semua Wilayah AWS yang diaktifkan di Anda Akun AWS, atau dapat diterapkan ke satu Wilayah. Jejak yang berlaku untuk semua Wilayah AWS yang diaktifkan di Anda Akun AWS disebut sebagai jalur Multi-wilayah. Sebagai praktik terbaik, kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Anda hanya dapat membuat jejak wilayah Tunggal menggunakan operasi AWS CLI atau `CreateTrail`API.

> **Note**
>
> Setelah membuat jejak, Anda dapat mengonfigurasi yang lain Layanan AWS untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat AWS integrasi layanan dengan log CloudTrail.

Topik

- Membuat jejak dengan konsol
- Langkah selanjutnya

Membuat jejak dengan konsol

Gunakan prosedur berikut untuk membuat jejak Multi-wilayah. Untuk mencatat peristiwa di satu Wilayah (tidak disarankan), gunakan AWS CLI.

Untuk membuat CloudTrail jejak dengan Konsol Manajemen AWS

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada halaman beranda CloudTrail layanan, halaman Trails, atau bagian Trails pada halaman Dasbor, pilih Buat jejak.
3. Pada halaman Create Trail, untuk nama Trail, ketikkan nama untuk jejak Anda. Untuk informasi selengkapnya, lihat Persyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS.

4. Jika ini adalah jejak AWS Organizations organisasi, Anda dapat mengaktifkan jejak untuk semua akun di organisasi Anda. Untuk melihat opsi ini, Anda harus masuk ke konsol dengan pengguna atau peran di akun administrator manajemen atau yang didelegasikan. Agar berhasil membuat jejak organisasi, pastikan bahwa pengguna atau peran memiliki izin yang memadai. Untuk informasi selengkapnya, lihat Membuat jejak untuk sebuah organisasi.
5. Untuk lokasi Storage, pilih Create new S3 bucket untuk membuat bucket. Saat Anda membuat bucket, CloudTrail membuat dan menerapkan kebijakan bucket yang diperlukan. Jika Anda memilih untuk membuat bucket S3 baru, kebijakan IAM Anda harus menyertakan izin untuk `s3:PutEncryptionConfiguration` tindakan tersebut karena secara default enkripsi sisi server diaktifkan untuk bucket.

   > **Note**
   >
   > Jika Anda memilih Gunakan bucket S3 yang ada, tentukan bucket di nama bucket log Trail, atau pilih Browse untuk memilih bucket di akun Anda sendiri. Jika Anda ingin menggunakan bucket di akun lain, Anda harus menentukan nama bucket. Kebijakan bucket harus memberikan CloudTrail izin untuk menulis ke sana. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk CloudTrail.

   Untuk mempermudah menemukan log Anda, buat folder baru (juga dikenal sebagai awalan) di bucket yang ada untuk menyimpan CloudTrail log Anda. Masukkan awalan di Awalan.
6. Untuk SSE-KMS enkripsi file Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda dan mencerna file menggunakan SSE-KMS enkripsi alih-alih SSE-S3 enkripsi. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan SSE-KMS enkripsi, file log dan file digest Anda dienkripsi menggunakan enkripsi. SSE-S3 Untuk informasi selengkapnya tentang SSE-KMS enkripsi, lihat Menggunakan enkripsi sisi server dengan AWS Key Management Service (). SSE-KMS Untuk informasi selengkapnya tentang SSE-S3 enkripsi, lihat Menggunakan Server-Side Enkripsi dengan Kunci S3-Managed Enkripsi Amazon (SSE-S3).

   Jika Anda mengaktifkan SSE-KMS enkripsi, pilih New atau Existing AWS KMS key. Di AWS KMS Alias, tentukan alias, dalam format. `alias/` *`MyAliasName`* Untuk informasi lebih lanjut, lihatMemperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

> **Note**
>
> Anda juga dapat mengetikkan ARN kunci dari akun lain. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol. Kebijakan kunci harus mengizinkan penggunaan kunci CloudTrail untuk mengenkripsi file log dan mencerna file, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log atau mencerna file dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

7. Di Pengaturan tambahan, konfigurasikan yang berikut ini.

   a. Untuk validasi file Log, pilih Diaktifkan agar intisari log dikirimkan ke bucket S3 Anda. Anda dapat menggunakan file intisari untuk memverifikasi bahwa file log Anda tidak berubah setelah CloudTrail dikirimkan. Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas file log.

   b. Untuk pengiriman notifikasi SNS, pilih Diaktifkan untuk diberi tahu setiap kali log dikirimkan ke bucket Anda. CloudTrail menyimpan beberapa peristiwa dalam file log. Notifikasi SNS dikirim untuk setiap file log, bukan untuk setiap acara. Untuk informasi selengkapnya, lihat Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail.

      Jika Anda mengaktifkan notifikasi SNS, untuk Membuat topik SNS baru, pilih Baru untuk membuat topik, atau pilih Ada untuk menggunakan topik yang ada. Jika Anda membuat jejak Multi-wilayah, notifikasi SNS untuk pengiriman file log dari semua Wilayah yang diaktifkan akan dikirim ke satu topik SNS yang Anda buat.

      Jika Anda memilih Baru, CloudTrail menentukan nama untuk topik baru untuk Anda, atau Anda dapat mengetikkan nama. Jika Anda memilih yang ada, pilih topik SNS dari daftar drop-down. Anda juga dapat memasukkan ARN topik dari Wilayah lain atau dari akun dengan izin yang sesuai. Untuk informasi selengkapnya, lihat Kebijakan topik Amazon SNS untuk CloudTrail.

      Jika Anda membuat topik, Anda harus berlangganan topik untuk diberitahu tentang pengiriman file log. Anda dapat berlangganan dari konsol Amazon SNS. Karena frekuensi pemberitahuan, kami menyarankan Anda mengonfigurasi langganan untuk menggunakan antrian Amazon SQS untuk menangani notifikasi secara terprogram. Untuk informasi

lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

8. Secara opsional, konfigurasikan CloudTrail untuk mengirim file CloudWatch log ke Log dengan memilih Diaktifkan di CloudWatch Log. Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log.

   a. Jika Anda mengaktifkan integrasi dengan CloudWatch Log, pilih Baru untuk membuat grup log baru, atau Ada untuk menggunakan yang sudah ada. Jika Anda memilih Baru, CloudTrail menentukan nama untuk grup log baru untuk Anda, atau Anda dapat mengetikkan nama.

   b. Jika Anda memilih Ada, pilih grup log dari daftar drop-down.

   c. Pilih Baru untuk membuat peran IAM baru untuk izin mengirim log ke CloudWatch Log. Pilih Existing untuk memilih peran IAM yang ada dari daftar drop-down. Pernyataan kebijakan untuk peran baru atau yang sudah ada ditampilkan saat Anda memperluas dokumen Kebijakan. Untuk informasi selengkapnya tentang peran ini, silakan lihat Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

   > **Note**
   >
   > - Saat mengonfigurasi jejak, Anda dapat memilih bucket S3 dan topik SNS milik akun lain. Namun, jika Anda CloudTrail ingin mengirimkan peristiwa ke grup CloudWatch log Log, Anda harus memilih grup log yang ada di akun Anda saat ini.
   > - Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi menggunakan konsol. Administrator yang didelegasikan dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API.

9. Untuk Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke jejak Anda. Tag dapat membantu Anda mengidentifikasi CloudTrail jejak dan bucket Amazon S3 yang CloudTrail berisi file log. Anda kemudian dapat menggunakan grup sumber daya untuk CloudTrail sumber daya Anda. Untuk informasi selengkapnya, lihat AWS Resource Groups dan Tanda.

10. Pada halaman Pilih peristiwa log, pilih jenis acara yang ingin Anda log. Untuk acara Manajemen, lakukan hal berikut.

a. Untuk aktivitas API, pilih apakah Anda ingin jejak Anda mencatat peristiwa Baca, peristiwa Tulis, atau keduanya. Untuk informasi selengkapnya, lihat Peristiwa manajemen.

b. Pilih Kecualikan AWS KMS acara untuk memfilter AWS Key Management Service (AWS KMS) peristiwa dari jejak Anda. Pengaturan default adalah untuk memasukkan semua AWS KMS acara.

   Opsi untuk mencatat atau mengecualikan AWS KMS peristiwa hanya tersedia jika Anda mencatat peristiwa manajemen di jejak Anda. Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan AWS KMS peristiwa.

   AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Low-volume, AWS KMS tindakan yang relevan seperti`Disable`,`Delete`, dan `ScheduleKey` (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

   Untuk mengecualikan peristiwa bervolume tinggi seperti`Encrypt`,`Decrypt`, dan`GenerateDataKey`, tetapi masih mencatat peristiwa yang relevan seperti`Disable`, `Delete` dan`ScheduleKey`, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa.

c. Pilih Kecualikan peristiwa Amazon RDS Data API untuk memfilter peristiwa Amazon Relational Database Service Data Data API dari jejak Anda. Pengaturan default adalah untuk menyertakan semua peristiwa Amazon RDS Data API. Untuk informasi selengkapnya tentang peristiwa Amazon RDS Data API, lihat Pencatatan panggilan API Data dengan AWS CloudTrail di Panduan Pengguna Amazon RDS untuk Aurora.

11. Untuk mencatat peristiwa data, pilih Peristiwa data. Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

12. **Important**

    Langkah 12-16 adalah untuk mengonfigurasi peristiwa data menggunakan pemilih acara lanjutan, yang merupakan default. Penyeleksi acara tingkat lanjut memungkinkan Anda mengonfigurasi lebih banyak jenis sumber daya dan menawarkan kontrol halus atas peristiwa data mana yang ditangkap jejak Anda. Jika Anda memilih untuk menggunakan

pemilih acara dasar, selesaikan langkah-langkahnyaKonfigurasikan pengaturan peristiwa data menggunakan pemilih acara dasar, lalu kembali ke langkah 17 dari prosedur ini.

Untuk tipe Sumber Daya, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang jenis sumber daya yang tersedia, lihatPeristiwa data.

13. Pilih templat pemilih log. Anda dapat memilih template yang telah ditentukan sebelumnya, atau memilih Custom untuk menentukan kondisi koleksi acara Anda sendiri.

    Anda dapat memilih dari template yang telah ditentukan berikut:

    - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
    - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
    - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau `Write*` peristiwa.
    - Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
    - Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` ofAwsServiceEvent, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).

    > **Note**
    >
    > Memilih template yang telah ditentukan untuk bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain. Jika jejak hanya berlaku untuk satu Wilayah, memilih templat yang telah ditentukan sebelumnya yang mencatat semua bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS

Jika Anda membuat jejak Multi-wilayah, memilih templat yang telah ditentukan untuk fungsi Lambda memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.
Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

14. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.
15. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan `readOnly` pemilih.

- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk menyertakan atau mengecualikan peristiwa data apa pun yang dicatat CloudTrail, sepertiPutBucket,GetItem, atauGetSnapshotBlock.
- **`eventSource`**— Sumber acara untuk menyertakan atau mengecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk dikecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType`diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- Sesi CredentialFromConsole — Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- pengguna Identity.arn - Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.ARN`, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai. `resources.type`

  > **Note**
  >
  > Anda tidak dapat menggunakan `resources.ARN` bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

  Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Kunci tindakan, sumber daya, dan kondisi Layanan AWS di Referensi Otorisasi Layanan.

b. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data acara, Anda dapat mengatur bidang ke Resources.arn, mengatur operator untuk tidak memulai, lalu menempelkan ARN bucket S3 yang tidak ingin Anda catat peristiwa.

Untuk menambahkan bucket S3 kedua, pilih + Condition, lalu ulangi instruksi sebelumnya, tempelkan di ARN untuk atau jelajahi bucket yang berbeda.

Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

c. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan tentukan ARN dalam satu pemilih agar sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

16. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 12 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk jenis sumber daya.
17. Untuk mengaktifkan agregasi pada peristiwa data, pilih satu atau beberapa templat agregasi. Template ini menentukan bagaimana peristiwa data Anda akan diringkas. Anda dapat memilih dari template berikut:

    a. Aktivitas API untuk mendapatkan ringkasan 5 menit dari peristiwa data Anda berdasarkan panggilan API yang dilakukan. Gunakan ini untuk memahami pola penggunaan API Anda, termasuk frekuensi, penelepon, dan sumber.

    b. Akses Sumber Daya untuk mendapatkan pola aktivitas pada AWS sumber daya Anda. Gunakan ini untuk memahami bagaimana AWS sumber daya Anda diakses, berapa kali mereka diakses di jendela 5 menit, siapa yang mengakses sumber daya, dan tindakan apa yang sedang dilakukan.

    c. Tindakan Pengguna untuk mendapatkan pola aktivitas berdasarkan prinsip IAM yang melakukan panggilan API di akun Anda.

> **Note**
>
> Agregasi berlaku untuk semua peristiwa data yang dikumpulkan di jejak Anda.

18. Untuk mencatat peristiwa aktivitas jaringan, pilih Acara aktivitas jaringan. Peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

    Untuk mencatat peristiwa aktivitas jaringan, lakukan hal berikut:

    a. Dari sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

    b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua peristiwa yang ditolak akses aktivitas jaringan, atau memilih Kustom untuk membuat pemilih log kustom untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

    c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

    d. Di Penyeleksi acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

        i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

        - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
        - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
        - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan`vpcEndpointId`.

        ii. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi.

iii. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

e. Untuk menambahkan sumber peristiwa lain yang ingin Anda log peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

19. Pilih acara Insights jika Anda ingin jejak Anda mencatat peristiwa CloudTrail Wawasan.

    Di Jenis acara, pilih Acara Wawasan. Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.

    CloudTrail Wawasan menganalisis peristiwa manajemen untuk aktivitas yang tidak biasa, dan mencatat peristiwa saat anomali terdeteksi. Secara default, jejak tidak mencatat peristiwa Wawasan. Untuk informasi selengkapnya tentang peristiwa Wawasan, lihatBekerja dengan CloudTrail Wawasan. Biaya tambahan berlaku untuk acara logging Insights. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

    Peristiwa Insights dikirimkan ke folder berbeda bernama `/CloudTrail-Insight` bucket S3 yang sama yang ditentukan di area lokasi penyimpanan halaman detail jejak. CloudTrailmenciptakan awalan baru untuk Anda. Misalnya, jika bucket S3 tujuan Anda saat ini diberi nama`amzn-s3-demo-bucket/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`

20. Setelah selesai memilih jenis acara untuk dicatat, pilih Berikutnya.

21. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit di bagian untuk mengubah pengaturan jejak yang ditampilkan di bagian itu. Saat Anda siap untuk membuat jejak, pilih Buat jejak.

22. Jejak baru muncul di halaman Trails. Dalam waktu sekitar 5 menit, CloudTrail menerbitkan file log yang menampilkan panggilan AWS API yang dilakukan di akun Anda. Anda dapat melihat file log di bucket S3 yang Anda tentukan.

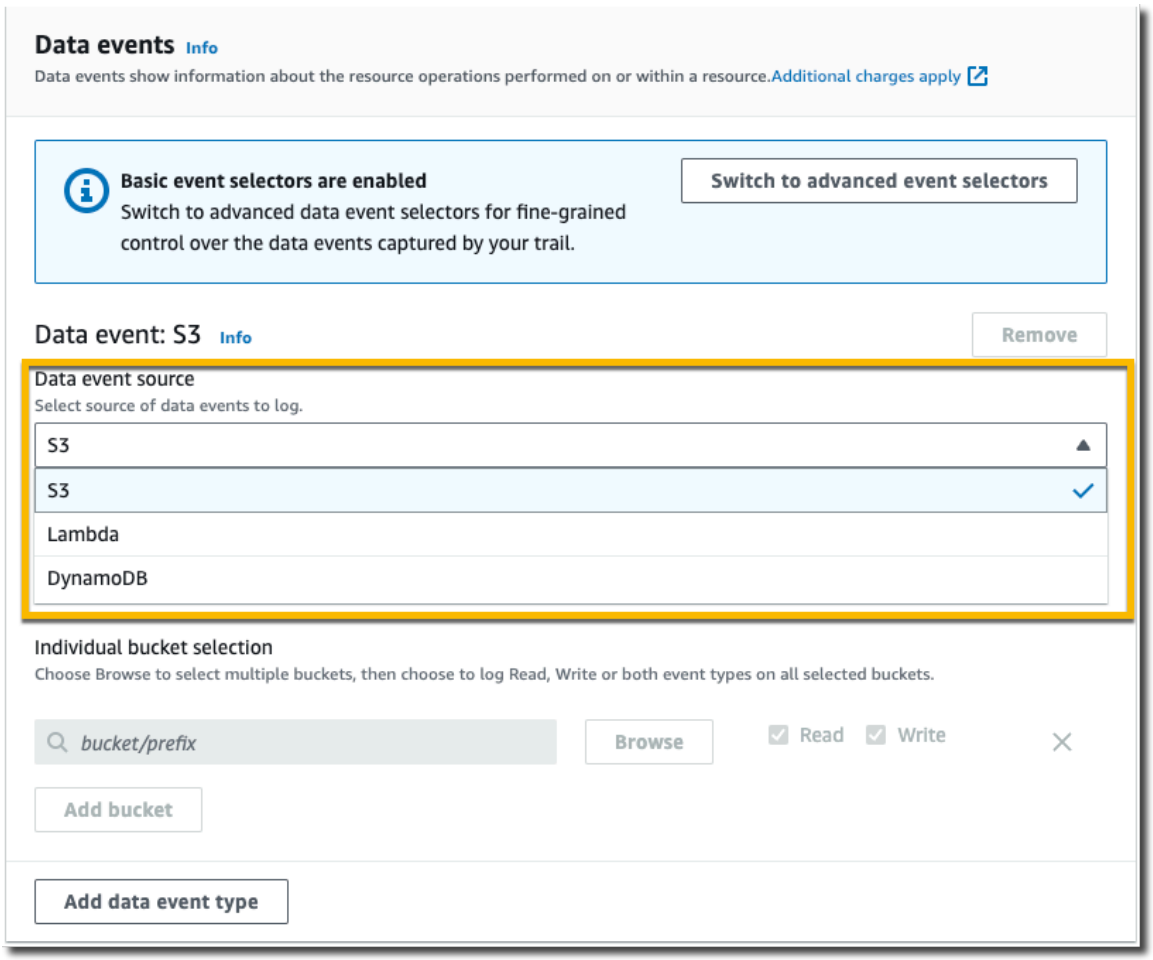
    Jika Anda mengaktifkan acara Insights untuk jejak, CloudTrail mungkin memerlukan waktu hingga 36 jam untuk mulai mengirimkan peristiwa ini, asalkan aktivitas yang tidak biasa terdeteksi selama waktu tersebut.

> **Note**
>
> CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian Tingkat AWS CloudTrail Layanan untuk informasi lebih lanjut.
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan peristiwa yang dicoba dikirim ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Konfigurasikan pengaturan peristiwa data menggunakan pemilih acara dasar

Anda dapat menggunakan pemilih acara lanjutan untuk mengonfigurasi semua jenis peristiwa data serta peristiwa aktivitas jaringan. Penyeleksi acara tingkat lanjut memungkinkan Anda membuat penyeleksi berbutir halus untuk mencatat hanya peristiwa yang menarik.

Jika Anda menggunakan pemilih peristiwa dasar untuk mencatat peristiwa data, Anda dibatasi untuk mencatat peristiwa data untuk bucket, fungsi AWS Lambda , dan tabel Amazon DynamoDB Amazon S3. Anda tidak dapat memfilter pada `eventName` bidang menggunakan pemilih acara dasar. Anda juga tidak dapat mencatat peristiwa aktivitas jaringan.



Gunakan prosedur berikut untuk mengonfigurasi pengaturan peristiwa data menggunakan pemilih acara dasar.

Untuk mengkonfigurasi pengaturan peristiwa data menggunakan pemilih acara dasar

1. Di Peristiwa, pilih Peristiwa data untuk mencatat peristiwa data. Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.
2. Untuk ember Amazon S3:
    a. Untuk sumber peristiwa Data, pilih S3.
    b. Anda dapat memilih untuk mencatat Semua bucket S3 saat ini dan masa depan, atau Anda dapat menentukan masing-masing bucket atau fungsi. Secara default, peristiwa data dicatat untuk semua bucket S3 saat ini dan masa depan.

> **Note**
>
> Menjaga opsi All current and future S3 bucket default memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.
> Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), memilih Semua bucket S3 saat ini dan masa depan memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS

c. Jika Anda meninggalkan default, Semua bucket S3 saat ini dan masa depan, pilih untuk mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.

d. Untuk memilih bucket individual, kosongkan kotak centang Baca dan Tulis untuk Semua bucket S3 saat ini dan masa depan. Dalam pemilihan bucket Individual, telusuri bucket untuk mencatat peristiwa data. Temukan bucket tertentu dengan mengetikkan awalan bucket untuk bucket yang Anda inginkan. Anda dapat memilih beberapa ember di jendela ini. Pilih Tambahkan bucket untuk mencatat peristiwa data untuk bucket lainnya. Pilih untuk mencatat peristiwa Baca, seperti`GetObject`, Menulis peristiwa, seperti`PutObject`, atau keduanya.

   Pengaturan ini lebih diutamakan daripada setelan individual yang Anda konfigurasikan untuk masing-masing bucket. Misalnya, jika Anda menentukan peristiwa Pencatatan Baca untuk semua bucket S3, lalu memilih untuk menambahkan bucket tertentu untuk pencatatan peristiwa data, Baca sudah dipilih untuk bucket yang Anda tambahkan. Anda tidak dapat menghapus pilihan. Anda hanya dapat mengonfigurasi opsi untuk Menulis.

   Untuk menghapus ember dari logging, pilih X.

3. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data.
4. Untuk fungsi Lambda:

   a. Untuk sumber peristiwa Data, pilih Lambda.

b. Dalam fungsi Lambda, pilih Semua wilayah untuk mencatat semua fungsi Lambda, atau Fungsi input sebagai ARN untuk mencatat peristiwa data pada fungsi tertentu.

   Untuk mencatat peristiwa data untuk semua fungsi Lambda di AWS akun Anda, pilih Log semua fungsi saat ini dan masa depan. Pengaturan ini lebih diutamakan daripada pengaturan individual yang Anda konfigurasikan untuk fungsi individual. Semua fungsi dicatat, bahkan jika semua fungsi tidak ditampilkan.

   > **Note**
   >
   > Jika Anda membuat jejak Multi-wilayah, pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.
   > Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

c. Jika Anda memilih fungsi Input sebagai ARN, masukkan ARN dari fungsi Lambda.

   > **Note**
   >
   > Jika Anda memiliki lebih dari 15.000 fungsi Lambda di akun Anda, Anda tidak dapat melihat atau memilih semua fungsi di CloudTrail konsol saat membuat jejak. Anda masih dapat memilih opsi untuk mencatat semua fungsi, meskipun tidak ditampilkan. Jika Anda ingin mencatat peristiwa data untuk fungsi tertentu, Anda dapat menambahkan fungsi secara manual jika Anda mengetahui ARN-nya. Anda juga dapat menyelesaikan pembuatan jejak di konsol, lalu menggunakan dan put-event-selectors perintah untuk mengonfigurasi pencatatan peristiwa data untuk fungsi Lambda tertentu. AWS CLI Untuk informasi selengkapnya, lihat Mengelola jalur dengan AWS CLI.

5. Untuk tabel DynamoDB:

a. Untuk sumber peristiwa Data, pilih DynamoDB.

b. Dalam pemilihan tabel DynamoDB, pilih Browse untuk memilih tabel, atau tempel di ARN tabel DynamoDB yang dapat Anda akses. Sebuah DynamoDB tabel ARN menggunakan format berikut:

```
arn:partition:dynamodb:region:account_ID:table/table_name
```

Untuk menambahkan tabel lain, pilih Tambah baris, dan telusuri tabel atau tempel di ARN tabel yang dapat Anda akses.

6. Untuk mengonfigurasi peristiwa Wawasan dan setelan lain untuk jejak Anda, kembali ke prosedur sebelumnya dalam topik ini,. ???

Langkah selanjutnya

Setelah Anda membuat jejak Anda, Anda dapat kembali ke jejak untuk membuat perubahan:

- Jika Anda belum melakukannya, Anda dapat mengonfigurasi CloudTrail untuk mengirim file log ke CloudWatch Log. Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log.
- Buat tabel dan gunakan untuk menjalankan kueri di Amazon Athena untuk menganalisis aktivitas AWS layanan Anda. Untuk informasi selengkapnya, lihat Membuat Tabel untuk CloudTrail Log di CloudTrail Konsol di Panduan Pengguna Amazon Athena.
- Tambahkan tag khusus (pasangan kunci-nilai) ke jejak.
- Untuk membuat jejak lain, buka halaman Trails, dan pilih Create trail.

Memperbarui jejak dengan CloudTrail konsol

Bagian ini menjelaskan cara mengubah pengaturan jejak.

Untuk mengonversi jejak wilayah Tunggal menjadi jejak Multi-wilayah, atau memperbarui jejak Multi-wilayah untuk mencatat peristiwa hanya dalam satu Wilayah, Anda harus menggunakan. AWS CLI Untuk informasi selengkapnya tentang cara mengonversi jejak wilayah Tunggal menjadi jejak Multi-wilayah, lihat. Mengkonversi jalur satu wilayah ke jalur multi-wilayah Untuk informasi selengkapnya tentang cara memperbarui jejak Multi-wilayah untuk mencatat peristiwa di satu Wilayah, lihatMengonversi jalur Multi-wilayah menjadi jalur satu wilayah.

Jika Anda telah mengaktifkan peristiwa CloudTrail manajemen di Amazon Security Lake, Anda diharuskan untuk mempertahankan setidaknya satu jejak organisasi yaitu Multi-wilayah dan mencatat keduanya `read` dan peristiwa `write` manajemen. Anda tidak dapat memperbarui jejak kualifikasi sedemikian rupa sehingga gagal memenuhi persyaratan Security Lake. Misalnya, dengan mengubah jejak ke wilayah Tunggal, atau dengan mematikan pencatatan `read` atau acara `write` pengelolaan.

> **Note**
>
> CloudTrail memperbarui jejak organisasi di akun anggota meskipun validasi sumber daya gagal. Contoh kegagalan validasi meliputi:
>
> - kebijakan bucket Amazon S3 yang salah
> - kebijakan topik Amazon SNS yang salah
> - ketidakmampuan untuk mengirimkan ke grup CloudWatch log Log
> - izin yang tidak memadai untuk mengenkripsi menggunakan kunci KMS
>
> Akun anggota dengan CloudTrail izin dapat melihat kegagalan validasi untuk jejak organisasi dengan melihat halaman detail jejak di CloudTrail konsol, atau dengan menjalankan perintah. AWS CLI get-trail-status

Untuk memperbarui jejak dengan Konsol Manajemen AWS

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Jalur, lalu pilih nama jejak.
3. Dalam Rincian umum, pilih Edit untuk mengubah pengaturan berikut. Anda tidak dapat mengubah nama jejak.
   - Terapkan jejak ke organisasi saya - Ubah apakah jejak ini adalah jejak AWS Organizations organisasi.

> **Note**
>
> Hanya akun manajemen untuk organisasi yang dapat mengubah jejak organisasi menjadi jejak non-organisasi, atau mengubah jejak non-organisasi menjadi jejak organisasi.

- Lokasi log jejak - Ubah nama bucket atau awalan S3 tempat Anda menyimpan log untuk jejak ini.
- SSE-KMS Enkripsi file log - Pilih untuk mengaktifkan atau menonaktifkan enkripsi file log dengan SSE-KMS bukan. SSE-S3
- Validasi file log - Pilih untuk mengaktifkan atau menonaktifkan validasi integritas file log.
- Pengiriman notifikasi SNS - Pilih untuk mengaktifkan atau menonaktifkan notifikasi Amazon Simple Notification Service (Amazon SNS) bahwa file log telah dikirim ke bucket yang ditentukan untuk jejak.

a. Untuk mengubah jejak ke jejak AWS Organizations organisasi, Anda dapat memilih untuk mengaktifkan jejak untuk semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat Membuat jejak untuk sebuah organisasi.

b. Untuk mengubah bucket yang ditentukan di lokasi Storage, pilih Create new S3 bucket untuk membuat bucket. Saat Anda membuat bucket, CloudTrail membuat dan menerapkan kebijakan bucket yang diperlukan. Jika Anda memilih untuk membuat bucket S3 baru, kebijakan IAM Anda harus menyertakan izin untuk `s3:PutEncryptionConfiguration` tindakan tersebut karena secara default enkripsi sisi server diaktifkan untuk bucket.

> **Note**
>
> Jika Anda memilih Gunakan bucket S3 yang ada, tentukan bucket di nama bucket log Trail, atau pilih Browse untuk memilih bucket. Kebijakan bucket harus memberikan CloudTrail izin untuk menulis ke sana. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk CloudTrail.

Untuk mempermudah menemukan log Anda, buat folder baru (juga dikenal sebagai awalan) di bucket yang ada untuk menyimpan CloudTrail log Anda. Masukkan awalan di Awalan.

c. Untuk SSE-KMS enkripsi file Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda dan mencerna file menggunakan SSE-KMS enkripsi alih-alih SSE-S3 enkripsi. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan SSE-KMS enkripsi, file log dan file digest Anda dienkripsi menggunakan enkripsi. SSE-S3 Untuk informasi selengkapnya tentang SSE-KMS enkripsi, lihat Menggunakan enkripsi sisi server dengan AWS Key Management Service (). SSE-KMS Untuk informasi selengkapnya tentang SSE-S3 enkripsi, lihat Menggunakan Server-Side Enkripsi dengan Kunci S3-Managed Enkripsi Amazon (SSE-S3).

   Jika Anda mengaktifkan SSE-KMS enkripsi, pilih New atau Existing AWS KMS key. Di AWS KMS Alias, tentukan alias, dalam format. `alias/` *`MyAliasName`* Untuk informasi lebih lanjut, lihatMemperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol. CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

   > **Note**
   >
   > Anda juga dapat mengetikkan ARN kunci dari akun lain. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol. Kebijakan kunci harus mengizinkan penggunaan kunci CloudTrail untuk mengenkripsi file log dan mencerna file, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log atau mencerna file dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

d. Untuk validasi file Log, pilih Diaktifkan agar intisari log dikirimkan ke bucket S3 Anda. Anda dapat menggunakan file intisari untuk memverifikasi bahwa file log Anda tidak berubah setelah CloudTrail dikirimkan. Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas file log.

e. Untuk pengiriman notifikasi SNS, pilih Diaktifkan untuk diberi tahu setiap kali log dikirimkan ke bucket Anda. CloudTrail menyimpan beberapa peristiwa dalam file log. Notifikasi SNS dikirim untuk setiap file log, bukan untuk setiap acara. Untuk informasi selengkapnya, lihat Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail.

   Jika Anda mengaktifkan notifikasi SNS, untuk Membuat topik SNS baru, pilih Baru untuk membuat topik, atau pilih Ada untuk menggunakan topik yang ada. Jika Anda membuat jejak

Multi-wilayah, notifikasi SNS untuk pengiriman file log dari semua Wilayah yang diaktifkan akan dikirim ke satu topik SNS yang Anda buat.

Jika Anda memilih Baru, CloudTrail menentukan nama untuk topik baru untuk Anda, atau Anda dapat mengetikkan nama. Jika Anda memilih yang ada, pilih topik SNS dari daftar drop-down. Anda juga dapat memasukkan ARN topik dari Wilayah lain atau dari akun dengan izin yang sesuai. Untuk informasi selengkapnya, lihat Kebijakan topik Amazon SNS untuk CloudTrail.

Jika Anda membuat topik, Anda harus berlangganan topik untuk diberitahu tentang pengiriman file log. Anda dapat berlangganan dari konsol Amazon SNS. Karena frekuensi pemberitahuan, kami menyarankan Anda mengonfigurasi langganan untuk menggunakan antrian Amazon SQS untuk menangani notifikasi secara terprogram. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

4. Di CloudWatch Log, pilih Edit untuk mengubah pengaturan pengiriman file CloudTrail log ke CloudWatch Log. Pilih Diaktifkan di CloudWatch Log untuk mengaktifkan pengiriman file log. Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log.

   a. Jika Anda mengaktifkan integrasi dengan CloudWatch Log, pilih Baru untuk membuat grup log baru, atau Ada untuk menggunakan yang sudah ada. Jika Anda memilih Baru, CloudTrail menentukan nama untuk grup log baru untuk Anda, atau Anda dapat mengetikkan nama.

   b. Jika Anda memilih Ada, pilih grup log dari daftar drop-down.

   c. Pilih Baru untuk membuat peran IAM baru untuk izin mengirim log ke CloudWatch Log. Pilih Existing untuk memilih peran IAM yang ada dari daftar drop-down. Pernyataan kebijakan untuk peran baru atau yang sudah ada ditampilkan saat Anda memperluas dokumen Kebijakan. Untuk informasi selengkapnya tentang peran ini, silakan lihat Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

   > **Note**
   >
   > - Saat mengonfigurasi jejak, Anda dapat memilih bucket S3 dan topik SNS milik akun lain. Namun, jika Anda CloudTrail ingin mengirimkan peristiwa ke grup CloudWatch log Log, Anda harus memilih grup log yang ada di akun Anda saat ini.
   > - Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi menggunakan konsol. Administrator yang didelegasikan

dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API.

5. Di Tag, pilih Edit untuk mengubah, menambah, atau menghapus tag di jejak. Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke jejak Anda. Tag dapat membantu Anda mengidentifikasi CloudTrail jejak dan bucket Amazon S3 yang CloudTrail berisi file log. Anda kemudian dapat menggunakan grup sumber daya untuk CloudTrail sumber daya Anda. Untuk informasi selengkapnya, lihat AWS Resource Groups dan Tanda.
6. Di acara Manajemen, pilih Edit untuk mengubah pengaturan pencatatan peristiwa manajemen.

   a. Untuk aktivitas API, pilih apakah Anda ingin jejak Anda mencatat peristiwa Baca, peristiwa Tulis, atau keduanya. Untuk informasi selengkapnya, lihat Peristiwa manajemen.

   b. Pilih Kecualikan AWS KMS acara untuk memfilter AWS Key Management Service (AWS KMS) peristiwa dari jejak Anda. Pengaturan default adalah untuk memasukkan semua AWS KMS acara.

      Opsi untuk mencatat atau mengecualikan AWS KMS peristiwa hanya tersedia jika Anda mencatat peristiwa manajemen di jejak Anda. Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan AWS KMS peristiwa.

      AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Low-volume, AWS KMS tindakan yang relevan seperti`Disable`,`Delete`, dan `ScheduleKey` (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

      Untuk mengecualikan peristiwa bervolume tinggi seperti`Encrypt`,`Decrypt`, dan`GenerateDataKey`, tetapi masih mencatat peristiwa yang relevan seperti`Disable`, `Delete` dan`ScheduleKey`, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa.

   c. Pilih Kecualikan peristiwa Amazon RDS Data API untuk memfilter peristiwa Amazon Relational Database Service Data Data API dari jejak Anda. Pengaturan default adalah untuk menyertakan semua peristiwa Amazon RDS Data API. Untuk informasi selengkapnya tentang peristiwa Amazon RDS Data API, lihat Pencatatan panggilan API Data dengan AWS CloudTrail di Panduan Pengguna Amazon RDS untuk Aurora.

7.

> **Important**
>
> Langkah 7-11 adalah untuk mengonfigurasi peristiwa data menggunakan pemilih acara lanjutan, yang merupakan default. Penyeleksi acara tingkat lanjut memungkinkan Anda mengonfigurasi lebih banyak jenis peristiwa data dan menawarkan kontrol halus atas peristiwa data mana yang ditangkap jejak Anda. Jika Anda berencana untuk mencatat peristiwa aktivitas jaringan, Anda harus menggunakan pemilih acara lanjutan. Jika Anda menggunakan pemilih acara dasar, lihatMemperbarui pengaturan peristiwa data dengan pemilih acara dasar, lalu kembali ke langkah 12 dari prosedur ini.

Dalam peristiwa Data, pilih Edit untuk mengubah pengaturan pencatatan peristiwa data. Secara default, jejak tidak mencatat peristiwa data. Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Untuk tipe Sumber Daya, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang jenis sumber daya yang tersedia, lihatPeristiwa data.

8. Pilih templat pemilih log. Anda dapat memilih template yang telah ditentukan sebelumnya, atau memilih Custom untuk menentukan kondisi koleksi acara Anda sendiri.

   Anda dapat memilih dari template yang telah ditentukan berikut:

   - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
   - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
   - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau `Write*` peristiwa.
   - Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
   - Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` ofAwsServiceEvent, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).

> **Note**
>
> Memilih template yang telah ditentukan untuk bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.
>
> Jika jejak hanya berlaku untuk satu Wilayah, memilih templat yang telah ditentukan sebelumnya yang mencatat semua bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS
>
> Jika Anda membuat jejak Multi-wilayah, memilih templat yang telah ditentukan untuk fungsi Lambda memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.
>
> Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

9. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.
10. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,`Delete*`, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan `readOnly` pemilih.
- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk menyertakan atau mengecualikan peristiwa data apa pun yang dicatat CloudTrail, sepertiPutBucket,`GetItem`, atau`GetSnapshotBlock`.
- **`eventSource`**— Sumber acara untuk menyertakan atau mengecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk dikecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType`diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- Sesi CredentialFromConsole — Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- pengguna Identity.arn - Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.`ARN, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai. `resources.type`

> **Note**
>
> Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Kunci tindakan, sumber daya, dan kondisi Layanan AWS di Referensi Otorisasi Layanan.

b. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data acara, Anda dapat mengatur bidang ke Resources.arn, mengatur operator untuk tidak memulai, lalu menempelkan ARN bucket S3 yang tidak ingin Anda catat peristiwa.

   Untuk menambahkan bucket S3 kedua, pilih + Condition, lalu ulangi instruksi sebelumnya, tempelkan di ARN untuk atau jelajahi bucket yang berbeda.

   Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

c. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan tentukan ARN dalam satu pemilih agar sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

11. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 3 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk jenis sumber daya.

12. Dalam peristiwa aktivitas jaringan, pilih Edit untuk mengubah setelan pencatatan peristiwa aktivitas jaringan. Secara default, jejak tidak mencatat peristiwa aktivitas jaringan. Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

    Untuk mencatat peristiwa aktivitas jaringan, lakukan hal berikut:

    a. Dari sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

    b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua peristiwa yang ditolak akses aktivitas jaringan, atau memilih Kustom untuk membuat pemilih log kustom untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

    c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

    d. Di Penyeleksi acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

        i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

            - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
            - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
            - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan`vpcEndpointId`.

        ii. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi.

        iii. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

    e. Untuk menambahkan sumber peristiwa lain yang ingin Anda log peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

13. Di acara Insights, pilih Edit jika Anda ingin jejak Anda mencatat peristiwa CloudTrail Insights.

    Di Jenis acara, pilih Acara Wawasan.

    Dalam peristiwa Insights, pilih API call rate, API error rate, atau keduanya. Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.

    CloudTrail Wawasan menganalisis peristiwa manajemen untuk aktivitas yang tidak biasa, dan mencatat peristiwa saat anomali terdeteksi. Secara default, jejak tidak mencatat peristiwa Wawasan. Untuk informasi selengkapnya tentang peristiwa Wawasan, lihatBekerja dengan CloudTrail Wawasan. Biaya tambahan berlaku untuk acara logging Insights. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

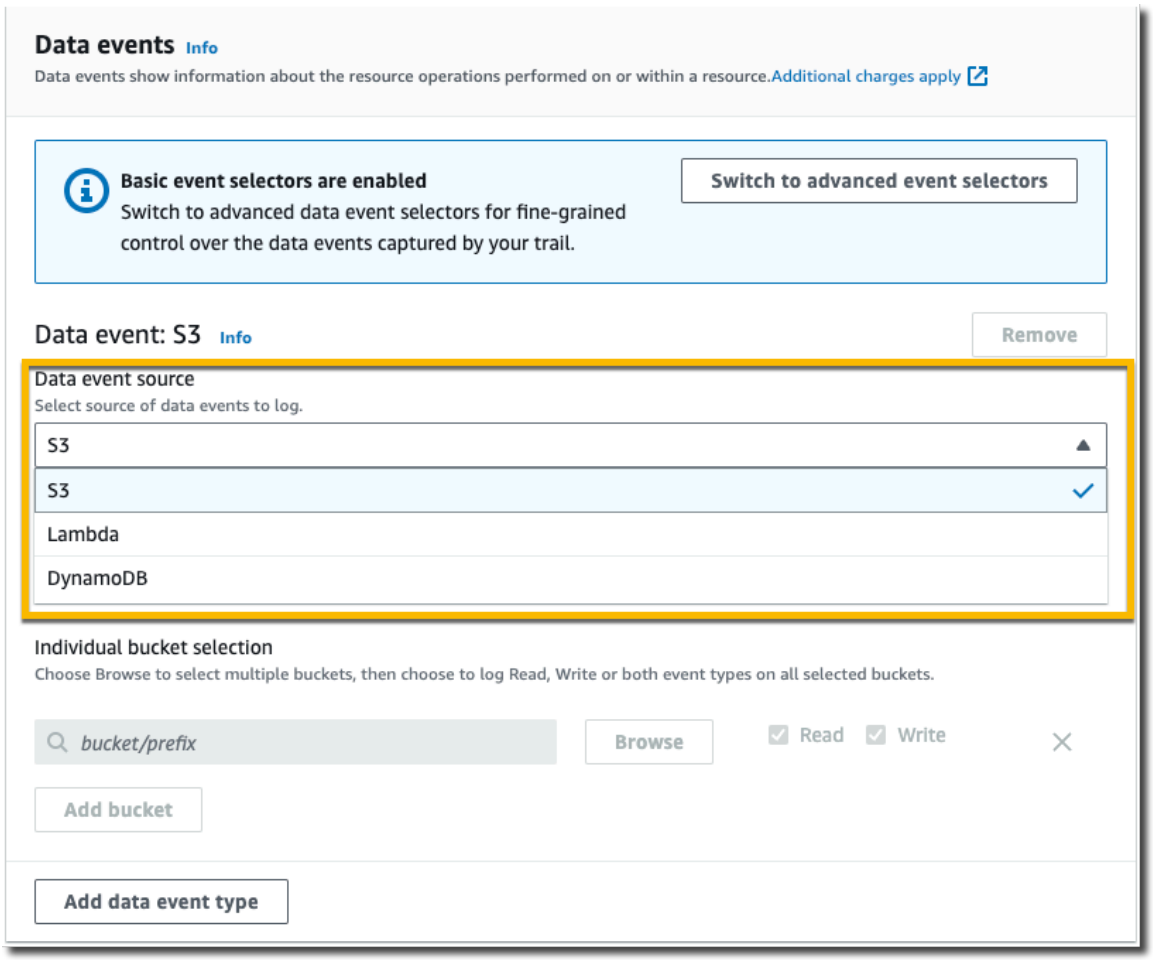
    Peristiwa Insights dikirimkan ke folder berbeda bernama `/CloudTrail-Insight` bucket S3 yang sama yang ditentukan di area lokasi penyimpanan halaman detail jejak. CloudTrailmenciptakan awalan baru untuk Anda. Misalnya, jika bucket S3 tujuan Anda saat ini diberi nama`amzn-s3-demo-bucket/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`

14. Setelah Anda selesai mengubah pengaturan di jejak Anda, pilih Perbarui jejak.

Memperbarui pengaturan peristiwa data dengan pemilih acara dasar

Anda dapat menggunakan pemilih acara lanjutan untuk mengonfigurasi semua jenis peristiwa data serta peristiwa aktivitas jaringan. Penyeleksi acara tingkat lanjut memungkinkan Anda membuat penyeleksi berbutir halus untuk mencatat hanya peristiwa yang menarik.

Jika Anda menggunakan pemilih peristiwa dasar untuk mencatat peristiwa data, Anda dibatasi untuk mencatat peristiwa data untuk bucket, fungsi AWS Lambda , dan tabel Amazon DynamoDB Amazon S3. Anda tidak dapat memfilter pada `eventName` bidang menggunakan pemilih acara dasar. Anda juga tidak dapat mencatat peristiwa aktivitas jaringan.



Gunakan prosedur berikut untuk mengonfigurasi pengaturan peristiwa data menggunakan pemilih acara dasar.

1. Dalam peristiwa Data, pilih Edit untuk mengubah pengaturan pencatatan peristiwa data. Dengan pemilih peristiwa dasar, Anda dapat menentukan peristiwa data pencatatan untuk bucket Amazon S3 AWS Lambda , fungsi, DynamoDbTables, atau kombinasi sumber daya tersebut. Jenis sumber daya peristiwa data tambahan didukung dengan pemilih acara tingkat lanjut. Secara default, jejak tidak mencatat peristiwa data. Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, lihat Peristiwa data. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

   Untuk ember Amazon S3:

   a. Untuk sumber peristiwa Data, pilih S3.

b. Anda dapat memilih untuk mencatat Semua bucket S3 saat ini dan masa depan, atau Anda dapat menentukan masing-masing bucket atau fungsi. Secara default, peristiwa data dicatat untuk semua bucket S3 saat ini dan masa depan.

> **Note**
>
> Menjaga opsi All current and future S3 bucket default memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.
> Jika jejak hanya berlaku untuk satu Wilayah, memilih Semua bucket S3 saat ini dan masa depan memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS

c. Jika Anda meninggalkan default, Semua bucket S3 saat ini dan masa depan, pilih untuk mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.

d. Untuk memilih bucket individual, kosongkan kotak centang Baca dan Tulis untuk Semua bucket S3 saat ini dan masa depan. Dalam pemilihan bucket Individual, telusuri bucket untuk mencatat peristiwa data. Untuk menemukan bucket tertentu, ketikkan awalan bucket untuk bucket yang Anda inginkan. Anda dapat memilih beberapa ember di jendela ini. Pilih Tambahkan bucket untuk mencatat peristiwa data untuk bucket lainnya. Pilih untuk mencatat peristiwa Baca, seperti`GetObject`, Menulis peristiwa, seperti`PutObject`, atau keduanya.

   Pengaturan ini lebih diutamakan daripada setelan individual yang Anda konfigurasikan untuk masing-masing bucket. Misalnya, jika Anda menentukan peristiwa Pencatatan Baca untuk semua bucket S3, lalu memilih untuk menambahkan bucket tertentu untuk pencatatan peristiwa data, Baca sudah dipilih untuk bucket yang Anda tambahkan. Anda tidak dapat menghapus pilihan. Anda hanya dapat mengonfigurasi opsi untuk Menulis.

   Untuk menghapus ember dari logging, pilih X.

2. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data.

3. Untuk fungsi Lambda:

a. Untuk sumber peristiwa Data, pilih Lambda.

b. Dalam fungsi Lambda, pilih Semua wilayah untuk mencatat semua fungsi Lambda, atau Fungsi input sebagai ARN untuk mencatat peristiwa data pada fungsi tertentu.

   Untuk mencatat peristiwa data untuk semua fungsi Lambda di AWS akun Anda, pilih Log semua fungsi saat ini dan masa depan. Pengaturan ini lebih diutamakan daripada pengaturan individual yang Anda konfigurasikan untuk fungsi individual. Semua fungsi dicatat, bahkan jika semua fungsi tidak ditampilkan.

   > **Note**
   >
   > Jika Anda membuat jejak Multi-wilayah, pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.
   > Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

c. Jika Anda memilih fungsi Input sebagai ARN, masukkan ARN dari fungsi Lambda.

   > **Note**
   >
   > Jika Anda memiliki lebih dari 15.000 fungsi Lambda di akun Anda, Anda tidak dapat melihat atau memilih semua fungsi di CloudTrail konsol saat membuat jejak. Anda masih dapat memilih opsi untuk mencatat semua fungsi, meskipun tidak ditampilkan. Jika Anda ingin mencatat peristiwa data untuk fungsi tertentu, Anda dapat menambahkan fungsi secara manual jika Anda mengetahui ARN-nya. Anda juga dapat menyelesaikan pembuatan jejak di konsol, lalu menggunakan dan put-event-selectors perintah untuk mengonfigurasi pencatatan peristiwa data untuk

fungsi Lambda tertentu. AWS CLI Untuk informasi selengkapnya, lihat Mengelola jalur dengan AWS CLI.

4. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data.
5. Untuk tabel DynamoDB:
   a. Untuk sumber peristiwa Data, pilih DynamoDB.
   b. Dalam pemilihan tabel DynamoDB, pilih Browse untuk memilih tabel, atau tempel di ARN tabel DynamoDB yang dapat Anda akses. Sebuah DynamoDB tabel ARN dalam format berikut:

      ```
      arn:partition:dynamodb:region:account_ID:table/table_name
      ```

      Untuk menambahkan tabel lain, pilih Tambah baris, dan telusuri tabel atau tempel di ARN tabel yang dapat Anda akses.
6. Untuk mengonfigurasi peristiwa Wawasan dan setelan lain untuk jejak Anda, kembali ke prosedur sebelumnya dalam topik ini,. Memperbarui jejak dengan CloudTrail konsol

Menghapus jejak dengan konsol CloudTrail

Anda dapat menghapus jejak dengan CloudTrail konsol. Jika akun manajemen organisasi atau akun administrator yang didelegasikan menghapus jejak organisasi, jejak akan dihapus dari semua akun anggota organisasi.

Important

Meskipun menghapus CloudTrail jejak adalah tindakan yang tidak dapat diubah, CloudTrail tidak menghapus file log di bucket Amazon S3 untuk jejak itu, bucket Amazon S3 itu sendiri, atau grup CloudWatch log tempat jejak mengirimkan peristiwa. Menghapus jejak Multi-wilayah akan menghentikan pencatatan peristiwa di semua AWS Wilayah yang diaktifkan di Anda. Akun AWS Menghapus jejak wilayah Tunggal akan menghentikan pencatatan peristiwa di Wilayah tersebut saja. Ini tidak akan menghentikan pencatatan peristiwa di Wilayah lain bahkan jika jalur di Wilayah lain tersebut memiliki nama yang identik dengan jejak yang dihapus.

Untuk informasi tentang penutupan akun dan penghapusan CloudTrail jejak, lihat. Akun AWS penutupan dan jalan setapak

Jika Anda telah mengaktifkan peristiwa CloudTrail manajemen di Amazon Security Lake, Anda diharuskan untuk mempertahankan setidaknya satu jejak organisasi yaitu Multi-wilayah dan mencatat keduanya `read` dan peristiwa `write` manajemen. Anda tidak dapat menghapus jejak jika itu adalah satu-satunya jejak yang Anda miliki yang memenuhi persyaratan ini, kecuali jika Anda mematikan acara CloudTrail manajemen di Security Lake.

Untuk menghapus jejak dengan CloudTrail konsol

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Buka halaman Trails CloudTrail konsol.
3. Pilih nama jejak.
4. Di bagian atas halaman detail jejak, pilih Hapus.
5. Ketika Anda diminta untuk mengonfirmasi, pilih Hapus untuk menghapus jejak secara permanen. Jejak dihapus dari daftar jalan setapak. File log yang sudah dikirim ke bucket Amazon S3 tidak dihapus dan terus dikenakan biaya S3.

> **Note**
>
> Konten yang dikirimkan ke bucket Amazon S3 mungkin berisi konten pelanggan. Untuk informasi selengkapnya tentang menghapus data sensitif, lihat Mengosongkan bucket dan Menghapus bucket di Panduan Pengguna Amazon S3.

Mematikan pencatatan log untuk jejak

Saat Anda membuat jejak, logging diaktifkan secara otomatis. Anda dapat mematikan pencatatan untuk jejak dari halaman detail jejak.

> **Note**
>
> Saat Anda mematikan logging, log yang ada masih disimpan di bucket Amazon S3 trail dan terus dikenakan biaya S3. Untuk informasi tentang harga S3, lihat harga Amazon S3.

⚠ Pengiriman acara setelah logging dihentikan

Setelah Anda mematikan logging untuk jalan setapak, jejak masih dapat menerima peristiwa yang terjadi sebelum logging dimatikan. Acara dapat ditunda karena sejumlah alasan, termasuk lalu lintas jaringan yang tinggi, masalah konektivitas, pemadaman layanan, atau pembaruan untuk acara yang ada. CloudTrail menggunakan waktu terbaru bahwa logging dimatikan untuk menentukan apakah akan mengirimkan peristiwa yang tertunda, bukan status logging dari jejak pada saat peristiwa itu terjadi. Akibatnya, peristiwa tertunda yang terjadi sebelum penebangan terakhir dimatikan masih dapat dikirim ke jalan setapak. Untuk informasi selengkapnya tentang pengiriman acara tertunda, lihat `addendum` bidang di[CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan](). Selain itu, penyeleksi acara dan penyeleksi acara lanjutan tidak dievaluasi untuk peristiwa tertunda yang dikirim ke jejak setelah logging dimatikan. Ini berarti bahwa jejak dapat menerima semua jenis peristiwa yang terjadi sebelum logging dimatikan, terlepas dari konfigurasi pemilih peristiwa jejak.

Untuk mematikan logging untuk jejak dengan CloudTrail konsol

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Jalur, lalu pilih nama jejak.
3. Di bagian atas halaman detail jejak, pilih Hentikan pencatatan untuk mematikan pencatatan untuk jejak.
4. Ketika Anda diminta untuk mengonfirmasi, pilih Hentikan pencatatan. CloudTrailmenghentikan aktivitas logging untuk jejak itu.
5. Untuk melanjutkan pencatatan untuk jejak itu, pilih Mulai masuk di halaman konfigurasi jejak.

Membuat, memperbarui, dan mengelola jalur dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk membuat, memperbarui, dan mengelola jejak Anda. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wil AWS ayah yang dikonfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

> **Note**
>
> Anda memerlukan alat baris AWS perintah untuk menjalankan perintah AWS Command Line Interface (AWS CLI) dalam topik ini. Pastikan Anda memiliki versi terbaru dari yang AWS CLI diinstal. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Command Line Interface. Untuk bantuan dengan CloudTrail perintah di baris AWS CLI perintah, ketik`aws cloudtrail help`.

Perintah yang umum digunakan untuk pembuatan jejak, manajemen, dan status

Beberapa perintah yang lebih umum digunakan untuk membuat dan memperbarui jalur CloudTrail termasuk:

- create-trailuntuk membuat jejak.
- update-trailuntuk mengubah konfigurasi jejak yang ada.
- add-tagsuntuk menambahkan satu atau lebih tag (pasangan kunci-nilai) ke jejak yang ada.
- remove-tagsuntuk menghapus satu atau lebih tag dari jejak.
- list-tagsuntuk mengembalikan daftar tag yang terkait dengan jejak.
- put-event-selectorsuntuk menambah atau memodifikasi pemilih acara untuk jejak.
- put-insight-selectorsuntuk menambahkan atau memodifikasi pemilih peristiwa Insights untuk jejak yang ada, dan mengaktifkan atau menonaktifkan peristiwa Wawasan.
- start-logginguntuk mulai mencatat peristiwa dengan jejak Anda.
- stop-logginguntuk menjeda peristiwa logging dengan jejak Anda.
- delete-trailuntuk menghapus jejak. Perintah ini tidak menghapus bucket Amazon S3 yang berisi file log untuk jejak tersebut, jika ada.
- describe-trailsuntuk mengembalikan informasi tentang jalur di suatu Wil AWS ayah.
- get-trailuntuk mengembalikan informasi pengaturan untuk jejak.
- get-trail-statusuntuk mengembalikan informasi tentang status jejak saat ini.
- get-event-selectorsuntuk mengembalikan informasi tentang pemilih acara yang dikonfigurasi untuk jejak.
- get-insight-selectorsuntuk mengembalikan informasi tentang pemilih peristiwa Insights yang dikonfigurasi untuk jejak.

Perintah yang didukung untuk membuat dan memperbarui jalur: create-trail dan update-trail

Per `create-trail` `update-trail` intah dan menawarkan berbagai fungsi untuk membuat dan mengelola jalur, termasuk:

- Membuat jejak yang menerima log di seluruh Wilayah, atau memperbarui jejak dengan `--is-multi-region-trail` opsi tersebut. Dalam sebagian besar keadaan, Anda harus membuat jalur yang mencatat peristiwa di semua Wil AWS ayah.
- Membuat jejak yang menerima log untuk semua AWS akun dalam organisasi dengan --is-organization-trail opsi.
- Mengonversi jalur Multi-wilayah ke Jejak wilayah tunggal dengan opsi. `--no-is-multi-region-trail`
- Mengaktifkan atau menonaktifkan enkripsi file log dengan `--kms-key-id` opsi. Opsi ini menentukan AWS KMS kunci yang sudah Anda buat dan yang telah Anda lampirkan kebijakan yang memungkinkan CloudTrail untuk mengenkripsi log Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan enkripsi untuk file CloudTrail log, mencerna file dan penyimpanan data peristiwa dengan AWS CLI.
- Mengaktifkan atau menonaktifkan validasi file log dengan `--no-enable-log-file-validation` opsi `--enable-log-file-validation` dan. Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas file log.
- Anda dapat menekan peristiwa rekursif yang dihasilkan oleh operasi CloudTrail pengiriman dengan `--no-recursive-logging` opsi. Untuk informasi selengkapnya, lihat Menekan peristiwa rekursif dengan logging rekursif.
- Menentukan grup CloudWatch log log dan peran sehingga CloudTrail dapat mengirimkan peristiwa ke grup CloudWatch log log. Untuk informasi selengkapnya, lihat Memantau File CloudTrail Log dengan CloudWatch Log Amazon.

Perintah yang tidak digunakan lagi: create-subscription dan update-subscription

> **Important**
>
> Per `create-subscription` `update-subscription` intah and digunakan untuk membuat dan memperbarui jalur, tetapi tidak digunakan lagi. Jangan gunakan perintah ini. Mereka tidak menyediakan fungsionalitas penuh untuk membuat dan mengelola jalur.

Jika Anda mengonfigurasi otomatisasi yang menggunakan salah satu atau kedua perintah ini, sebaiknya perbarui kode atau skrip untuk menggunakan perintah yang didukung seperticreate-trail.

Menggunakan **`perintah`** create-trail untuk membuat jejak

Anda dapat menjalankan `create-trail` perintah untuk membuat jalur yang secara khusus dikonfigurasi untuk memenuhi kebutuhan bisnis Anda. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wil AWS ayah yang dikonfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Membuat jejak multi-wilayah

Jejak dapat diterapkan ke semua Wilayah AWS yang di aktifkan di Anda Akun AWS, atau dapat diterapkan ke satu Wilayah. Jejak yang berlaku untuk semua Wilayah AWS yang diaktifkan di Akun AWS jalur Anda disebut sebagai jalur multi-wilayah. Sebagai praktik terbaik, sebaiknya buat jejak Multi-wilayah karena ini menangkap aktivitas di semua Wilayah yang diaktifkan.

Untuk membuat jejak Multi-wilayah, gunakan `--is-multi-region-trail` opsi. Secara default, `create-trail` perintah membuat jejak yang mencatat peristiwa hanya di AWS Wilayah tempat jejak dibuat. Untuk memastikan bahwa Anda mencatat peristiwa layanan global dan menangkap semua aktivitas peristiwa manajemen di AWS akun Anda, Anda harus membuat jejak yang mencatat peristiwa di semua Wil AWS ayah.

> **Note**
>
> Saat membuat jejak, jika Anda menentukan bucket Amazon S3 yang tidak dibuat dengan CloudTrail, Anda perlu melampirkan kebijakan yang sesuai. Lihat Kebijakan bucket Amazon S3 untuk CloudTrail.

Contoh berikut membuat jejak Multi-wilayah dengan nama *`my-trail`* dan tag dengan kunci bernama *`Group`* dengan nilai yang mengirimkan log dari semua Wilayah *`Marketing`* yang diaktifkan di akun Anda ke bucket yang ada bernama*`amzn-s3-demo-bucket`*.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

Untuk mengonfirmasi bahwa jejak Anda adalah jejak Multi-wilayah, verifikasi bahwa `IsMultiRegionTrail` elemen dalam output ditampilkan. `true`

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

> **Note**
>
> Gunakan `start-logging` perintah untuk mulai mencatat jejak Anda.

Mulai mencatat untuk jejak

Setelah `create-trail` perintah selesai, jalankan `start-logging` perintah untuk mulai mencatat jejak itu.

> **Note**
>
> Saat Anda membuat jejak dengan CloudTrail konsol, logging diaktifkan secara otomatis.

Contoh berikut mulai mencatat jejak.

```
aws cloudtrail start-logging --name my-trail
```

Perintah ini tidak mengembalikan output, tetapi Anda dapat menggunakan `get-trail-status` perintah untuk memverifikasi bahwa logging telah dimulai.

```
aws cloudtrail get-trail-status --name my-trail
```

Untuk mengonfirmasi bahwa jejak sedang dicatat, `IsLogging` elemen dalam output ditampilkan`true`.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Membuat jejak satu wilayah

Perintah berikut membuat jejak wilayah tunggal. Bucket Amazon S3 yang ditentukan harus sudah ada dan memiliki CloudTrail izin yang sesuai diterapkan. Untuk informasi selengkapnya, lihat Kebijakan bucket Amazon S3 untuk CloudTrail.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket
```

Berikut ini adalah output contoh.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Membuat jejak Multi-wilayah yang mengaktifkan validasi file log

Untuk mengaktifkan validasi file log saat menggunakan`create-trail`, gunakan `--enable-log-file-validation` opsi.

Untuk informasi tentang validasi file log, lihatMemvalidasi CloudTrail integritas file log.

Contoh berikut membuat jejak Multi-wilayah yang mengirimkan log ke bucket yang ditentukan. Perintah menggunakan `--enable-log-file-validation` opsi.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail --enable-log-file-validation
```

Untuk mengonfirmasi bahwa validasi file log diaktifkan, `LogFileValidationEnabled` elemen dalam output ditampilkan`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Menggunakan **perintah** update-trail untuk memperbarui jejak

> **Important**
>
> Pada 22 November 2021, AWS CloudTrail mengubah cara jejak menangkap acara layanan global. Sekarang, peristiwa yang dibuat oleh Amazon CloudFront AWS Identity and Access Management,, dan AWS STS dicatat di Wilayah tempat mereka dibuat, Wilayah AS Timur (Virginia Utara), us-east-1. Ini membuat bagaimana CloudTrail memperlakukan layanan ini konsisten dengan layanan AWS global lainnya. Untuk terus menerima acara layanan global di luar AS Timur (Virginia Utara), pastikan untuk mengubah jalur satu wilayah menggunakan acara layanan global di luar AS Timur (Virginia Utara) menjadi jalur multi-wilayah. Untuk informasi selengkapnya tentang menangkap peristiwa layanan global, lihat Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global nanti di bagian ini.
> Sebaliknya, ri wayat peristiwa di CloudTrail konsol dan aws cloudtrail lookup-events perintah akan menunjukkan peristiwa ini di Wilayah AWS tempat mereka terjadi.

Anda dapat menggunakan `update-trail` perintah untuk mengubah pengaturan konfigurasi untuk jejak. Anda juga dapat menggunakan remove-tags perintah add-tags dan untuk menambah dan menghapus tag untuk jejak. Anda hanya dapat memperbarui jalur dari Wil AWS ayah tempat jejak dibuat (Wilayah Asal). Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wil AWS ayah yang dikonfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah

yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Jika Anda telah mengaktifkan peristiwa CloudTrail manajemen di Amazon Security Lake, Anda diharuskan untuk memelihara setidaknya satu jejak organisasi yaitu Multi-wilayah dan mencatat keduanya `read` dan peristiwa `write` manajemen. Anda tidak dapat memperbarui jalur kualifikasi sedemikian rupa sehingga gagal memenuhi persyaratan Danau Keamanan. Misalnya, dengan mengubah jejak ke Wilayah tunggal, atau dengan mematikan pencatatan `read` atau peristiwa `write` manajemen.

> **Note**
>
> Jika Anda menggunakan AWS CLI atau salah satu AWS SDK untuk memodifikasi jejak, pastikan kebijakan bucket jejak telah diperbarui. Agar bucket Anda secara otomatis menerima peristiwa dari yang baru Wilayah AWS, kebijakan harus berisi nama layanan lengkap,`cloudtrail.amazonaws.com`. Untuk informasi selengkapnya, lihat Kebijakan bucket Amazon S3 untuk CloudTrail.

Topik

- Mengkonversi jalur satu wilayah ke jalur multi-wilayah
- Mengonversi jalur Multi-wilayah menjadi jalur satu wilayah
- Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global
- Mengaktifkan validasi file log
- Menonaktifkan validasi file log

Mengkonversi jalur satu wilayah ke jalur multi-wilayah

Untuk mengubah jalur satu wilayah yang ada menjadi jalur Multi-wilayah, gunakan opsi. `--is-multi-region-trail`

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak sekarang adalah jejak Multi-wilayah, verifikasi bahwa `IsMultiRegionTrail` elemen dalam output ditampilkan. `true`

```
{
```

```
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Mengonversi jalur Multi-wilayah menjadi jalur satu wilayah

Untuk mengubah jalur Multi-wilayah yang ada sehingga hanya berlaku untuk Wilayah di mana ia dibuat, gunakan `--no-is-multi-region-trail` opsi.

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak sekarang berlaku untuk satu Wilayah, `IsMultiRegionTrail` elemen dalam output ditampilkan`false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

> **Peristiwa layanan global setelah konversi jejak**
>
> `IncludeGlobalServiceEvents`Nilai tetap `true` setelah konversi. CloudTrail memberikan acara layanan global hanya ke jalur satu wilayah di AS Timur (Virginia Utara).

Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global

`IncludeGlobalServiceEvents`Kapan ya`true`, CloudTrail berikan acara layanan global hanya ke jalur satu wilayah di AS Timur (Virginia Utara). Untuk jalur multi-wilayah, `IncludeGlobalServiceEvents` harus`true`.

Untuk mengubah jejak sehingga tidak mencatat peristiwa layanan global, gunakan `--no-include-global-service-events` opsi.

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

Untuk mengonfirmasi bahwa jejak tidak lagi mencatat peristiwa layanan global, `IncludeGlobalServiceEvents` elemen dalam output ditampilkan`false`.

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Untuk mengubah jejak sehingga mencatat peristiwa layanan global, gunakan `--include-global-service-events` opsi.

Single-Region jalur tidak akan lagi menerima acara layanan global mulai 22 November 2021, kecuali jejak sudah muncul di Wilayah AS Timur (Virginia Utara), us-east-1. Untuk terus menangkap peristiwa layanan global, perbarui konfigurasi jejak ke jalur Multi-wilayah. Misalnya, perintah ini memperbarui jejak wilayah tunggal di AS Timur (Ohio), us-east-2, menjadi jalur Multi-wilayah. Ganti *myExistingSingleRegionTrailWithGSE* dengan nama jejak yang sesuai untuk konfigurasi Anda.

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

Karena acara layanan global hanya tersedia di AS Timur (Virginia Utara) mulai 22 November 2021, Anda juga dapat membuat jejak satu wilayah untuk berlangganan acara layanan global di Wilayah AS Timur (Virginia Utara), us-east-1. Perintah berikut membuat jejak wilayah tunggal di us-east-1 untuk menerima CloudFront, IAM, dan peristiwa: AWS STS

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name amzn-s3-demo-bucket
```

Mengaktifkan validasi file log

Untuk mengaktifkan validasi file log untuk jejak, gunakan `--enable-log-file-validation` opsi. File intisari dikirim ke bucket Amazon S3 untuk jejak tersebut.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Untuk mengonfirmasi bahwa validasi file log diaktifkan, `LogFileValidationEnabled` elemen dalam output ditampilkan`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Menonaktifkan validasi file log

Untuk menonaktifkan validasi file log untuk jejak, gunakan `--no-enable-log-file-validation` opsi.

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

Untuk mengonfirmasi bahwa validasi file log dinonaktifkan, `LogFileValidationEnabled` elemen dalam output ditampilkan`false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Untuk memvalidasi file log dengan AWS CLI, lihatMemvalidasi integritas file CloudTrail log dengan AWS CLI.

Mengelola jalur dengan AWS CLI

Ini AWS CLI termasuk beberapa perintah lain yang membantu Anda mengelola jalur Anda. Perintah ini menambahkan tag ke jalur, mendapatkan status jejak, memulai dan menghentikan pencatatan untuk jalur, dan menghapus jejak. Anda harus menjalankan perintah ini dari Wil AWS ayah yang sama tempat jejak dibuat (Wilayah Asal). Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di Wil AWS ayah yang dikonfigurasi untuk profil Anda. Jika Anda ingin menjalankan perintah di Wilayah yang berbeda, ubah Wilayah default untuk profil Anda, atau gunakan parameter --region bersama perintah tersebut.

Topik

- Menambahkan satu atau lebih tag ke jejak
- Daftar tag untuk satu atau lebih jalur
- Menghapus satu atau beberapa tag dari jejak
- Mengambil pengaturan jejak dan status jejak
- Mengkonfigurasi CloudTrail pemilih acara Insights
- Mengkonfigurasi pemilih acara lanjutan
- Mengkonfigurasi pemilih acara dasar
- Menghentikan dan mulai mencatat jejak
- Menghapus jejak

Menambahkan satu atau lebih tag ke jejak

Untuk menambahkan satu atau lebih tag ke jejak yang ada, jalankan add-tags perintah.

Contoh berikut menambahkan tag dengan nama *Owner* dan nilai *Mary* ke jejak dengan ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* di Wilayah AS Timur (Ohio).

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

Jika berhasil, perintah ini tidak mengembalikan apa pun.

Daftar tag untuk satu atau lebih jalur

Untuk melihat tag yang terkait dengan satu atau lebih jalur yang ada, gunakan list-tags perintah.

Contoh berikut mencantumkan tag untuk *Trail1* dan*Trail2*.

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut.

```
{
 "ResourceTagList": [
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
         "TagsList": [
             {
                 "Value": "Alice",
                 "Key": "Name"
             },
             {
                 "Value": "Ohio",
                 "Key": "Location"
             }
         ]
     },
     {
         "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
         "TagsList": [
             {
                 "Value": "Bob",
                 "Key": "Name"
             }
         ]
     }
  ]
}
```

Menghapus satu atau beberapa tag dari jejak

Untuk menghapus satu atau lebih tag dari jejak yang ada, jalankan remove-tags perintah.

Contoh berikut menghapus tag dengan nama *Location* dan *Name* dari jejak dengan ARN *arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1* di Wilayah AS Timur (Ohio).

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

Jika berhasil, perintah ini tidak mengembalikan apa pun.

Mengambil pengaturan jejak dan status jejak

Jalan `describe-trails` kan perintah untuk mengambil informasi tentang jalur di suatu Wil AWS ayah. Contoh berikut mengembalikan informasi tentang jalur yang dikonfigurasi di Wilayah AS Timur (Ohio).

```
aws cloudtrail describe-trails --region us-east-2
```

Jika perintah berhasil, Anda melihat output yang serupa dengan berikut ini.

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "amzn-s3-demo-bucket1",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "amzn-s3-demo-bucket2",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
```

```
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "amzn-s3-demo-bucket3",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
    }
  ]
}
```

Jalan `get-trail` kan perintah untuk mengambil informasi pengaturan tentang jejak tertentu. Contoh berikut mengembalikan informasi pengaturan untuk jejak bernama*my-trail*.

```
aws cloudtrail get-trail - -name my-trail
```

Jika berhasil, perintah ini mengembalikan output yang serupa dengan yang berikut.

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "amzn-s3-demo-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

Jalankan `get-trail-status` perintah untuk mengambil status jejak. Anda harus menjalankan perintah ini dari Wil AWS ayah tempat ia dibuat (Daerah Beranda), atau Anda harus menentukan Wilayah itu dengan menambahkan --region parameter.

> **Note**
>
> Jika jejak adalah jejak organisasi dan Anda adalah akun anggota di organisasi di AWS Organizations, Anda harus memberikan ARN lengkap dari jejak itu, dan bukan hanya namanya.

```
aws cloudtrail get-trail-status --name my-trail
```

Jika perintah berhasil, Anda melihat output yang serupa dengan berikut ini.

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

Selain bidang yang ditampilkan dalam kode JSON sebelumnya, status berisi bidang berikut jika ada kesalahan Amazon SNS atau Amazon S3:

- `LatestNotificationError`. Berisi kesalahan yang dipancarkan oleh Amazon SNS jika langganan topik gagal.
- `LatestDeliveryError`. Berisi kesalahan yang dipancarkan oleh Amazon S3 jika CloudTrail tidak dapat mengirimkan file log ke bucket.

Mengkonfigurasi CloudTrail pemilih acara Insights

Aktifkan peristiwa Wawasan di trek dengan menjalankan put-insight-selectors `ApiCallRateInsightApiErrorRateInsight`, dan menentukan, atau keduanya sebagai nilai `InsightType` atribut. Untuk melihat pengaturan pemilih Insights untuk jejak, jalankan `get-insight-selectors` perintah. Anda harus menjalankan perintah ini dari Wil AWS ayah tempat jejak dibuat (Daerah Rumah), atau Anda harus menentukan Wilayah itu dengan menambahkan --region parameter ke perintah.

> **Note**
>
> Untuk mencatat peristiwa Insights`ApiCallRateInsight`, jejak harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Wawasan`ApiErrorRateInsight`, jejak harus mencatat `read` atau peristiwa `write` manajemen.

Contoh jejak yang mencatat peristiwa Insights

Contoh berikut digunakan put-insight-selectors untuk membuat pemilih peristiwa Insights untuk jejak bernama*`TrailName3`*. Ini memungkinkan pengumpulan acara Insights untuk *`TrailName3`* trek. Pemilih peristiwa Insights mencatat kedua jenis `ApiErrorRateInsight` peristiwa dan `ApiCallRateInsight` Insights.

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

Contoh mengembalikan pemilih peristiwa Insights yang dikonfigurasi untuk jejak.

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Contoh: Matikan pengumpulan peristiwa Wawasan

Contoh berikut digunakan put-insight-selectors untuk menghapus pemilih peristiwa Insights untuk jejak bernama*TrailName3*. Menghapus string JSON dari pemilih Insights akan menonaktifkan pengumpulan peristiwa Insights untuk jejak. *TrailName3*

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

Contoh mengembalikan pemilih peristiwa Insights yang sekarang kosong yang dikonfigurasi untuk jejak.

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

Mengkonfigurasi pemilih acara lanjutan

Anda dapat menggunakan pemilih peristiwa lanjutan untuk mencatat peristiwa manajemen, peristiwa data untuk semua jenis sumber daya, dan peristiwa aktivitas jaringan. Sebaliknya, Anda dapat menggunakan pemilih peristiwa dasar untuk mencatat peristiwa manajemen dan peristiwa data untuk`AWS::DynamoDB::Table`,`AWS::Lambda::Function`, dan jenis `AWS::S3::Object` sumber daya. Anda dapat menggunakan pemilih acara dasar, atau pemilih acara lanjutan, tetapi tidak keduanya. Jika Anda menerapkan pemilih acara lanjutan ke jejak yang menggunakan pemilih peristiwa dasar, pemilih peristiwa dasar akan diganti.

Untuk mengonversi jejak ke pemilih acara lanjutan, jalankan get-event-selectors perintah untuk mengonfirmasi pemilih peristiwa saat ini, lalu konfigurasikan pemilih acara lanjutan agar sesuai dengan cakupan pemilih acara sebelumnya, lalu tambahkan pemilih tambahan.

Anda harus menjalankan `get-event-selectors` perintah dari Wilayah AWS tempat jejak dibuat (Home Region), atau Anda harus menentukan Wilayah itu dengan menambahkan --region parameter.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Jika jejak adalah jejak organisasi, dan Anda masuk dengan akun anggota di organisasi AWS Organizations, Anda harus memberikan ARN lengkap dari jejak tersebut, dan bukan hanya namanya.

Contoh berikut menunjukkan pengaturan untuk jejak yang menggunakan pemilih peristiwa lanjutan untuk mencatat peristiwa manajemen. Secara default, jejak dikonfigurasi untuk mencatat semua peristiwa manajemen dan tidak ada peristiwa data atau peristiwa aktivitas jaringan.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events-
trail",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]

        }
    ]
}
```

Untuk membuat pemilih acara lanjutan, jalankan `put-event-selectors` perintah. Saat peristiwa terjadi di akun Anda, CloudTrail evaluasi konfigurasi untuk jalur Anda. Jika acara cocok dengan pemilih acara lanjutan untuk jejak, jejak akan memproses dan mencatat peristiwa tersebut. Anda dapat mengonfigurasi hingga 500 kondisi di jalur, termasuk semua nilai yang ditentukan untuk semua pemilih acara lanjutan di jalur Anda. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data dan Mencatat peristiwa aktivitas jaringan.

Topik

- Contoh jejak dengan pemilih acara lanjutan tertentu

- Contoh jejak yang menggunakan pemilih acara lanjutan khusus untuk mencatat Amazon S3 AWS Outposts peristiwa data
- Contoh jejak yang menggunakan pemilih acara lanjutan untuk mengecualikan AWS Key Management Service peristiwa
- Contoh jejak yang menggunakan pemilih peristiwa lanjutan untuk mengecualikan peristiwa manajemen API Data Amazon RDS

Contoh jejak dengan pemilih acara lanjutan tertentu

Contoh berikut membuat pemilih peristiwa lanjutan khusus untuk jejak yang diberi nama *TrailName* untuk menyertakan peristiwa manajemen baca dan tulis (dengan menghilangkan pem `readOnly` ilih), `PutObject` dan peristiwa `DeleteObject` data untuk semua bucket/prefix kombinasi Amazon S3 kecuali untuk bucket bernama`amzn-s3-demo-bucket`, peristiwa data untuk AWS Lambda fungsi bernama`MyLambdaFunction`, dan peristiwa aktivitas jaringan untuk peristiwa yang ditolak AWS KMS akses melalui titik akhir VPC. Karena ini adalah pemilih acara lanjutan khusus, setiap set pemilih memiliki nama deskriptif. Perhatikan bahwa garis miring adalah bagian dari nilai ARN untuk bucket S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
```

```
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  },
  {
     "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
     "FieldSelectors": [
       { "Field": "eventCategory", "Equals": ["NetworkActivity"]},
       { "Field": "eventSource", "Equals": ["kms.amazonaws.com"]},
       { "Field": "errorCode", "Equals": ["VpceAccessDenied"]}
     ]
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::amzn-s3-demo-bucket/" ]
        },
```

```
      ]
    },
    {
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:123456789012:function/
MyLambdaFunction" ]
        }
      ]
    },
    {
       "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
       "FieldSelectors": [
         {
           "Field": "eventCategory",
           "Equals": ["NetworkActivity"]
         },
         {
           "Field": "eventSource",
           "Equals": ["kms.amazonaws.com"]
         },
         {
           "Field": "errorCode",
           "Equals": ["VpceAccessDenied"]
         }
       ]
     }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

Contoh jejak yang menggunakan pemilih acara lanjutan khusus untuk mencatat Amazon S3 AWS Outposts peristiwa data

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan semua peristiwa data untuk semua Amazon S3 pada AWS Outposts objek di pos terdepan Anda. Dalam rilis ini, nilai yang didukung untuk S3 pada AWS Outposts acara untuk `resources.type` bidang adalah`AWS::S3Outposts::Object`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
```

```
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

Contoh jejak yang menggunakan pemilih acara lanjutan untuk mengecualikan AWS Key Management Service peristiwa

Contoh berikut membuat pemilih peristiwa lanjutan untuk jejak yang diberi nama untuk menyertakan *TrailName* peristiwa manajemen read-only dan write-only (dengan menghilangkan pem `readOnly` ilih), tetapi untuk mengecualikan () peristiwa. AWS Key Management Service AWS KMS Karena AWS KMS acara diperlakukan sebagai peristiwa manajemen, dan mungkin ada volume yang tinggi, mereka dapat berdampak besar pada CloudTrail tagihan Anda jika Anda memiliki lebih dari satu jejak yang menangkap peristiwa manajemen.

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan AWS KMS pencatatan peristiwa.

Untuk mulai mencatat AWS KMS peristiwa ke jejak lagi, hapus pem `eventSource` ilih, dan jalankan perintah lagi.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
```

```
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat peristiwa yang dikecualikan ke jejak lagi, hapus `eventSource` pemilih, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Contoh jejak yang menggunakan pemilih peristiwa lanjutan untuk mengecualikan peristiwa manajemen API Data Amazon RDS

Contoh berikut membuat pemilih peristiwa lanjutan untuk jejak yang diberi nama untuk menyertakan peristiwa manajemen read-only dan write-only (dengan menghilangkan pem `readOnly` ilih), tetapi untuk mengecualikan peristiwa manajemen API Data Amazon RDS. *`TrailName`* Untuk mengecualikan peristiwa manajemen API Data Amazon RDS, tentukan sumber peristiwa API Data Amazon RDS di nilai string untuk `eventSource` bidang:. `rdsdata.amazonaws.com`

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, peristiwa manajemen API Data Amazon RDS tidak dicatat, dan Anda tidak dapat mengubah setelan pencatatan peristiwa Amazon RDS Data API.

Untuk mulai mencatat peristiwa manajemen API Data Amazon RDS ke jejak lagi, hapus pem `eventSource` ilih, dan jalankan perintah lagi.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat peristiwa yang dikecualikan ke jejak lagi, hapus `eventSource` pemilih, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
```

```
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Mengkonfigurasi pemilih acara dasar

Anda hanya dapat menggunakan pemilih peristiwa dasar untuk mencatat peristiwa manajemen dan peristiwa data untuk`AWS::DynamoDB::Table`,`AWS::Lambda::Function`, dan jenis `AWS::S3::Object` sumber daya. Anda dapat mencatat peristiwa manajemen, semua jenis sumber daya data, dan peristiwa aktivitas jaringan dengan menggunakan pemilih peristiwa lanjutan.

Anda dapat menggunakan pemilih acara dasar, atau pemilih acara lanjutan, tetapi tidak keduanya. Jika Anda menerapkan pemilih peristiwa dasar ke jejak yang menggunakan pemilih peristiwa lanjutan, pemilih peristiwa lanjutan akan diganti.

Untuk melihat pengaturan pemilih acara untuk jejak, jalankan `get-event-selectors` perintah. Anda harus menjalankan perintah ini dari Wilayah AWS tempat ia dibuat (Home Region), atau Anda harus menentukan Wilayah itu dengan menggunakan --region parameter.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> Jika jejak adalah jejak organisasi dan Anda adalah akun anggota di organisasi di AWS Organizations, Anda harus memberikan ARN lengkap dari jejak itu, dan bukan hanya namanya.

Contoh berikut menunjukkan pengaturan untuk jejak yang menggunakan pemilih peristiwa dasar untuk mencatat peristiwa manajemen.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
```

```
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk membuat pemilih acara, jalankan `put-event-selectors` perintah. Jika Anda ingin mencatat peristiwa Wawasan di jalur, pastikan pemilih peristiwa mengaktifkan pencatatan jenis Wawasan yang ingin Anda konfigurasi jejak Anda. Untuk informasi selengkapnya tentang mencatat peristiwa Wawasan, lihatBekerja dengan CloudTrail Wawasan.

Saat peristiwa terjadi di akun Anda, CloudTrail evaluasi konfigurasi untuk jalur Anda. Jika acara cocok dengan pemilih acara apa pun untuk jejak, jejak memproses dan mencatat peristiwa tersebut. Anda dapat mengonfigurasi hingga 5 pemilih acara untuk jejak dan hingga 250 sumber daya data untuk jejak. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data.

Topik

- Contoh jejak dengan pemilih acara tertentu
- Contoh jejak yang mencatat semua peristiwa manajemen dan data
- Contoh jejak yang tidak mencatat AWS Key Management Service peristiwa
- Contoh jejak yang mencatat volume rendah yang relevan AWS Key Management Service peristiwa
- Contoh jejak yang tidak mencatat peristiwa API data Amazon RDS

Contoh jejak dengan pemilih acara tertentu

Contoh berikut membuat pemilih peristiwa untuk jejak yang diberi nama untuk menyer *`TrailName`* takan peristiwa manajemen read-only dan write-only, peristiwa data untuk dua bucket/prefix kombinasi Amazon S3, dan peristiwa data untuk satu fungsi bernama. AWS Lambda *`hello-world-python-function`*

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-
demo-bucket/prefix","arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"]},
{"Type": "AWS::Lambda::Function","Values": ["arn:aws:lambda:us-
west-2:999999999999:function:hello-world-python-function"]}]}]'
```

Contoh mengembalikan pemilih acara yang dikonfigurasi untuk jejak.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Contoh jejak yang mencatat semua peristiwa manajemen dan data

Contoh berikut membuat pemilih peristiwa untuk jejak bernama *TrailName2* yang mencakup semua peristiwa manajemen, termasuk peristiwa manajemen read-only dan write-only, dan peristiwa data untuk semua bucket, AWS Lambda fungsi, dan tabel Amazon DynamoDB di Amazon S3. Akun AWS Karena contoh ini menggunakan pemilih peristiwa dasar, contoh ini tidak dapat mengonfigurasi logging untuk peristiwa S3 aktif AWS Outposts, JSON-RPC panggilan Amazon Managed Blockchain pada node Ethereum, atau jenis sumber daya pemilih peristiwa lanjutan lainnya. Anda juga tidak dapat mencatat peristiwa aktivitas jaringan menggunakan pemilih peristiwa dasar. Anda harus menggunakan pemilih peristiwa lanjutan untuk mencatat peristiwa aktivitas jaringan dan peristiwa data untuk semua jenis sumber daya lainnya. Untuk informasi selengkapnya, lihat Mengkonfigurasi pemilih acara lanjutan.

> **Note**
>
> Jika jejak hanya berlaku untuk satu Wilayah, hanya peristiwa di Wilayah tersebut yang dicatat, meskipun parameter pemilih peristiwa menentukan semua bucket Amazon S3 dan fungsi Lambda. Pemilih acara hanya berlaku untuk Wilayah tempat jejak dibuat.

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

Contoh mengembalikan pemilih acara yang dikonfigurasi untuk jejak.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
```

```
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

Contoh jejak yang tidak mencatat AWS Key Management Service peristiwa

Contoh berikut membuat pemilih peristiwa untuk jejak yang diberi nama untuk menyertakan peristiwa manajemen read-only dan write-only, tetapi untuk mengecualikan () event. *TrailName* AWS Key Management Service AWS KMS Karena AWS KMS acara diperlakukan sebagai peristiwa manajemen, dan mungkin ada volume yang tinggi, mereka dapat berdampak besar pada CloudTrail tagihan Anda jika Anda memiliki lebih dari satu jejak yang menangkap peristiwa manajemen. Pengguna dalam contoh ini telah memilih untuk mengecualikan AWS KMS peristiwa dari setiap jejak kecuali satu. Untuk mengecualikan sumber peristiwa, tambahkan `ExcludeManagementEventSources` ke pemilih acara Anda, dan tentukan sumber peristiwa dalam nilai string.

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan AWS KMS pencatatan peristiwa.

Untuk mulai AWS KMS mencatat peristiwa ke jejak lagi, berikan array kosong sebagai nilai`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

Contoh mengembalikan pemilih peristiwa yang dikonfigurasi untuk jejak.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat AWS KMS peristiwa ke jejak lagi, berikan array kosong sebagai nilai`ExcludeManagementEventSources`, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Contoh jejak yang mencatat volume rendah yang relevan AWS Key Management Service peristiwa

Contoh berikut membuat pemilih peristiwa untuk jejak yang diberi nama untuk menyer *TrailName* takan peristiwa dan peristiwa manajemen khusus tulis. AWS KMS Karena AWS KMS acara diperlakukan sebagai peristiwa manajemen, dan mungkin ada volume yang tinggi, mereka dapat berdampak besar pada CloudTrail tagihan Anda jika Anda memiliki lebih dari satu jejak yang menangkap peristiwa manajemen. Pengguna dalam contoh ini telah memilih untuk menyertakan peristiwa T AWS KMS ulis, yang akan menyertakan`Disable`, `Delete` dan`ScheduleKey`, tetapi tidak lagi menyertakan tindakan volume tinggi seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` (ini sekarang diperlakukan sebagai acara Baca).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Contoh mengembalikan pemilih peristiwa yang dikonfigurasi untuk jejak. Ini mencatat peristiwa manajemen penulisan saja, termasuk AWS KMS peristiwa.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Contoh jejak yang tidak mencatat peristiwa API data Amazon RDS

Contoh berikut membuat pemilih peristiwa untuk jejak yang diberi nama untuk menyertakan peristiwa manajemen read-only dan write-only, tetapi untuk mengecualikan peristiwa API Data

Amazon RDS. *TrailName* Karena peristiwa API Data Amazon RDS diperlakukan sebagai peristiwa manajemen, dan mungkin ada volume yang tinggi, peristiwa tersebut dapat berdampak besar pada CloudTrail tagihan Anda jika Anda memiliki lebih dari satu jejak yang menangkap peristiwa manajemen. Pengguna dalam contoh ini telah memilih untuk mengecualikan peristiwa API Data Amazon RDS dari setiap jejak kecuali satu. Untuk mengecualikan sumber peristiwa, tambahkan `ExcludeManagementEventSources` ke pemilih acara Anda, dan tentukan sumber peristiwa API Data Amazon RDS dalam nilai string:. `rdsdata.amazonaws.com`

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, peristiwa API Data Amazon RDS tidak dicatat, dan Anda tidak dapat mengubah setelan pencatatan peristiwa.

Untuk mulai mencatat peristiwa manajemen API Data Amazon RDS ke jejak lagi, berikan array kosong sebagai nilai`ExcludeManagementEventSources`.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

Contoh mengembalikan pemilih peristiwa yang dikonfigurasi untuk jejak.

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat peristiwa manajemen API Data Amazon RDS ke jejak lagi, berikan array kosong sebagai nilai`ExcludeManagementEventSources`, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Menghentikan dan mulai mencatat jejak

Perintah berikut memulai dan menghentikan CloudTrail logging.

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> Sebelum menghapus bucket, jalankan `stop-logging` perintah untuk berhenti mengirimkan acara ke bucket. Jika Anda tidak menghentikan pencatatan CloudTrail , cobalah untuk mengirimkan file log ke bucket dengan nama yang sama untuk jangka waktu terbatas.
> Jika Anda berhenti mencatat atau menghapus jejak, CloudTrail Insights dinonaktifkan pada jejak tersebut.

> **Pengiriman acara setelah logging dihentikan**
>
> Setelah Anda berhenti mencatat jejak, jejak masih dapat menerima peristiwa yang terjadi sebelum pencatatan dihentikan. Peristiwa dapat ditunda karena sejumlah alasan, termasuk lalu lintas jaringan yang tinggi, masalah konektivitas, pemadaman layanan, atau pembaruan untuk peristiwa yang ada. CloudTrail menggunakan waktu terakhir pencatatan dihentikan untuk menentukan apakah akan mengirimkan peristiwa yang tertunda, bukan status pencatatan jejak pada saat peristiwa terjadi. Akibatnya, peristiwa tertunda yang terjadi sebelum penebangan terakhir dihentikan masih dapat dikirim ke jalur. Untuk informasi selengkapnya tentang pengiriman acara yang tertunda, lihat `addendum` bidang di[CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan](#).
> Selain itu, pemilih acara dan pemilih acara lanjutan tidak dievaluasi untuk peristiwa tertunda yang dikirim ke jejak setelah pencatatan dihentikan. Ini berarti bahwa jejak dapat menerima semua jenis peristiwa yang terjadi sebelum pencatatan dihentikan, terlepas dari konfigurasi pemilih peristiwa jejak.

Menghapus jejak

Jika Anda telah mengaktifkan peristiwa CloudTrail manajemen di Amazon Security Lake, Anda diharuskan untuk memelihara setidaknya satu jejak organisasi yaitu Multi-wilayah dan mencatat

keduanya `read` dan peristiwa `write` manajemen. Anda tidak dapat menghapus jejak jika itu adalah satu-satunya jejak yang Anda miliki yang memenuhi persyaratan ini, kecuali Anda mematikan acara CloudTrail manajemen di Security Lake.

Anda dapat menghapus jejak dengan perintah berikut. Anda dapat menghapus jejak hanya di Wilayah yang dibuat (Wilayah Rumah).

> **Important**
>
> Meskipun menghapus CloudTrail jejak adalah tindakan yang CloudTrail tidak dapat diubah, tidak menghapus file log di bucket Amazon S3 untuk jejak tersebut, bucket Amazon S3 itu sendiri, atau grup CloudWatch log tempat jejak mengirimkan peristiwa. Menghapus jejak Multi-wilayah akan menghentikan pencatatan peristiwa di semua AWS Wilayah yang diaktifkan di Anda Akun AWS. Menghapus jejak satu wilayah akan menghentikan pencatatan peristiwa di Wilayah tersebut saja. Itu tidak akan menghentikan pencatatan peristiwa di Wilayah lain bahkan jika jalur di Wilayah lain tersebut memiliki nama yang identik dengan jejak yang dihapus.
> Untuk informasi tentang penutupan akun dan penghapusan CloudTrail jalur, lihatAkun AWS penutupan dan jalan setapak.

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Saat menghapus jejak, Anda tidak menghapus bucket Amazon S3 atau topik Amazon SNS yang terkait dengannya. Gunakan API Konsol Manajemen AWS, AWS CLI, atau layanan untuk menghapus sumber daya ini secara terpisah.

Membuat beberapa jalur

Anda dapat menggunakan file CloudTrail log untuk memecahkan masalah operasional atau keamanan di akun Anda AWS . Anda dapat membuat jejak untuk pengguna yang berbeda, yang dapat membuat dan mengelola jalur mereka sendiri. Anda dapat mengonfigurasi jejak untuk mengirimkan file log ke bucket S3 terpisah atau bucket S3 bersama.

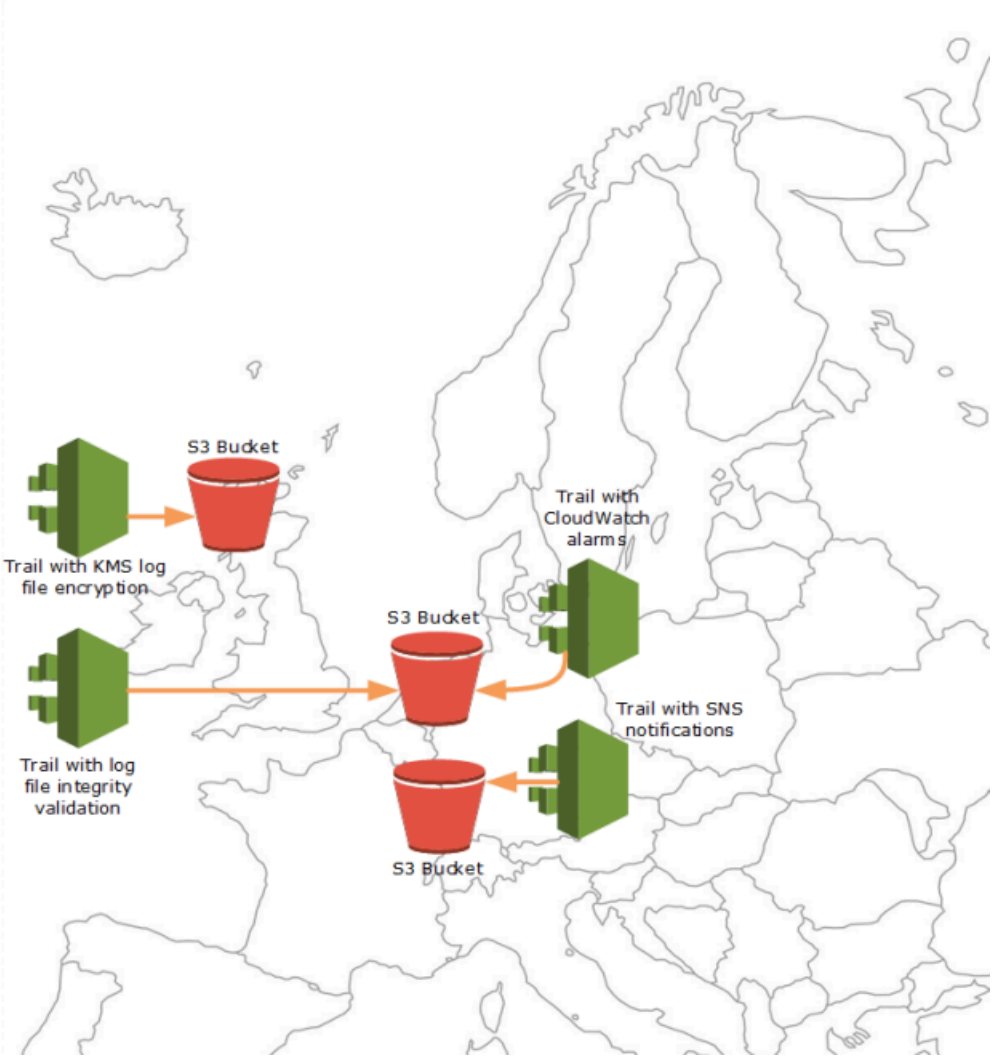
> **Note**
>
> Salinan pertama acara manajemen di masing-masing akun Wilayah AWS gratis. Jika Anda membuat lebih banyak jalur yang mengirimkan acara manajemen yang sama ke tujuan lain,

pengiriman berikutnya akan dikenakan CloudTrail biaya. Untuk informasi selengkapnya tentang CloudTrail biaya, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail jejak.

Misalnya, Anda mungkin memiliki pengguna berikut:

- Administrator keamanan membuat jejak di Wilayah Eropa (Irlandia) dan mengonfigurasi enkripsi file log KMS. Jejak mengirimkan file log ke ember S3 di Wilayah Eropa (Irlandia).
- Auditor TI membuat jejak di Wilayah Eropa (Irlandia) dan mengonfigurasi validasi integritas file log untuk memastikan file log tidak berubah sejak dikirimkan. CloudTrail Jejak dikonfigurasi untuk mengirimkan file log ke bucket S3 di Wilayah Eropa (Frankfurt)
- Pengembang membuat jejak di Wilayah Eropa (Frankfurt) dan mengonfigurasi CloudWatch alarm untuk menerima pemberitahuan untuk aktivitas API tertentu. Trail berbagi bucket S3 yang sama dengan jejak yang dikonfigurasi untuk integritas file log.
- Pengembang lain membuat jejak di Wilayah Eropa (Frankfurt) dan mengkonfigurasi SNS. File log dikirim ke bucket S3 terpisah di Wilayah Eropa (Frankfurt).

Gambar berikut menggambarkan contoh ini.



> **Note**
>
> Anda dapat membuat hingga lima jalur per Wilayah AWS. Jejak multi-wilayah dihitung sebagai satu jalur per Wilayah.

Anda dapat menggunakan izin tingkat sumber daya untuk mengelola kemampuan pengguna untuk melakukan operasi tertentu. CloudTrail

Misalnya, Anda mungkin memberikan izin kepada satu pengguna untuk melihat aktivitas jejak, tetapi membatasi pengguna untuk memulai atau menghentikan pencatatan untuk jejak. Anda dapat memberikan izin penuh kepada pengguna lain untuk membuat dan menghapus jejak. Ini memberi Anda kontrol terperinci atas jalur dan akses pengguna Anda.

Untuk informasi selengkapnya tentang izin tingkat sumber daya, lihat. Contoh: Membuat dan menerapkan kebijakan untuk tindakan pada jalur tertentu

Untuk informasi selengkapnya tentang beberapa jalur, lihat CloudTrail FAQ.

Membuat jejak untuk sebuah organisasi

Jika Anda telah membuat organisasi di AWS Organizations, Anda dapat membuat jejak yang mencatat semua peristiwa untuk semua Akun AWS di organisasi itu. Ini kadang-kadang disebut jejak organisasi.

Akun manajemen untuk organisasi dapat menetapkan administrator yang didelegasikan untuk membuat jejak organisasi baru atau mengelola jejak organisasi yang ada. Untuk informasi selengkapnya tentang menambahkan administrator yang didelegasikan, lihatMenambahkan administrator yang CloudTrail didelegasikan.

Akun manajemen untuk organisasi dapat mengedit jejak yang ada di akun mereka, dan menerapkannya ke organisasi, menjadikannya jejak organisasi. Organisasi melacak peristiwa log untuk akun manajemen dan semua akun anggota di organisasi. Untuk informasi selengkapnya AWS Organizations, lihat Organizations Terminology and Concepts.

> **Note**
>
> Anda harus masuk dengan akun manajemen atau akun administrator yang didelegasikan yang terkait dengan organisasi untuk membuat jejak organisasi. Anda juga harus memiliki izin yang cukup untuk pengguna atau peran dalam manajemen atau akun administrator yang didelegasikan untuk membuat jejak. Jika Anda tidak memiliki izin yang memadai, Anda tidak akan memiliki opsi untuk menerapkan jejak ke organisasi.

Semua jejak organisasi yang dibuat menggunakan konsol adalah jejak organisasi multi-wilayah yang mencatat peristiwa dari diaktifkan di setiap akun anggota Wilayah AWS di organisasi. Untuk mencatat peristiwa di semua AWS partisi di organisasi Anda, buat jejak organisasi Multi-region di setiap partisi. Anda dapat membuat jejak organisasi Single-region atau Multi-region dengan menggunakan. AWS CLI Jika Anda membuat jejak wilayah Tunggal, Anda mencatat aktivitas hanya di jalur Wilayah AWS (juga disebut sebagai Wilayah Asal).

Meskipun sebagian besar Wilayah AWS diaktifkan secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual (juga disebut sebagai Wilayah keikutsertaan).

Untuk informasi tentang Wilayah mana yang diaktifkan secara default, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi.AWS Account Management Untuk daftar CloudTrail dukungan Wilayah, lihatCloudTrail Daerah yang didukung.

Saat Anda membuat jejak organisasi, salinan jejak dengan nama yang Anda berikan dibuat di akun anggota milik organisasi Anda.

- Jika jejak organisasi adalah untuk Wilayah Tunggal dan Wilayah asal jejak bukan Wilayah keikutsertaan, salinan jejak dibuat di Wilayah asal jejak organisasi di setiap akun anggota.
- Jika jejak organisasi adalah untuk Wilayah Tunggal dan Wilayah asal jejak adalah Wilayah keikutsertaan, salinan jejak tersebut dibuat di Wilayah asal jejak organisasi di akun anggota yang telah mengaktifkan Wilayah tersebut.
- Jika jejak organisasi adalah Multi-wilayah dan Wilayah asal jejak bukan merupakan Wilayah keikutsertaan, salinan jejak dibuat di setiap akun yang diaktifkan Wilayah AWS di setiap akun anggota. Ketika akun anggota mengaktifkan Wilayah keikutsertaan, salinan jejak Multi-wilayah dibuat di Wilayah yang baru dipilih untuk akun anggota setelah aktivasi Wilayah tersebut selesai.
- Jika jejak organisasi adalah Multi-wilayah dan Wilayah asal adalah Wilayah keikutsertaan, akun anggota tidak akan mengirim aktivitas ke jejak organisasi kecuali mereka memilih Wilayah AWS tempat jejak Multi-wilayah dibuat. Misalnya, jika Anda membuat jejak Multi-wilayah dan memilih Wilayah Eropa (Spanyol) sebagai Wilayah asal untuk jejak tersebut, hanya akun anggota yang mengaktifkan Wilayah Eropa (Spanyol) untuk akun mereka yang akan mengirimkan aktivitas akun mereka ke jejak organisasi.

> **Note**
>
> CloudTrail membuat jejak organisasi di akun anggota meskipun validasi sumber daya gagal. Contoh kegagalan validasi meliputi:
>
> - kebijakan bucket Amazon S3 yang salah
> - kebijakan topik Amazon SNS yang salah
> - ketidakmampuan untuk mengirimkan ke grup CloudWatch log Log
> - izin yang tidak memadai untuk mengenkripsi menggunakan kunci KMS

Akun anggota dengan CloudTrail izin dapat melihat kegagalan validasi untuk jejak organisasi dengan melihat halaman detail jejak di CloudTrail konsol, atau dengan menjalankan perintah. AWS CLI get-trail-status

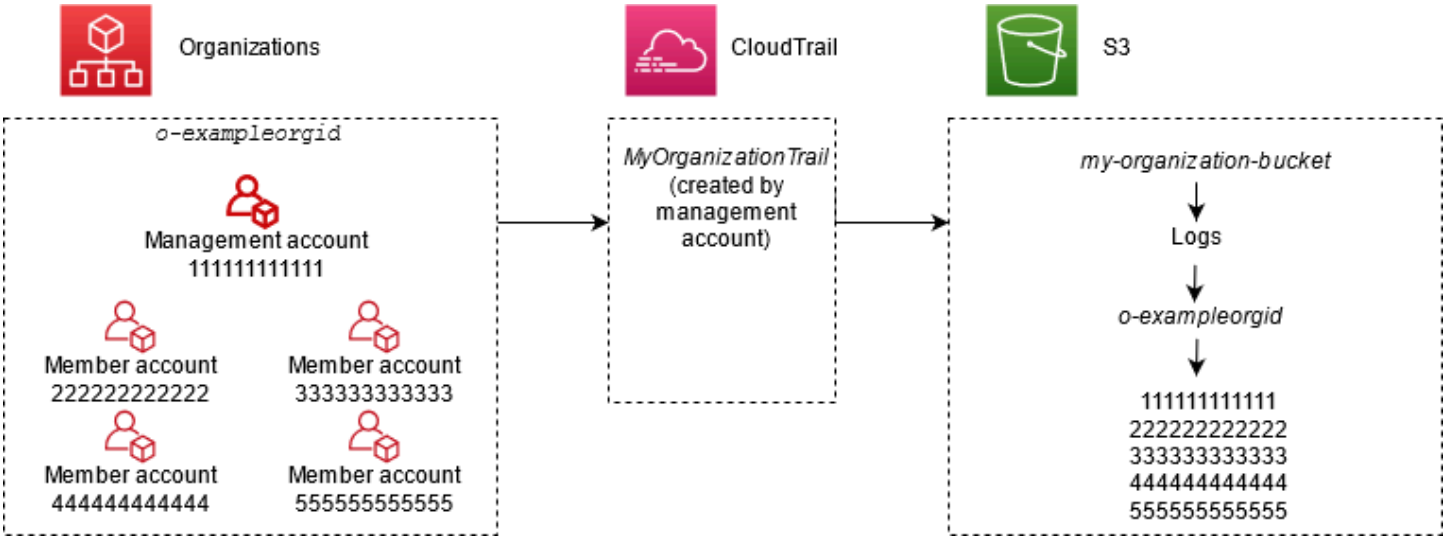
Pengguna dengan CloudTrail izin di akun anggota dapat melihat jejak organisasi saat mereka masuk ke CloudTrail konsol dari akun mereka Akun AWS, atau ketika mereka menjalankan AWS CLI perintah seperti. `describe-trails` Namun, pengguna di akun anggota tidak memiliki izin yang cukup untuk menghapus jejak organisasi, mengaktifkan atau menonaktifkan log, mengubah jenis peristiwa apa yang dicatat, atau mengubah jejak organisasi dengan cara apa pun.

Saat Anda membuat jejak organisasi di konsol, CloudTrail buat peran terkait layanan untuk melakukan tugas pencatatan di akun anggota organisasi Anda. Peran ini diberi nama AWSServiceRoleForCloudTrail, dan diperlukan CloudTrail untuk mencatat peristiwa untuk organisasi. Jika Akun AWS ditambahkan ke organisasi, jejak organisasi dan peran terkait layanan ditambahkan ke dalamnya Akun AWS, dan pencatatan dimulai untuk akun tersebut secara otomatis di jejak organisasi. Jika sebuah Akun AWS dihapus dari organisasi, jejak organisasi dan peran terkait layanan dihapus dari Akun AWS yang tidak lagi menjadi bagian dari organisasi. Namun, file log untuk akun yang dihapus yang dibuat sebelum penghapusan akun tetap berada di bucket Amazon S3 tempat file log disimpan untuk jejak.

Jika akun manajemen untuk AWS Organizations organisasi membuat jejak organisasi, tetapi kemudian dihapus sebagai akun manajemen organisasi, jejak organisasi apa pun yang dibuat menggunakan akun mereka menjadi jejak non-organisasi.

Dalam contoh berikut, akun manajemen organisasi 111111111111 membuat jejak yang dinamai untuk organisasi. *`MyOrganizationTrail o-exampleorgid`* Aktivitas log jejak untuk semua akun di organisasi dalam bucket Amazon S3 yang sama. Semua akun di organisasi dapat melihat *`MyOrganizationTrail`* dalam daftar jejak mereka, tetapi akun anggota tidak dapat menghapus atau mengubah jejak organisasi. Hanya akun manajemen atau akun administrator yang didelegasikan yang dapat mengubah atau menghapus jejak untuk organisasi. Hanya akun manajemen yang dapat menghapus akun anggota dari organisasi. Demikian pula, secara default, hanya akun manajemen yang memiliki akses ke bucket Amazon S3 untuk jejak, dan log yang terkandung di dalamnya. Struktur bucket tingkat tinggi untuk file log berisi folder bernama dengan ID organisasi, dan subfolder yang diberi nama dengan ID akun untuk setiap akun di organisasi. Acara untuk setiap akun anggota dicatat di folder yang sesuai dengan ID akun anggota. Jika akun anggota 44444444444444 dihapus dari organisasi, *`MyOrganizationTrail`* dan peran terkait layanan tidak

lagi muncul di AWS akun 444444444444444, dan tidak ada peristiwa lebih lanjut yang dicatat untuk akun tersebut oleh jejak organisasi. Namun, folder 444444444444 tetap berada di bucket Amazon S3, dengan semua log dibuat sebelum penghapusan akun dari organisasi.



Dalam contoh ini, ARN jejak yang dibuat di akun manajemen adalah. `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail` ARN ini adalah ARN untuk jejak di semua akun anggota juga.

Jalur organisasi mirip dengan jalur biasa dalam banyak hal. Anda dapat membuat beberapa jalur untuk organisasi Anda, dan memilih apakah akan membuat jejak organisasi Multi-region atau Single-region, dan jenis peristiwa apa yang ingin Anda catat di jejak organisasi Anda, seperti di jejak lainnya. Namun, ada beberapa perbedaan. Misalnya, saat Anda membuat jejak di konsol dan memilih apakah akan mencatat peristiwa data untuk bucket atau AWS Lambda fungsi Amazon S3, satu-satunya sumber daya yang tercantum di CloudTrail konsol adalah sumber daya untuk akun manajemen, tetapi Anda dapat menambahkan ARN untuk sumber daya di akun anggota. Peristiwa data untuk sumber daya akun anggota tertentu dicatat tanpa harus mengonfigurasi akses lintas akun secara manual ke sumber daya tersebut. Untuk informasi selengkapnya tentang peristiwa manajemen logging, peristiwa Wawasan, dan peristiwa data, lihat Mencatat log peristiwa manajemenMencatat log peristiwa data, danBekerja dengan CloudTrail Wawasan.

> **Note**
>
> Di konsol, Anda membuat jejak Multi-wilayah. Ini adalah praktik terbaik yang disarankan untuk mencatat aktivitas di semua Wilayah yang diaktifkan di Anda Akun AWS, karena ini membantu Anda menjaga AWS lingkungan Anda lebih aman. Untuk membuat jejak wilayah Tunggal, gunakan. AWS CLI

Saat Anda melihat peristiwa dalam Riwayat acara untuk organisasi AWS Organizations, Anda dapat melihat acara hanya untuk acara Akun AWS yang Anda masuki. Misalnya, jika Anda masuk dengan akun manajemen organisasi, Riwayat acara menunjukkan 90 hari terakhir peristiwa manajemen untuk akun manajemen. Acara akun anggota organisasi tidak ditampilkan dalam Riwayat acara untuk akun manajemen. Untuk melihat peristiwa akun anggota di Riwayat acara, masuk dengan akun anggota.

Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log untuk jejak organisasi dengan cara yang sama seperti yang Anda lakukan untuk jejak lainnya. Misalnya, Anda dapat menganalisis data dalam jejak organisasi menggunakan Amazon Athena. Untuk informasi selengkapnya, lihat AWS integrasi layanan dengan log CloudTrail.

Topik

- Pindah dari jejak akun anggota ke jalur organisasi
- Bersiaplah untuk membuat jejak untuk organisasi Anda
- Membuat jejak untuk organisasi Anda di konsol
- Membuat jejak untuk organisasi dengan AWS CLI
- Memecahkan masalah dengan jejak organisasi

Pindah dari jejak akun anggota ke jalur organisasi

Jika Anda sudah memiliki CloudTrail jejak yang dikonfigurasi untuk akun anggota individu, tetapi ingin pindah ke jejak organisasi untuk mencatat peristiwa di semua akun, Anda tidak ingin kehilangan peristiwa dengan menghapus jejak akun anggota individu sebelum membuat jejak organisasi. Tetapi ketika Anda memiliki dua jalur, Anda dikenakan biaya lebih tinggi karena salinan acara tambahan yang dikirimkan ke jalur organisasi.

Untuk membantu mengelola biaya, tetapi hindari kehilangan acara sebelum pengiriman log dimulai di jalur organisasi, pertimbangkan untuk menjaga jejak akun anggota individu Anda dan jejak organisasi Anda hingga satu hari. Ini memastikan bahwa jejak organisasi mencatat semua peristiwa, tetapi Anda dikenakan biaya acara duplikat hanya untuk satu hari. Setelah hari pertama, Anda dapat berhenti masuk (atau menghapus) jejak akun anggota individu mana pun.

Bersiaplah untuk membuat jejak untuk organisasi Anda

Sebelum membuat jejak untuk organisasi, pastikan akun manajemen organisasi atau akun administrator yang didelegasikan disiapkan dengan benar untuk pembuatan jejak.

- Organisasi Anda harus mengaktifkan semua fitur sebelum Anda dapat membuat jejak untuk itu. Untuk informasi selengkapnya, lihat Mengaktifkan Semua Fitur di Organisasi Anda.
- Akun manajemen harus memiliki AWSServiceRoleForOrganizationsperan. Peran ini dibuat secara otomatis oleh Organizations saat Anda membuat organisasi, dan diperlukan CloudTrail untuk mencatat peristiwa untuk organisasi. Untuk informasi selengkapnya, lihat Organizations and service-linked role.
- Pengguna atau peran yang membuat jejak organisasi di akun administrator manajemen atau yang didelegasikan harus memiliki izin yang cukup untuk membuat jejak organisasi. Anda setidaknya harus menerapkan AWSCloudTrail_FullAccesskebijakan, atau kebijakan yang setara, untuk peran atau pengguna tersebut. Anda juga harus memiliki izin yang memadai di IAM dan Organizations untuk membuat peran terkait layanan dan mengaktifkan akses tepercaya. Jika Anda memilih untuk membuat bucket S3 baru untuk jejak organisasi menggunakan CloudTrail konsol, Kebijakan Anda juga harus menyertakan `s3:PutEncryptionConfiguration` tindakan karena secara default enkripsi sisi server diaktifkan untuk bucket. Contoh kebijakan berikut menunjukkan izin minimum yang diperlukan.

  > **Note**
  >
  > Anda tidak boleh membagikan AWSCloudTrail_FullAccesskebijakan secara luas di seluruh Anda Akun AWS. Sebaliknya, Anda harus membatasinya kepada Akun AWS administrator karena sifat sangat sensitif dari informasi yang dikumpulkan oleh. CloudTrail Pengguna dengan peran ini memiliki kemampuan untuk mematikan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di dalamnya. Akun AWS Untuk alasan ini, Anda harus mengontrol dan memantau akses ke kebijakan ini dengan cermat.

  JSON

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

```
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

- Untuk menggunakan AWS CLI atau CloudTrail API untuk membuat jejak organisasi, Anda harus mengaktifkan akses tepercaya untuk CloudTrail di Organizations, dan Anda harus membuat bucket Amazon S3 secara manual dengan kebijakan yang memungkinkan pencatatan untuk jejak organisasi. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dengan AWS CLI.
- Untuk menggunakan peran IAM yang ada untuk menambahkan pemantauan jejak organisasi ke CloudWatch Log Amazon, Anda harus mengubah peran IAM secara manual untuk mengizinkan pengiriman CloudWatch Log untuk akun anggota ke grup CloudWatch Log untuk akun manajemen, seperti yang ditunjukkan pada contoh berikut.

> **Note**
>
> Anda harus menggunakan peran IAM dan grup CloudWatch log Log yang ada di akun Anda sendiri. Anda tidak dapat menggunakan peran IAM atau grup CloudWatch log Log yang dimiliki oleh akun lain.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
```

```
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",

                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Anda dapat mempelajari lebih lanjut tentang CloudTrail dan Amazon CloudWatch Logs inMemantau File CloudTrail Log dengan CloudWatch Log Amazon. Selain itu, pertimbangkan batasan pada CloudWatch Log dan pertimbangan harga untuk layanan sebelum memutuskan untuk mengaktifkan pengalaman untuk jejak organisasi. Untuk informasi selengkapnya, lihat Batas CloudWatch Log dan CloudWatchHarga Amazon.

- Untuk mencatat peristiwa data di jejak organisasi Anda untuk sumber daya tertentu di akun anggota, siapkan daftar Nama Sumber Daya Amazon (ARN) untuk masing-masing sumber daya tersebut. Sumber daya akun anggota tidak ditampilkan di CloudTrail konsol saat Anda membuat jejak; Anda dapat menelusuri sumber daya di akun manajemen tempat pengumpulan peristiwa data didukung, seperti bucket S3. Demikian pula, jika Anda ingin menambahkan sumber daya anggota tertentu saat membuat atau memperbarui jejak organisasi di baris perintah, Anda memerlukan ARN untuk sumber daya tersebut.

> **Note**
>
> Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Anda juga harus mempertimbangkan untuk meninjau berapa banyak jejak yang sudah ada di akun manajemen dan di akun anggota sebelum membuat jejak organisasi. CloudTrail membatasi jumlah jalur yang dapat dibuat di setiap Wilayah. Anda tidak dapat melampaui batas ini di Wilayah tempat Anda membuat jejak organisasi di akun manajemen. Namun, jejak akan dibuat di akun anggota meskipun akun anggota telah mencapai batas jejak di Wilayah. Meskipun jejak pertama acara manajemen di Wilayah mana pun gratis, biaya berlaku untuk jalur tambahan. Untuk mengurangi potensi biaya jejak organisasi, pertimbangkan untuk menghapus jejak yang tidak dibutuhkan di akun manajemen dan anggota. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Praktik terbaik keamanan di jalur organisasi

Sebagai praktik terbaik keamanan, sebaiknya tambahkan kunci `aws:SourceArn` kondisi ke kebijakan sumber daya (seperti untuk bucket S3, kunci KMS, atau topik SNS) yang Anda gunakan dengan jejak organisasi. Nilai `aws:SourceArn` adalah jejak organisasi ARN (atau ARN, jika Anda menggunakan sumber daya yang sama untuk lebih dari satu jejak, seperti bucket S3 yang sama untuk menyimpan log untuk lebih dari satu jejak). Ini memastikan bahwa sumber daya, seperti bucket S3, hanya menerima data yang terkait dengan jejak tertentu. Trail ARN harus menggunakan ID akun akun manajemen. Cuplikan kebijakan berikut menunjukkan contoh di mana lebih dari satu jejak menggunakan sumber daya.

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

Untuk informasi tentang cara menambahkan kunci kondisi ke kebijakan sumber daya, lihat berikut ini:

- Kebijakan bucket Amazon S3 untuk CloudTrail
- Konfigurasi AWS KMS kebijakan utama untuk CloudTrail

- Kebijakan topik Amazon SNS untuk CloudTrail

Membuat jejak untuk organisasi Anda di konsol

Untuk membuat jejak organisasi dari CloudTrail konsol, Anda harus masuk ke konsol sebagai pengguna atau peran dalam manajemen atau akun administrator yang didelegasikan yang memiliki izin yang memadai. Jika Anda tidak masuk dengan akun administrator manajemen atau delegasi, Anda tidak akan melihat opsi untuk menerapkan jejak ke organisasi saat membuat atau mengedit jejak dari CloudTrail konsol.

Untuk membuat jejak organisasi dengan Konsol Manajemen AWS

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.

   Anda harus masuk menggunakan identitas IAM di manajemen atau akun administrator yang didelegasikan dengan izin yang memadai untuk membuat jejak organisasi.
2. Pilih Jejak, lalu pilih Buat jejak.
3. Pada halaman Create Trail, untuk nama Trail, ketikkan nama untuk jejak Anda. Untuk informasi selengkapnya, lihat Persyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS.
4. Pilih Aktifkan untuk semua akun di organisasi saya. Anda hanya melihat opsi ini jika Anda masuk ke konsol dengan pengguna atau peran di akun administrator manajemen atau yang didelegasikan. Agar berhasil membuat jejak organisasi, pastikan bahwa pengguna atau peran memiliki izin yang memadai.
5. Untuk lokasi Storage, pilih Create new S3 bucket untuk membuat bucket. Saat Anda membuat bucket, CloudTrail membuat dan menerapkan kebijakan bucket yang diperlukan.

   > **Note**
   >
   > Jika Anda memilih Gunakan bucket S3 yang ada, tentukan bucket di nama bucket log Trail, atau pilih Browse untuk memilih bucket. Anda dapat memilih bucket milik akun mana pun, namun kebijakan bucket harus memberikan CloudTrail izin untuk menulis ke akun tersebut. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon S3 untuk CloudTrail.

Untuk mempermudah menemukan log Anda, buat folder baru (juga dikenal sebagai awalan) di bucket yang ada untuk menyimpan CloudTrail log Anda. Masukkan awalan di Awalan.

6. Untuk SSE-KMS enkripsi file Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda dan mencerna file menggunakan SSE-KMS enkripsi alih-alih SSE-S3 enkripsi. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan SSE-KMS enkripsi, file log dan file digest Anda dienkripsi menggunakan enkripsi. SSE-S3 Untuk informasi selengkapnya tentang SSE-KMS enkripsi, lihat Menggunakan enkripsi sisi server dengan AWS Key Management Service (). SSE-KMS Untuk informasi selengkapnya tentang SSE-S3 enkripsi, lihat Menggunakan Server-Side Enkripsi dengan Kunci S3-Managed Enkripsi Amazon (SSE-S3).

   Jika Anda mengaktifkan SSE-KMS enkripsi, pilih New atau Existing AWS KMS key. Di AWS KMS Alias, tentukan alias, dalam format. `alias/` *`MyAliasName`* Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol.

   > **Note**
   >
   > Anda juga dapat mengetikkan ARN kunci dari akun lain. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol. Kebijakan kunci harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda dan mencerna file, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log atau mencerna file dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

7. Di Pengaturan tambahan, konfigurasikan yang berikut ini.

   a. Untuk validasi file Log, pilih Diaktifkan agar intisari log dikirimkan ke bucket S3 Anda. Anda dapat menggunakan file intisari untuk memverifikasi bahwa file log Anda tidak berubah setelah CloudTrail dikirimkan. Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas file log.

   b. Untuk pengiriman notifikasi SNS, pilih Diaktifkan untuk diberi tahu setiap kali log dikirimkan ke bucket Anda. CloudTrail menyimpan beberapa peristiwa dalam file log. Notifikasi SNS dikirim untuk setiap file log, bukan untuk setiap acara. Untuk informasi selengkapnya, lihat Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail.

Jika Anda mengaktifkan notifikasi SNS, untuk Membuat topik SNS baru, pilih Baru untuk membuat topik, atau pilih Ada untuk menggunakan topik yang ada. Jika Anda membuat jejak Multi-wilayah, pemberitahuan SNS untuk pengiriman file log dari semua Wilayah dikirim ke topik SNS tunggal yang Anda buat.

Jika Anda memilih Baru, CloudTrail menentukan nama untuk topik baru untuk Anda, atau Anda dapat mengetikkan nama. Jika Anda memilih yang ada, pilih topik SNS dari daftar drop-down. Anda juga dapat memasukkan ARN topik dari Wilayah lain atau dari akun dengan izin yang sesuai. Untuk informasi selengkapnya, lihat Kebijakan topik Amazon SNS untuk CloudTrail.

Jika Anda membuat topik, Anda harus berlangganan topik untuk diberitahu tentang pengiriman file log. Anda dapat berlangganan dari konsol Amazon SNS. Karena frekuensi pemberitahuan, kami menyarankan Anda mengonfigurasi langganan untuk menggunakan antrian Amazon SQS untuk menangani notifikasi secara terprogram. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

8. Secara opsional, konfigurasikan CloudTrail untuk mengirim file CloudWatch log ke Log dengan memilih Diaktifkan di CloudWatch Log. Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log.

> **Note**
>
> Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi menggunakan konsol. Administrator yang didelegasikan dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API.

   a. Jika Anda mengaktifkan integrasi dengan CloudWatch Log, pilih Baru untuk membuat grup log baru, atau Ada untuk menggunakan yang sudah ada. Jika Anda memilih Baru, CloudTrail menentukan nama untuk grup log baru untuk Anda, atau Anda dapat mengetikkan nama.

   b. Jika Anda memilih yang ada, pilih grup log dari daftar drop-down.

   c. Pilih Baru untuk membuat peran IAM baru untuk izin mengirim log ke CloudWatch Log. Pilih Existing untuk memilih peran IAM yang ada dari daftar drop-down. Pernyataan kebijakan

untuk peran baru atau yang sudah ada ditampilkan saat Anda memperluas dokumen Kebijakan. Untuk informasi selengkapnya tentang peran ini, silakan lihat Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

> **Note**
>
> Saat mengonfigurasi jejak, Anda dapat memilih bucket S3 dan topik Amazon SNS yang menjadi milik akun lain. Namun, jika Anda CloudTrail ingin mengirimkan peristiwa ke grup CloudWatch log Log, Anda harus memilih grup log yang ada di akun Anda saat ini.

9. Untuk Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke jejak Anda. Tag dapat membantu Anda mengidentifikasi CloudTrail jejak dan bucket Amazon S3 yang CloudTrail berisi file log. Anda kemudian dapat menggunakan grup sumber daya untuk CloudTrail sumber daya Anda. Untuk informasi selengkapnya, lihat AWS Resource Groups dan Tanda.
10. Pada halaman Pilih peristiwa log, pilih jenis acara yang ingin Anda log. Untuk acara Manajemen, lakukan hal berikut.

    a. Untuk aktivitas API, pilih apakah Anda ingin jejak Anda mencatat peristiwa Baca, peristiwa Tulis, atau keduanya. Untuk informasi selengkapnya, lihat Peristiwa manajemen.

    b. Pilih Kecualikan AWS KMS acara untuk memfilter AWS Key Management Service (AWS KMS) peristiwa dari jejak Anda. Pengaturan default adalah untuk memasukkan semua AWS KMS acara.

    Opsi untuk mencatat atau mengecualikan AWS KMS peristiwa hanya tersedia jika Anda mencatat peristiwa manajemen di jejak Anda. Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan AWS KMS peristiwa.

    AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Low-volume, AWS KMS tindakan yang relevan seperti`Disable`,`Delete`, dan `ScheduleKey` (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

    Untuk mengecualikan peristiwa bervolume tinggi seperti`Encrypt`,`Decrypt`, dan`GenerateDataKey`, tetapi masih mencatat peristiwa yang relevan seperti`Disable`,

`Delete` dan`ScheduleKey`, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa.

c. Pilih Kecualikan peristiwa Amazon RDS Data API untuk memfilter peristiwa Amazon Relational Database Service Data Data API dari jejak Anda. Pengaturan default adalah untuk menyertakan semua peristiwa Amazon RDS Data API. Untuk informasi selengkapnya tentang peristiwa Amazon RDS Data API, lihat Pencatatan panggilan API Data dengan AWS CloudTrail di Panduan Pengguna Amazon RDS untuk Aurora.

11. Untuk mencatat peristiwa data, pilih Peristiwa data. Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

12. **Important**

    Langkah 12-16 adalah untuk mengonfigurasi peristiwa data menggunakan pemilih acara lanjutan, yang merupakan default. Penyeleksi acara tingkat lanjut memungkinkan Anda mengonfigurasi lebih banyak jenis sumber daya dan menawarkan kontrol halus atas peristiwa data mana yang ditangkap jejak Anda. Jika Anda berencana untuk mencatat peristiwa aktivitas jaringan, Anda harus menggunakan pemilih acara lanjutan. Jika Anda menggunakan pemilih acara dasar, selesaikan langkah-langkahnyaKonfigurasikan pengaturan peristiwa data menggunakan pemilih acara dasar, lalu kembali ke langkah 17 dari prosedur ini.

    Untuk tipe Sumber Daya, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang jenis sumber daya yang tersedia, lihatPeristiwa data.

13. Pilih templat pemilih log. Anda dapat memilih template yang telah ditentukan sebelumnya, atau memilih Custom untuk menentukan kondisi koleksi acara Anda sendiri.

    Anda dapat memilih dari template yang telah ditentukan berikut:

    - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
    - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
    - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,`Delete*`, atau `Write*` peristiwa.

- Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
- Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` of`AwsServiceEvent`, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).

> **Note**
>
> Memilih template yang telah ditentukan untuk bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.
> Jika jejak hanya berlaku untuk satu Wilayah, memilih templat yang telah ditentukan sebelumnya yang mencatat semua bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS
> Jika Anda membuat jejak Multi-wilayah, memilih templat yang telah ditentukan untuk fungsi Lambda memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.
> Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh identitas IAM apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

14. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

15. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan `readOnly` pemilih.
- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk menyertakan atau mengecualikan peristiwa data apa pun yang dicatat CloudTrail, seperti`PutBucket`,`GetItem`, atau`GetSnapshotBlock`.
- **`eventSource`**— Sumber acara untuk menyertakan atau mengecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk dikecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType`diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- Sesi CredentialFromConsole — Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- pengguna Identity.arn - Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.`ARN, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan

ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai. `resources.type`

> **Note**
>
> Anda tidak dapat menggunakan `resources.ARN` bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Kunci tindakan, sumber daya, dan kondisi Layanan AWS di Referensi Otorisasi Layanan.

b. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data acara, Anda dapat menyetel bidang ke Resources.arn, mengatur operator untuk tidak memulai, lalu menempelkan ARN bucket S3 yang tidak ingin Anda catat peristiwa.

   Untuk menambahkan bucket S3 kedua, pilih + Condition, lalu ulangi instruksi sebelumnya, tempelkan di ARN untuk atau jelajahi bucket yang berbeda.

   Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

c. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan tentukan ARN dalam satu pemilih agar sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

16. Untuk menambahkan jenis sumber daya untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 12 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk jenis sumber daya.

17. Untuk mencatat peristiwa aktivitas jaringan, pilih Acara aktivitas jaringan. Peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

    Untuk mencatat peristiwa aktivitas jaringan, lakukan hal berikut:

    a. Dari sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

    b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua peristiwa yang ditolak akses aktivitas jaringan, atau memilih Kustom untuk membuat pemilih log kustom untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

    c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

    d. Di Penyeleksi acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

        i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

        - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
        - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
        - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan`vpcEndpointId`.

        ii. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi.

        iii. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

    e. Untuk menambahkan sumber peristiwa lain yang ingin Anda log peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

18. Pilih acara Insights jika Anda ingin jejak Anda mencatat peristiwa CloudTrail Wawasan.

    Di Jenis acara, pilih Acara Wawasan. Dalam peristiwa Insights, pilih API call rate, API error rate, atau keduanya. Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.

    CloudTrail Wawasan menganalisis peristiwa manajemen untuk aktivitas yang tidak biasa, dan mencatat peristiwa saat anomali terdeteksi. Secara default, jejak tidak mencatat peristiwa Wawasan. Untuk informasi selengkapnya tentang peristiwa Wawasan, lihatBekerja dengan CloudTrail Wawasan. Biaya tambahan berlaku untuk acara logging Insights. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

    Peristiwa Insights dikirimkan ke folder berbeda bernama `/CloudTrail-Insight` bucket S3 yang sama yang ditentukan di area lokasi penyimpanan halaman detail jejak. CloudTrailmenciptakan awalan baru untuk Anda. Misalnya, jika bucket S3 tujuan Anda saat ini diberi nama`amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail-Insight/`

19. Setelah selesai memilih jenis acara untuk dicatat, pilih Berikutnya.

20. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit di bagian untuk mengubah pengaturan jejak yang ditampilkan di bagian itu. Saat Anda siap untuk membuat jejak, pilih Buat jejak.

21. Jejak baru muncul di halaman Trails. Jejak organisasi mungkin membutuhkan waktu hingga 24 jam untuk dibuat di semua Wilayah yang diaktifkan di semua akun anggota. Halaman Trails menunjukkan jejak di akun Anda dari semua Wilayah. Dalam waktu sekitar 5 menit, CloudTrail menerbitkan file log yang menampilkan panggilan AWS API yang dilakukan di organisasi Anda. Anda dapat melihat file log di bucket Amazon S3 yang Anda tentukan.

> **Note**
>
> Anda tidak dapat mengganti nama jejak setelah dibuat. Sebagai gantinya, Anda dapat menghapus jejak dan membuat yang baru.

Langkah selanjutnya

Setelah Anda membuat jejak Anda, Anda dapat kembali ke jejak untuk membuat perubahan:

- Ubah konfigurasi jejak Anda dengan mengeditnya. Untuk informasi selengkapnya, lihat Memperbarui jejak dengan CloudTrail konsol.
- Jika diperlukan, konfigurasikan bucket Amazon S3 untuk memungkinkan pengguna tertentu di akun anggota membaca file log untuk organisasi. Untuk informasi selengkapnya, lihat Berbagi file CloudTrail log antar AWS akun.
- Konfigurasikan CloudTrail untuk mengirim file log ke CloudWatch Log. Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log dan item CloudWatch Log masukBersiaplah untuk membuat jejak untuk organisasi Anda.

  > **Note**
  >
  > Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi.

- Buat tabel dan gunakan untuk menjalankan kueri di Amazon Athena untuk menganalisis aktivitas AWS layanan Anda. Untuk informasi selengkapnya, lihat Membuat Tabel untuk CloudTrail Log di CloudTrail Konsol di Panduan Pengguna Amazon Athena.
- Tambahkan tag khusus (pasangan nilai kunci) ke jejak.
- Untuk membuat jejak organisasi lain, kembali ke halaman Trails dan pilih Buat jejak.

> **Note**
>
> Saat mengonfigurasi jejak, Anda dapat memilih bucket Amazon S3 dan topik SNS yang menjadi milik akun lain. Namun, jika Anda CloudTrail ingin mengirimkan peristiwa ke grup CloudWatch log Log, Anda harus memilih grup log yang ada di akun Anda saat ini.

Membuat jejak untuk organisasi dengan AWS CLI

Anda dapat membuat jejak organisasi dengan menggunakan AWS CLI. AWS CLI Ini diperbarui secara berkala dengan fungsionalitas dan perintah tambahan. Untuk membantu memastikan kesuksesan, pastikan bahwa Anda telah menginstal atau memperbarui ke AWS CLI versi terbaru sebelum Anda mulai.

> **Note**
>
> Contoh di bagian ini khusus untuk membuat dan memperbarui jejak organisasi. Untuk contoh menggunakan AWS CLI untuk mengelola jalur, lihat Mengelola jalur dengan AWS CLI danMengkonfigurasi pemantauan CloudWatch Log dengan AWS CLI. Saat membuat atau memperbarui jejak organisasi dengan AWS CLI, Anda harus menggunakan AWS CLI profil di akun manajemen atau akun administrator yang didelegasikan dengan izin yang memadai. Jika Anda mengubah jejak organisasi menjadi jejak non-organisasi, Anda harus menggunakan akun manajemen untuk organisasi tersebut.
> Anda harus mengonfigurasi bucket Amazon S3 yang digunakan untuk jejak organisasi dengan izin yang memadai.

Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi

Anda harus menentukan bucket Amazon S3 untuk menerima file log untuk jejak organisasi. Bucket ini harus memiliki kebijakan yang memungkinkan CloudTrail untuk menempatkan file log untuk organisasi ke dalam bucket.

Berikut ini adalah contoh kebijakan untuk bucket Amazon S3 bernama*amzn-s3-demo-bucket*, yang dimiliki oleh akun manajemen organisasi. Ganti *amzn-s3-demo-bucketregion*,*managementAccountID*,*trailName*,, dan *o-organizationID* dengan nilai-nilai untuk organisasi Anda

Kebijakan bucket ini berisi tiga pernyataan.

- Pernyataan pertama memungkinkan CloudTrail untuk memanggil `GetBucketAcl` tindakan Amazon S3 di ember Amazon S3.
- Pernyataan kedua memungkinkan pencatatan jika jejak diubah dari jejak organisasi menjadi jejak untuk akun itu saja.
- Pernyataan ketiga memungkinkan pencatatan untuk jejak organisasi.

Kebijakan contoh menyertakan kunci `aws:SourceArn` kondisi untuk kebijakan bucket Amazon S3. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk jejak atau jalur tertentu. Dalam jejak organisasi, nilai `aws:SourceArn` harus berupa jejak ARN yang dimiliki oleh akun manajemen, dan menggunakan ID akun manajemen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/
AWSLogs/managementAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/AWSLogs/o-
organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Kebijakan contoh ini tidak mengizinkan pengguna dari akun anggota untuk mengakses file log yang dibuat untuk organisasi. Secara default, file log organisasi hanya dapat diakses oleh akun manajemen. Untuk informasi tentang cara mengizinkan akses baca ke bucket Amazon S3 untuk pengguna IAM di akun anggota, lihat. Berbagi file CloudTrail log antar AWS akun

Mengaktifkan CloudTrail sebagai layanan tepercaya di AWS Organizations

Sebelum Anda dapat membuat jejak organisasi, Anda harus terlebih dahulu mengaktifkan semua fitur di Organizations. Untuk informasi selengkapnya, lihat Mengaktifkan Semua Fitur di Organisasi Anda, atau jalankan perintah berikut menggunakan profil dengan izin yang memadai di akun manajemen:

```
aws organizations enable-all-features
```

Setelah mengaktifkan semua fitur, Anda harus mengonfigurasi Organizations agar dipercaya CloudTrail sebagai layanan tepercaya.

Untuk membuat hubungan layanan tepercaya antara AWS Organizations dan CloudTrail, buka terminal atau baris perintah dan gunakan profil di akun manajemen. Jalankan `aws organizations enable-aws-service-access` perintah, seperti yang ditunjukkan dalam contoh berikut.

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

Menggunakan create-trail

Membuat jejak organisasi yang berlaku untuk semua Wilayah

Untuk membuat jejak organisasi yang berlaku untuk semua Wilayah, tambahkan `--is-organization-trail` dan `--is-multi-region-trail` opsi.

> **Note**
>
> Saat Anda membuat jejak organisasi dengan AWS CLI, Anda harus menggunakan AWS CLI profil di akun manajemen atau akun administrator yang didelegasikan dengan izin yang memadai.

Contoh berikut membuat jejak organisasi yang mengirimkan log dari semua Wilayah ke bucket yang sudah ada bernama*amzn-s3-demo-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-
organization-trail --is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak Anda ada di semua Wilayah, `IsMultiRegionTrail` parameter `IsOrganizationTrail` dan dalam output disetel ke`true`:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

> **Note**
>
> Jalankan `start-logging` perintah untuk mulai mencatat jejak Anda. Untuk informasi selengkapnya, lihat Menghentikan dan mulai mencatat jejak.

Membuat jejak organisasi sebagai jalur Single-region

Perintah berikut membuat jejak organisasi yang hanya mencatat peristiwa dalam satu Wilayah AWS, juga dikenal sebagai jejak wilayah Tunggal. AWS Wilayah tempat peristiwa dicatat adalah Wilayah yang ditentukan dalam profil konfigurasi untuk AWS CLI.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-organization-trail
```

Untuk informasi selengkapnya, lihat Persyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS.

Contoh output:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Secara default, `create-trail` perintah membuat jejak wilayah Tunggal yang tidak mengaktifkan validasi file log.

> **Note**
>
> Jalankan `start-logging` perintah untuk mulai mencatat jejak Anda.

Berjalan perbaruan-jejak untuk memperbarui jejak organisasi

Anda dapat menjalankan `update-trail` perintah untuk mengubah pengaturan konfigurasi untuk jejak organisasi, atau menerapkan jejak yang ada untuk satu AWS akun ke seluruh organisasi. Ingatlah bahwa Anda dapat menjalankan `update-trail` perintah hanya dari Wilayah tempat jejak itu dibuat.

> **Note**
>
> Jika Anda menggunakan AWS CLI atau salah satu AWS SDK untuk memperbarui jejak, pastikan kebijakan bucket trail sudah mutakhir. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dengan AWS CLI.
> Ketika Anda memperbarui jejak organisasi dengan AWS CLI, Anda harus menggunakan AWS CLI profil di akun manajemen atau akun administrator yang didelegasikan dengan izin yang memadai. Jika Anda ingin mengubah jejak organisasi menjadi jejak non-organisasi, Anda harus menggunakan akun manajemen untuk organisasi, karena akun manajemen adalah pemilik semua sumber daya organisasi.
> CloudTrail memperbarui jejak organisasi di akun anggota meskipun validasi sumber daya gagal. Contoh kegagalan validasi meliputi:
>
> - kebijakan bucket Amazon S3 yang salah
> - kebijakan topik Amazon SNS yang salah
> - ketidakmampuan untuk mengirimkan ke grup CloudWatch log Log
> - izin yang tidak memadai untuk mengenkripsi menggunakan kunci KMS
>
> Akun anggota dengan CloudTrail izin dapat melihat kegagalan validasi untuk jejak organisasi dengan melihat halaman detail jejak di CloudTrail konsol, atau dengan menjalankan perintah. AWS CLI get-trail-status

Menerapkan jejak yang ada ke organisasi

Untuk mengubah jejak yang ada sehingga juga berlaku untuk organisasi, bukan satu AWS akun, tambahkan `--is-organization-trail` opsi, seperti yang ditunjukkan pada contoh berikut.

> **Note**
>
> Gunakan akun manajemen untuk mengubah jejak non-organisasi yang ada menjadi jejak organisasi.

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

Untuk mengonfirmasi bahwa jejak sekarang berlaku untuk organisasi, `IsOrganizationTrail` parameter dalam output memiliki nilai`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Pada contoh sebelumnya, jejak dikonfigurasi sebagai jejak Multi-wilayah (). `"IsMultiRegionTrail": true` Jejak yang diterapkan hanya pada satu Wilayah akan ditampilkan `"IsMultiRegionTrail": false` dalam output.

Mengonversi jejak organisasi Single-region menjadi jejak organisasi Multi-wilayah

Untuk mengonversi jejak organisasi Single-region yang ada ke jejak organisasi Multi-wilayah, tambahkan `--is-multi-region-trail` opsi seperti yang ditunjukkan pada contoh berikut.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak sekarang adalah Multi-region, periksa apakah `IsMultiRegionTrail` parameter dalam output memiliki nilai. `true`

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
```

```
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Memecahkan masalah dengan jejak organisasi

Bagian ini memberikan informasi tentang cara memecahkan masalah dengan jejak organisasi.

Topik

- CloudTrail tidak menyampaikan acara
- CloudTrail tidak mengirim notifikasi Amazon SNS untuk akun anggota di organisasi

CloudTrail tidak menyampaikan acara

Jika CloudTrail tidak mengirimkan file CloudTrail log ke bucket Amazon S3

Periksa apakah ada masalah dengan bucket S3.

- Dari CloudTrail konsol, periksa halaman detail jejak. Jika ada masalah dengan bucket S3, halaman detail menyertakan peringatan bahwa pengiriman ke bucket S3 gagal.
- Dari AWS CLI, jalankan get-trail-statusperintah. Jika terjadi kegagalan, output perintah menyertakan `LatestDeliveryError` bidang, yang menampilkan kesalahan Amazon S3 apa pun yang terjadi saat CloudTrail mencoba mengirimkan file log ke bucket yang ditentukan. Kesalahan ini hanya terjadi ketika ada masalah dengan bucket S3 tujuan, dan tidak terjadi untuk permintaan waktu yang habis. Untuk mengatasi masalah ini, perbaiki kebijakan bucket sehingga CloudTrail dapat menulis ke bucket; atau buat bucket baru, lalu panggil `update-trail` untuk menentukan bucket baru. Untuk informasi tentang kebijakan bucket organisasi, lihat Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi.

> **Note**
>
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan

peristiwa yang dicoba dikirim ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Jika CloudTrail tidak mengirimkan log ke CloudWatch Log

Periksa apakah ada masalah dengan konfigurasi kebijakan peran CloudWatch Log.

- Dari CloudTrail konsol, periksa halaman detail jejak. Jika ada masalah dengan CloudWatch Log, halaman detail menyertakan peringatan yang menunjukkan pengiriman CloudWatch Log gagal.
- Dari AWS CLI, jalankan get-trail-statusperintah. Jika terjadi kegagalan, output perintah menyertakan `LatestCloudWatchLogsDeliveryError` bidang, yang menampilkan kesalahan CloudWatch Log apa pun yang CloudTrail ditemui saat mencoba mengirimkan CloudWatch log ke Log. Untuk mengatasi masalah ini, perbaiki kebijakan peran CloudWatch Log. Untuk informasi tentang kebijakan peran CloudWatch Log, lihatDokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

Jika Anda tidak melihat aktivitas untuk akun anggota di jejak organisasi

Jika Anda tidak melihat aktivitas untuk akun anggota di jejak organisasi, periksa hal berikut:

- Periksa Wilayah asal untuk mengetahui apakah itu adalah Wilayah keikutsertaan

  Meskipun sebagian besar Wilayah AWS diaktifkan secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual (juga disebut sebagai Wilayah keikutsertaan). Untuk informasi tentang Wilayah mana yang diaktifkan secara default, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi.AWS Account Management Untuk daftar CloudTrail dukungan Wilayah, lihatCloudTrail Daerah yang didukung.

  Jika jejak organisasi adalah Multi-wilayah dan Wilayah asal adalah Wilayah keikutsertaan, akun anggota tidak akan mengirim aktivitas ke jejak organisasi kecuali mereka memilih Wilayah AWS tempat jejak Multi-wilayah dibuat. Misalnya, jika Anda membuat jejak Multi-wilayah dan memilih Wilayah Eropa (Spanyol) sebagai Wilayah asal untuk jejak tersebut, hanya akun anggota yang mengaktifkan Wilayah Eropa (Spanyol) untuk akun mereka yang akan mengirimkan aktivitas akun mereka ke jejak organisasi. Untuk mengatasi masalah ini, aktifkan Wilayah keikutsertaan di setiap akun anggota di organisasi Anda. Untuk informasi tentang mengaktifkan Wilayah keikutsertaan, lihat Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda di Panduan AWS Account Management Referensi.

- Periksa apakah kebijakan berbasis sumber daya organisasi bertentangan dengan kebijakan peran terkait layanan CloudTrail

  CloudTrail menggunakan peran terkait layanan yang diberi nama `AWSServiceRoleForCloudTrail`untuk mendukung jejak organisasi. Peran terkait layanan ini memungkinkan CloudTrail untuk melakukan tindakan pada sumber daya organisasi, seperti. `organizations:DescribeOrganization` Jika kebijakan berbasis sumber daya organisasi menolak tindakan yang diizinkan dalam kebijakan peran terkait layanan, tidak CloudTrail akan dapat melakukan tindakan meskipun diizinkan dalam kebijakan peran terkait layanan. Untuk mengatasi masalah ini, perbaiki kebijakan berbasis sumber daya organisasi agar tidak menolak tindakan yang diizinkan dalam kebijakan peran terkait layanan.

CloudTrail tidak mengirim notifikasi Amazon SNS untuk akun anggota di organisasi

Ketika akun anggota dengan jejak AWS Organizations organisasi tidak mengirimkan notifikasi Amazon SNS, mungkin ada masalah dengan konfigurasi kebijakan topik SNS. CloudTrail membuat jejak organisasi di akun anggota meskipun validasi sumber daya gagal, misalnya, topik SNS jejak organisasi tidak menyertakan semua ID akun anggota. Jika kebijakan topik SNS salah, kegagalan otorisasi terjadi.

Untuk memeriksa apakah kebijakan topik SNS jejak mengalami kegagalan otorisasi:

- Dari CloudTrail konsol, periksa halaman detail jejak. Jika ada kegagalan otorisasi, halaman detail menyertakan peringatan `SNS authorization failed` dan menunjukkan untuk memperbaiki kebijakan topik SNS.
- Dari AWS CLI, jalankan get-trail-statusperintah. Jika ada kegagalan otorisasi, output perintah menyertakan `LastNotificationError` bidang dengan nilai. `AuthorizationError` Untuk mengatasi masalah ini, perbaiki kebijakan topik Amazon SNS. Untuk informasi tentang kebijakan topik Amazon SNS, lihat. Kebijakan topik Amazon SNS untuk CloudTrail

Untuk informasi selengkapnya tentang topik SNS dan berlangganannya, lihat Memulai Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Memahami jalur Multi-wilayah dan Wilayah keikutsertaan

Jejak dapat diterapkan ke semua Wilayah AWS yang diaktifkan di Anda Akun AWS, atau dapat diterapkan ke satu Wilayah. Jejak yang berlaku untuk semua Wilayah AWS yang diaktifkan di Anda

Akun AWS disebut sebagai jalur Multi-wilayah. Sebagai praktik terbaik, kami merekomendasikan untuk membuat jejak Multi-wilayah karena dapat menangkap aktivitas di semua Wilayah yang diaktifkan. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah. Anda hanya dapat membuat jejak wilayah Tunggal menggunakan operasi AWS CLI atau `CreateTrail`API.

Meskipun sebagian besar Wilayah AWS diaktifkan secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual (juga disebut sebagai Wilayah keikutsertaan). Untuk informasi tentang Wilayah mana yang diaktifkan secara default, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi.AWS Account Management Untuk daftar CloudTrail dukungan Wilayah, lihatCloudTrail Daerah yang didukung.

Topik

- Apa keuntungan dari jalur Multi-wilayah?
- Apa yang terjadi ketika Anda membuat jejak Multi-wilayah?
- Apa yang terjadi jika Anda mengaktifkan Region keikutsertaan?
- Apa yang terjadi jika Anda menonaktifkan Wilayah keikutsertaan?

Apa keuntungan dari jalur Multi-wilayah?

Jejak multi-wilayah memiliki keuntungan sebagai berikut:

- Pengaturan konfigurasi untuk jejak berlaku secara konsisten di semua yang diaktifkan Wilayah AWS.
- Anda menerima CloudTrail peristiwa dari semua yang diaktifkan Wilayah AWS dalam satu bucket Amazon S3 dan, secara opsional, dalam grup CloudWatch log Log.
- Anda mengelola konfigurasi jejak untuk semua yang diaktifkan Wilayah AWS dari satu lokasi.

Apa yang terjadi ketika Anda membuat jejak Multi-wilayah?

Membuat jejak Multi-region, memiliki efek sebagai berikut:

- CloudTrail mengirimkan file log untuk aktivitas akun dari semua yang diaktifkan Wilayah AWS ke bucket Amazon S3 tunggal yang Anda tentukan, dan, secara opsional, ke CloudWatch grup log Log.

- Jika Anda mengonfigurasi topik Amazon SNS untuk jejak, pemberitahuan SNS tentang pengiriman file log di semua yang diaktifkan Wilayah AWS akan dikirim ke topik SNS tunggal tersebut.
- Anda dapat melihat jejak Multi-wilayah di semua diaktifkan Wilayah AWS, tetapi Anda hanya dapat memodifikasi jejak di Wilayah asal tempat ia dibuat.

Apa yang terjadi jika Anda mengaktifkan Region keikutsertaan?

Setelah Anda mengaktifkan Wilayah keikutsertaan, CloudTrail buat salinan identik dari setiap jejak Multi-wilayah di Wilayah keikutsertaan yang Anda aktifkan.

CloudTrail menggunakan model komputasi terdistribusi yang disebut konsistensi akhirnya. Karena mengaktifkan Wilayah membutuhkan waktu beberapa menit hingga beberapa jam, Anda mungkin tidak segera melihat semua peristiwa di log untuk Wilayah yang baru diaktifkan. Mungkin diperlukan waktu hingga beberapa jam CloudTrail untuk mengirimkan semua log untuk Wilayah yang baru diaktifkan. Selama waktu ini, Anda dapat melihat 90 hari terakhir peristiwa manajemen yang dicatat di Wilayah tersebut dengan melihat Riwayat CloudTrail Peristiwa, atau dengan menjalankan aws cloudtrail lookup-events --region <region>perintah. Riwayat peristiwa aktif secara default di Anda Akun AWS, menangkap 90 hari terakhir peristiwa manajemen yang dicatat di Wilayah, dan tidak memerlukan jejak.

Untuk informasi tentang mengaktifkan Wilayah keikutsertaan untuk Anda Akun AWS, lihat Mengaktifkan atau menonaktifkan Wilayah untuk akun mandiri atau Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda.

Apa yang terjadi jika Anda menonaktifkan Wilayah keikutsertaan?

Karena akun Anda mungkin memiliki aktivitas di Wilayah yang Anda nonaktifkan, seperti tindakan Layanan AWS untuk menghapus sumber daya, CloudTrail akan terus menangkap aktivitas dan mencoba mengirimkan peristiwa ke bucket S3 untuk setiap jejak yang tidak dihapus sebelum Wilayah dinonaktifkan.

Menyalin acara jejak ke Danau CloudTrail

Anda dapat menyalin peristiwa jejak yang ada ke penyimpanan data acara CloudTrail Lake untuk membuat point-in-time snapshot peristiwa yang dicatat ke jejak. Menyalin peristiwa jejak tidak mengganggu kemampuan jejak untuk mencatat peristiwa dan tidak mengubah jejak dengan cara apa pun.

Anda dapat menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada yang dikonfigurasi untuk CloudTrail acara, atau Anda dapat membuat penyimpanan data CloudTrail acara baru dan memilih opsi Salin peristiwa jejak sebagai bagian dari pembuatan penyimpanan data acara. Untuk informasi selengkapnya tentang menyalin peristiwa jejak ke penyimpanan data acara yang ada, lihatSalin peristiwa jejak ke penyimpanan data acara yang ada menggunakan CloudTrail konsol. Untuk informasi selengkapnya tentang membuat penyimpanan data acara baru, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

Menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake, memungkinkan Anda menjalankan kueri pada peristiwa yang disalin. CloudTrail Kueri danau menawarkan tampilan acara yang lebih dalam dan lebih dapat disesuaikan daripada pencarian kunci dan nilai sederhana dalam riwayat Acara, atau berjalan. `LookupEvents` Untuk informasi lebih lanjut tentang CloudTrail Danau, lihatBekerja dengan AWS CloudTrail Danau.

Jika Anda menyalin peristiwa jejak ke penyimpanan data acara organisasi, Anda harus menggunakan akun manajemen untuk organisasi. Anda tidak dapat menyalin peristiwa jejak menggunakan akun administrator yang didelegasikan untuk organisasi.

CloudTrail Penyimpanan data acara danau dikenakan biaya. Saat Anda membuat penyimpanan data acara, Anda memilih opsi harga yang ingin Anda gunakan untuk penyimpanan data acara. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Untuk informasi tentang CloudTrail penetapan harga dan pengelolaan biaya Lake, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

Saat Anda menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data tidak terkompresi yang dikonsumsi oleh penyimpanan data acara.

Saat Anda menyalin peristiwa jejak ke CloudTrail Lake, CloudTrail buka ritsleting log yang disimpan dalam format gzip (terkompresi) dan kemudian menyalin peristiwa yang terdapat dalam log ke penyimpanan data acara Anda. Ukuran data yang tidak terkompresi bisa lebih besar dari ukuran penyimpanan S3 yang sebenarnya. Untuk mendapatkan perkiraan umum ukuran data yang tidak terkompresi, Anda dapat mengalikan ukuran log di bucket S3 dengan 10.

Anda dapat mengurangi biaya dengan menentukan rentang waktu yang lebih sempit untuk acara yang disalin. Jika Anda berencana untuk hanya menggunakan penyimpanan data acara untuk menanyakan peristiwa yang disalin, Anda dapat menonaktifkan konsumsi acara untuk menghindari timbulnya biaya pada peristiwa masa depan. Untuk informasi lebih lanjut, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

Skenario

Tabel berikut menjelaskan beberapa skenario umum untuk menyalin peristiwa jejak dan bagaimana Anda menyelesaikan setiap skenario menggunakan konsol.

Skenario	Bagaimana cara melakukannya di konsol?
Menganalisis dan menanyakan peristiwa jejak sejarah di CloudTrail Danau tanpa menelan peristiwa baru	Buat penyimpanan data acara baru dan pilih opsi Salin peristiwa jejak sebagai bagian dari pembuatan penyimpanan data acara. Saat membuat penyimpanan data acara, batalkan pilihan acara Ingest (langkah 15 dari prosedur) untuk memastikan penyimpanan data acara hanya berisi peristiwa historis untuk jejak Anda dan tidak ada peristiwa masa depan.
Ganti jejak Anda yang ada dengan penyimpanan data acara CloudTrail Lake	Buat penyimpanan data acara dengan pemilih acara yang sama dengan jejak Anda untuk memastikan bahwa penyimpanan data acara memiliki cakupan yang sama dengan jejak Anda. Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang tanggal untuk peristiwa yang disalin yang lebih awal dari pembuatan penyimpanan data peristiwa. Setelah penyimpanan data acara Anda dibuat, Anda dapat mematikan pencatatan untuk jejak untuk menghindari biaya tambahan.

Topik

- Pertimbangan untuk menyalin acara jejak
- Izin yang diperlukan untuk menyalin peristiwa jejak
- Salin peristiwa jejak ke penyimpanan data acara yang ada menggunakan CloudTrail konsol

Pertimbangan untuk menyalin acara jejak

Pertimbangkan faktor-faktor berikut saat menyalin peristiwa jejak.

- Saat menyalin peristiwa jejak, CloudTrail gunakan operasi S3 `GetObject`API untuk mengambil peristiwa jejak di bucket S3 sumber. Ada beberapa kelas penyimpanan yang diarsipkan S3, seperti S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, S3 Outposts, dan S3 Intelligent-Tiering Deep Archive tingkatan yang tidak dapat diakses dengan menggunakan. `GetObject` Untuk menyalin peristiwa jejak yang disimpan di kelas penyimpanan yang diarsipkan ini, Anda harus terlebih dahulu memulihkan salinan menggunakan operasi S3`RestoreObject`. Untuk informasi tentang memulihkan objek yang diarsipkan, lihat Memulihkan Objek yang Diarsipkan di Panduan Pengguna Amazon S3.
- Saat Anda menyalin peristiwa jejak ke penyimpanan data peristiwa, CloudTrail menyalin semua peristiwa jejak terlepas dari konfigurasi jenis acara penyimpanan data acara tujuan, pemilih acara lanjutan, atau Wilayah AWS.
- Sebelum menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada, pastikan opsi harga dan periode retensi penyimpanan data acara dikonfigurasi dengan tepat untuk kasus penggunaan Anda.
  - Opsi harga: Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan acara. Untuk informasi selengkapnya tentang opsi harga, lihat AWS CloudTrail Harga danOpsi harga toko data acara.
  - Periode retensi: Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Untuk menentukan periode retensi yang sesuai, ambil jumlah acara tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.
- Jika Anda menyalin peristiwa jejak ke penyimpanan data acara untuk diselidiki dan tidak ingin menelan peristiwa masa depan, Anda dapat menghentikan konsumsi di penyimpanan data acara. Saat membuat penyimpanan data acara, batalkan pilihan opsi Ingest event (langkah 15 dari prosedur) untuk memastikan penyimpanan data acara hanya berisi peristiwa historis untuk jejak Anda dan tidak ada peristiwa masa depan.
- Sebelum menyalin peristiwa jejak, nonaktifkan daftar kontrol akses (ACLs) yang dilampirkan ke bucket S3 sumber, dan perbarui kebijakan bucket S3 untuk penyimpanan data peristiwa tujuan. Untuk informasi selengkapnya tentang memperbarui kebijakan bucket S3, lihatKebijakan bucket Amazon S3 untuk menyalin peristiwa jejak. Untuk informasi selengkapnya tentang penonaktifan ACLs, lihat Mengontrol kepemilikan objek dan menonaktifkan bucket ACLs Anda.

- CloudTrail hanya menyalin peristiwa jejak dari file log terkompresi Gzip yang ada di bucket S3 sumber. CloudTrail tidak menyalin peristiwa jejak dari file log yang tidak terkompresi, atau file log yang dikompresi menggunakan format selain Gzip.
- Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang waktu untuk peristiwa yang disalin yang lebih awal dari pembuatan penyimpanan data peristiwa.
- Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam awalan bucket S3 dan `CloudTrail` awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, Anda harus memilih awalan saat menyalin peristiwa jejak.
- Untuk menyalin peristiwa jejak ke penyimpanan data acara organisasi, Anda harus menggunakan akun manajemen untuk organisasi. Anda tidak dapat menggunakan akun administrator yang didelegasikan untuk menyalin peristiwa jejak ke penyimpanan data acara organisasi.

Izin yang diperlukan untuk menyalin peristiwa jejak

Sebelum menyalin peristiwa jejak, pastikan Anda memiliki semua izin yang diperlukan untuk peran IAM Anda. Anda hanya perlu memperbarui izin peran IAM jika memilih peran IAM yang ada untuk menyalin peristiwa jejak. Jika Anda memilih untuk membuat peran IAM baru, CloudTrail berikan semua izin yang diperlukan untuk peran tersebut.

Jika bucket S3 sumber menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Jika bucket S3 sumber menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci agar memungkinkan CloudTrail untuk mendekripsi data dalam bucket.

Topik

- Izin IAM untuk menyalin peristiwa jejak
- Kebijakan bucket Amazon S3 untuk menyalin peristiwa jejak
- Kebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber

Izin IAM untuk menyalin peristiwa jejak

Saat menyalin peristiwa jejak, Anda memiliki opsi untuk membuat peran IAM baru, atau menggunakan peran IAM yang ada. Saat Anda memilih peran IAM baru, CloudTrail buat peran IAM dengan izin yang diperlukan dan tidak ada tindakan lebih lanjut yang diperlukan di pihak Anda.

Jika Anda memilih peran yang ada, pastikan kebijakan peran IAM memungkinkan CloudTrail untuk menyalin peristiwa jejak dari bucket S3 sumber. Bagian ini memberikan contoh izin peran IAM dan kebijakan kepercayaan yang diperlukan.

Contoh berikut menyediakan kebijakan izin, yang memungkinkan CloudTrail untuk menyalin peristiwa jejak dari bucket S3 sumber. Ganti *amzn-s3-demo-bucketmyAccountID*,*region*,*prefix*,, dan *eventDataStoreId* dengan nilai yang sesuai untuk konfigurasi Anda. *myAccountID*Ini adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

Ganti *key-regionkeyAccountID*,, dan *keyID* dengan nilai untuk kunci KMS yang digunakan untuk mengenkripsi bucket S3 sumber. Anda dapat menghilangkan `AWSCloudTrailImportKeyAccess` pernyataan jika bucket S3 sumber tidak menggunakan kunci KMS untuk enkripsi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
      ],
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

Contoh berikut memberikan kebijakan kepercayaan IAM, yang memungkinkan CloudTrail untuk mengambil peran IAM untuk menyalin peristiwa jejak dari bucket S3 sumber. Ganti *myAccountIDregion*,, dan *eventDataStoreArn* dengan nilai yang sesuai untuk konfigurasi Anda. *myAccountID*Ini adalah Akun AWS ID yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
        }
      }
    }
  ]
}
```

Kebijakan bucket Amazon S3 untuk menyalin peristiwa jejak

Secara default, ember dan objek Amazon S3 bersifat pribadi. Hanya pemilik sumber daya (AWS akun yang membuat bucket) yang dapat mengakses bucket dan objek yang dikandungnya. Pemilik sumber daya dapat memberikan izin akses ke sumber daya dan pengguna lain dengan menulis kebijakan akses.

Sebelum menyalin peristiwa jejak, Anda harus memperbarui kebijakan bucket S3 CloudTrail agar dapat menyalin peristiwa jejak dari bucket S3 sumber.

Anda dapat menambahkan pernyataan berikut ke kebijakan bucket S3 untuk memberikan izin ini. Ganti *roleArn* dan *amzn-s3-demo-bucket* dengan nilai yang sesuai untuk konfigurasi Anda.

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

Kebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber

Jika bucket S3 sumber menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS menyediakan `kms:Decrypt` dan `kms:GenerateDataKey` izin yang diperlukan untuk menyalin peristiwa jejak dari bucket S3 CloudTrail dengan enkripsi SSE-KMS diaktifkan. Jika bucket S3 sumber Anda menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci.

Memperbarui kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data di bucket S3 sumber, menjalankan pemeriksaan validasi untuk memastikan bahwa peristiwa sesuai dengan CloudTrail standar, dan menyalin peristiwa ke penyimpanan data peristiwa Lake. CloudTrail

Contoh berikut menyediakan kebijakan kunci KMS, yang memungkinkan CloudTrail untuk mendekripsi data dalam bucket S3 sumber. Ganti *roleArnamzn-s3-demo-bucket*,*myAccountID*,*region*,, dan *eventDataStoreId* dengan nilai yang sesuai untuk konfigurasi Anda. *myAccountID*Ini adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
  }
}
```

Salin peristiwa jejak ke penyimpanan data acara yang ada menggunakan CloudTrail konsol

Gunakan prosedur berikut untuk menyalin peristiwa jejak ke penyimpanan data acara yang ada. Untuk informasi tentang cara membuat penyimpanan data acara baru, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

> **Note**
>
> Sebelum menyalin peristiwa jejak ke penyimpanan data peristiwa yang ada, pastikan opsi harga dan periode retensi penyimpanan data acara dikonfigurasi dengan tepat untuk kasus penggunaan Anda.
>
> - Opsi harga: Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan acara. Untuk informasi selengkapnya tentang opsi harga, lihat AWS CloudTrail Harga danOpsi harga toko data acara.
> - Periode retensi: Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Untuk menentukan periode retensi yang sesuai, ambil jumlah acara tertua yang ingin Anda salin dalam beberapa hari dan jumlah hari yang ingin Anda simpan di penyimpanan data acara (periode retensi = *`oldest-event-in-days`* +*`number-days-to-retain`*). Misalnya, jika acara tertua yang Anda salin berusia 45 hari dan Anda ingin menyimpan acara di penyimpanan data acara selama 45 hari lagi, Anda akan mengatur periode retensi menjadi 90 hari.

Untuk menyalin peristiwa jejak ke penyimpanan data acara

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pilih Jalur di panel navigasi kiri konsol. CloudTrail
3. Pada halaman Trails, pilih jejak, lalu pilih Salin acara ke Danau. Jika bucket S3 sumber untuk jejak menggunakan kunci KMS untuk enkripsi data, pastikan kebijakan kunci KMS memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Jika bucket S3 sumber menggunakan beberapa kunci KMS, Anda harus memperbarui kebijakan setiap kunci agar memungkinkan CloudTrail untuk mendekripsi data dalam bucket. Untuk informasi selengkapnya tentang memperbarui kebijakan kunci KMS, lihatKebijakan kunci KMS untuk mendekripsi data di bucket S3 sumber.
4. (Opsional) Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam `CloudTrail` awalan bucket S3 dan awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, pilih Masukkan URI S3, lalu pilih Browse S3 untuk menelusuri awalan.

Kebijakan bucket S3 harus memberikan CloudTrail akses untuk menyalin peristiwa jejak. Untuk informasi selengkapnya tentang memperbarui kebijakan bucket S3, lihatKebijakan bucket Amazon S3 untuk menyalin peristiwa jejak.

5. Untuk Tentukan rentang waktu acara, pilih rentang waktu untuk menyalin acara. CloudTrail memeriksa awalan dan nama file log untuk memverifikasi nama berisi tanggal antara tanggal mulai dan akhir yang dipilih sebelum mencoba menyalin peristiwa jejak. Anda dapat memilih rentang Relatif atau rentang Absolut. Untuk menghindari duplikasi peristiwa antara jejak sumber dan penyimpanan data peristiwa tujuan, pilih rentang waktu yang lebih awal dari pembuatan penyimpanan data acara.

> **Note**
>
> CloudTrail hanya menyalin peristiwa jejak yang `eventTime` memiliki periode retensi penyimpanan data acara. Misalnya, jika periode penyimpanan data acara adalah 90 hari, maka tidak CloudTrail akan menyalin peristiwa jejak apa pun dengan `eventTime` lebih dari 90 hari.

   - Jika Anda memilih Rentang relatif, Anda dapat memilih untuk menyalin peristiwa yang dicatat dalam 6 bulan terakhir, 1 tahun, 2 tahun, 7 tahun, atau rentang khusus. CloudTrail menyalin peristiwa yang dicatat dalam periode waktu yang dipilih.
   - Jika Anda memilih Rentang absolut, Anda dapat memilih tanggal mulai dan berakhir tertentu. CloudTrail menyalin peristiwa yang terjadi antara tanggal mulai dan akhir yang dipilih.
6. Untuk lokasi Pengiriman, pilih penyimpanan data acara tujuan dari daftar drop-down.
7. Untuk Izin, pilih dari opsi peran IAM berikut. Jika Anda memilih peran IAM yang ada, verifikasi bahwa kebijakan peran IAM menyediakan izin yang diperlukan. Untuk informasi selengkapnya tentang memperbarui izin peran IAM, lihat. Izin IAM untuk menyalin peristiwa jejak

   - Pilih Buat peran baru (disarankan) untuk membuat peran IAM baru. Untuk Masukkan nama peran IAM, masukkan nama untuk peran tersebut. CloudTrail secara otomatis membuat izin yang diperlukan untuk peran baru ini.
   - Pilih Gunakan ARN peran IAM kustom untuk menggunakan peran IAM kustom yang tidak terdaftar. Untuk Masukkan peran IAM ARN, masukkan ARN IAM.
   - Pilih peran IAM yang ada dari daftar drop-down.
8. Pilih Salin acara.

9. Anda diminta untuk mengonfirmasi salinannya. Saat Anda siap untuk mengonfirmasi, pilih Salin acara jejak ke Danau, lalu pilih Salin acara.
10. Pada halaman Salin detail, Anda dapat melihat status salinan dan meninjau kegagalan apa pun. Ketika salinan peristiwa jejak selesai, status Salinannya disetel ke Selesai jika tidak ada kesalahan, atau Gagal jika terjadi kesalahan.

> **Note**
>
> Detail yang ditampilkan di halaman detail salinan acara tidak dalam waktu nyata. Nilai sebenarnya untuk detail seperti Awalan yang disalin mungkin lebih tinggi dari yang ditampilkan di halaman. CloudTrail memperbarui detail secara bertahap selama salinan acara.

11. Jika status Salin Gagal, perbaiki kesalahan yang ditampilkan dalam kegagalan Salin, lalu pilih Coba lagi salin. Ketika Anda mencoba kembali salinan, CloudTrail lanjutkan salinan di lokasi di mana kegagalan terjadi.

Untuk informasi selengkapnya tentang melihat detail salinan acara jejak, lihatLihat detail salinan acara dengan CloudTrail konsol.

Mendapatkan dan melihat file CloudTrail log Anda

Setelah Anda membuat jejak dan mengonfigurasinya untuk menangkap file log yang Anda inginkan, Anda harus dapat menemukan file log dan menafsirkan informasi yang dikandungnya.

CloudTrail mengirimkan file log Anda ke bucket Amazon S3 yang Anda tentukan saat membuat jejak. CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian Tingkat AWS CloudTrail Layanan untuk informasi lebih lanjut. Acara wawasan biasanya dikirimkan ke ember Anda dalam waktu 30 menit setelah aktivitas yang tidak biasa. Setelah mengaktifkan peristiwa Insights untuk pertama kalinya, biarkan hingga 36 jam untuk melihat peristiwa Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

> **Note**
>
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari,

dan attempted-to-deliver peristiwa ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Topik

- Menemukan file CloudTrail log Anda
- Mengunduh file CloudTrail log Anda

Menemukan file CloudTrail log Anda

CloudTrail menerbitkan file log ke bucket S3 Anda dalam arsip gzip. Di bucket S3, file log memiliki nama yang diformat yang mencakup elemen-elemen berikut:

- Nama bucket yang Anda tentukan saat membuat jejak (ditemukan di halaman Trails CloudTrail konsol)
- Awalan (opsional) yang Anda tentukan saat membuat jejak
- String "AWSLogs”
- Nomor rekening
- String "CloudTrail" untuk data, acara manajemen
- String "CloudTrail-Insight” untuk acara wawasan
- String "CloudTrail-NetworkActivity" untuk acara aktivitas jaringan
- String "CloudTrail-Aggregated” untuk peristiwa agregat untuk peristiwa data
- Pengidentifikasi wilayah seperti us-west-1
- Tahun file log diterbitkan dalam YYYY format
- Bulan file log diterbitkan dalam MM format
- Hari file log diterbitkan dalam DD format
- String alfanumerik yang membedakan file dari orang lain yang mencakup periode waktu yang sama

Contoh berikut menunjukkan nama objek file log lengkap untuk data, acara manajemen:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

Contoh berikut menunjukkan nama objek file log lengkap untuk peristiwa wawasan:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
Insight/region/YYYY/MM/DD/file_name.json.gz
```

Contoh berikut menunjukkan nama objek file log lengkap untuk peristiwa aktivitas jaringan:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
NetworkActivity/region/YYYY/MM/DD/file_name.json.gz
```

Contoh berikut menunjukkan nama objek file log lengkap untuk agregasi peristiwa data:

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
Aggregated/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> Untuk jejak organisasi, nama objek file log di bucket S3 menyertakan ID unit organisasi di jalur, sebagai berikut:
>
> ```
> amzn-s3-demo-bucket/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

Untuk mengambil file log, Anda dapat menggunakan konsol Amazon S3, antarmuka baris perintah Amazon S3 (CLI), atau API.

Untuk menemukan file log Anda dengan konsol Amazon S3

1. Buka konsol Amazon S3.
2. Pilih ember yang Anda tentukan.
3. Arahkan melalui hierarki objek hingga Anda menemukan file log yang Anda inginkan.

   Semua file log memiliki ekstensi.gz.

Anda akan menavigasi hierarki objek yang mirip dengan contoh berikut, tetapi dengan nama bucket, ID akun, Wilayah, dan tanggal yang berbeda.

```
All Buckets
    amzn-s3-demo-bucket
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

File log untuk hierarki objek sebelumnya akan terlihat seperti berikut:

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> Meskipun jarang, Anda mungkin menerima file log yang berisi satu atau lebih peristiwa duplikat. Dalam kebanyakan kasus, peristiwa duplikat akan memiliki hal yang sama`eventID`. Untuk informasi lebih lanjut tentang `eventID` bidang ini, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

Mengunduh file CloudTrail log Anda

File log dalam format JSON. Jika Anda memiliki add-on penampil JSON yang diinstal, Anda dapat melihat file langsung di browser Anda. Klik dua kali nama file log di bucket untuk membuka jendela atau tab browser baru. JSON ditampilkan dalam format yang dapat dibaca.

CloudTrail file log adalah objek Amazon S3. Anda dapat menggunakan konsol Amazon S3, (AWS Command Line Interface CLI), atau Amazon S3 API untuk mengambil file log.

Untuk informasi selengkapnya, lihat ikhtisar objek Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Prosedur berikut menjelaskan cara mengunduh file log dengan file Konsol Manajemen AWS.

Untuk mengunduh dan membaca file log

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih bucket dan pilih file log yang ingin Anda unduh.
3. Pilih Unduh atau Unduh sebagai dan ikuti petunjuk untuk menyimpan file. Ini menyimpan file dalam format terkompresi.

   > **Note**
   >
   > Beberapa browser, seperti Chrome, secara otomatis mengekstrak file log untuk Anda. Jika browser Anda melakukan ini untuk Anda, lewati ke langkah 5.

4. Gunakan produk seperti 7-Zip untuk mengekstrak file log.
5. Buka file log di editor teks seperti Notepad ++.

Untuk informasi selengkapnya tentang bidang peristiwa yang dapat muncul di entri file log, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

AWS bermitra dengan spesialis pihak ketiga dalam pencatatan dan analisis untuk memberikan solusi yang menggunakan CloudTrail output. Untuk informasi selengkapnya, lihat AWS CloudTrail mitra.

> **Note**
>
> Anda juga dapat menggunakan fitur Riwayat peristiwa untuk mencari peristiwa untuk membuat, memperbarui, dan menghapus aktivitas API selama 90 hari terakhir. Lihat informasi yang lebih lengkap di Bekerja dengan riwayat CloudTrail acara.

Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail

Anda dapat diberi tahu saat CloudTrail menerbitkan file log baru ke bucket Amazon S3 Anda. Anda mengelola notifikasi menggunakan Amazon Simple Notification Service (Amazon SNS).

Pemberitahuan bersifat opsional. Jika Anda menginginkan notifikasi, Anda CloudTrail mengonfigurasi untuk mengirim informasi pembaruan ke topik Amazon SNS setiap kali file log baru dikirim. Untuk menerima pemberitahuan ini, Anda dapat menggunakan Amazon SNS untuk berlangganan topik. Sebagai pelanggan, Anda bisa mendapatkan pembaruan yang dikirim ke antrian Amazon

Simple Queue Service (Amazon SQS), yang memungkinkan Anda menangani notifikasi ini secara terprogram.

Topik

- Mengkonfigurasi CloudTrail untuk mengirim notifikasi

Mengkonfigurasi CloudTrail untuk mengirim notifikasi

Di CloudTrail konsol, Anda dapat mengonfigurasi jejak untuk menggunakan topik Amazon SNS dengan mengaktifkan opsi pengiriman notifikasi SNS saat membuat atau memperbarui jejak. Jika Anda memilih untuk menggunakan topik baru, CloudTrail buat topik Amazon SNS untuk Anda dan lampirkan kebijakan yang sesuai, sehingga CloudTrail memiliki izin untuk mempublikasikan topik tersebut.

Dengan itu AWS CLI, Anda dapat membuat atau memperbarui jejak untuk menggunakan topik Amazon SNS dengan menentukan nilai untuk parameter. `--sns-topic-name` Anda dapat menentukan nama atau ARN untuk topik Amazon SNS.

Saat Anda membuat nama topik SNS, nama harus memenuhi persyaratan berikut:

- Antara 1 hingga 256 karakter
- Memuat huruf besar dan huruf kecil ASCII, angka, garis bawah, atau tanda hubung

Saat Anda mengonfigurasi notifikasi untuk jejak Multi-wilayah, notifikasi dari semua Wilayah akan dikirim ke topik Amazon SNS yang Anda tentukan. Jika Anda memiliki satu atau lebih jalur khusus Wilayah, Anda harus membuat topik terpisah untuk setiap Wilayah dan berlangganan masing-masing secara individual.

Untuk menerima notifikasi, berlangganan topik Amazon SNS atau topik yang CloudTrail digunakan. Anda melakukan ini dengan konsol Amazon SNS atau perintah Amazon SNS CLI. Untuk informasi selengkapnya, lihat Berlangganan topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> CloudTrail mengirimkan pemberitahuan saat file log ditulis ke bucket Amazon S3. Akun aktif dapat menghasilkan sejumlah besar notifikasi. Jika Anda berlangganan email atau SMS, Anda dapat menerima sejumlah besar pesan. Kami menyarankan Anda berlangganan

menggunakan Amazon Simple Queue Service (Amazon SQS), yang memungkinkan Anda menangani notifikasi secara terprogram. Untuk informasi selengkapnya, lihat Berlangganan antrean Amazon SQS untuk topik Amazon SNS (konsol) di Panduan Developer Amazon Simple Queue Service.

Notifikasi Amazon SNS terdiri dari objek JSON yang menyertakan bidang. `Message` `Message`Bidang ini mencantumkan path lengkap ke file log, seperti yang ditunjukkan pada contoh berikut:

```
{
    "s3Bucket": "amzn-s3-demo-bucket","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Jika beberapa file log dikirimkan ke bucket Amazon S3 Anda, notifikasi mungkin berisi beberapa log, seperti yang ditunjukkan pada contoh berikut:

```
{
    "s3Bucket": "amzn-s3-demo-bucket",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

Jika Anda memilih untuk menerima pemberitahuan melalui email, isi email terdiri dari konten `Message` bidang. Untuk informasi tentang struktur JSON, lihat antrian Fanout ke Amazon SQS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Hanya `Message` bidang yang menunjukkan CloudTrail informasi. Bidang lain berisi informasi dari layanan Amazon SNS.

Jika Anda membuat jejak dengan CloudTrail API, Anda dapat menentukan topik Amazon SNS yang ada yang CloudTrail ingin Anda kirimi notifikasi dengan `CreateTrail`atau `UpdateTrail`operasi.

Anda harus memastikan bahwa topik itu ada dan memiliki izin yang memungkinkan CloudTrail untuk mengirim pemberitahuan ke sana. Lihat Kebijakan topik Amazon SNS untuk CloudTrail.

Sumber daya tambahan

Untuk informasi selengkapnya tentang topik Amazon SNS dan tentang berlangganan topik tersebut, lihat Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Menggunakan AWS CloudTrail dengan antarmuka VPC endpoint

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat membuat koneksi pribadi antara VPC dan VPC. AWS CloudTrail Anda dapat menggunakan koneksi ini untuk mengaktifkan CloudTrail untuk berkomunikasi dengan sumber daya Anda di VPC Anda tanpa melalui internet publik.

Amazon VPC adalah AWS layanan yang dapat Anda gunakan untuk meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan. Dengan VPC, Anda memiliki kendali terhadap pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan pintu masuk jaringan. Dengan titik akhir VPC, perutean antara VPC dan AWS layanan ditangani oleh AWS jaringan, dan Anda dapat menggunakan kebijakan IAM untuk mengontrol akses ke sumber daya layanan.

Untuk menghubungkan VPC Anda CloudTrail, Anda menentukan titik akhir VPC antarmuka untuk. CloudTrail Endpoint antarmuka adalah elastic network interface dengan alamat IP pribadi yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan ke layanan yang didukung AWS . Endpoint menyediakan konektivitas yang andal dan dapat diskalakan CloudTrail tanpa memerlukan gateway internet, instance terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan Amazon VPC dalam Panduan Pengguna Amazon VPC.

Endpoint VPC antarmuka didukung oleh AWS PrivateLink, sebuah AWS teknologi yang memungkinkan komunikasi pribadi antara AWS layanan menggunakan antarmuka jaringan elastis dengan alamat IP pribadi. Untuk informasi selengkapnya, lihat AWS PrivateLink.

Bagian berikut adalah untuk pengguna Amazon VPC. Untuk informasi selengkapnya, lihat Memulai Amazon VPC di Panduan Pengguna Amazon VPC.

Topik

- Wilayah
- Buat titik akhir VPC untuk CloudTrail

- Membuat kebijakan titik akhir VPC untuk CloudTrail
- Subnet bersama

Wilayah

AWS CloudTrail mendukung kebijakan titik akhir VPC dan titik akhir VPC di semua yang didukung. Wilayah AWS CloudTrail

Buat titik akhir VPC untuk CloudTrail

Untuk mulai menggunakan CloudTrail dengan VPC Anda, buat antarmuka VPC endpoint untuk. CloudTrail Untuk informasi selengkapnya, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan Pengguna Amazon VPC.

Anda tidak perlu mengubah pengaturan untuk CloudTrail. CloudTrail panggilan lain Layanan AWS menggunakan titik akhir publik atau titik akhir VPC antarmuka pribadi, mana pun yang digunakan.

Membuat kebijakan titik akhir VPC untuk CloudTrail

Kebijakan titik akhir VPC adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir VPC antarmuka. Kebijakan endpoint default memberi Anda akses penuh CloudTrail APIs melalui titik akhir VPC antarmuka. Untuk mengontrol akses yang diberikan CloudTrail dari VPC Anda, lampirkan kebijakan endpoint kustom ke titik akhir VPC antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya tentang kebijakan titik akhir VPC, termasuk cara memperbarui kebijakan, lihat Mengontrol akses ke layanan dengan titik akhir VPC di Panduan Pengguna Amazon VPC.

Berikut ini adalah contoh kebijakan endpoint VPC kustom untuk. CloudTrail

Contoh kebijakan:

- Contoh: Izinkan semua CloudTrail tindakan
- Contoh: Izinkan CloudTrail tindakan tertentu
- Contoh: Tolak semua CloudTrail tindakan
- Contoh: Tolak CloudTrail tindakan tertentu
- Contoh: Izinkan semua CloudTrail tindakan dari VPC tertentu
- Contoh: Izinkan semua CloudTrail tindakan dari titik akhir VPC tertentu

Contoh: Izinkan semua CloudTrail tindakan

Contoh kebijakan titik akhir VPC berikut memberikan akses ke semua CloudTrail tindakan untuk semua prinsipal di semua sumber daya.

JSON

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

Contoh: Izinkan CloudTrail tindakan tertentu

Contoh kebijakan titik akhir VPC berikut memberikan akses untuk melakukan `cloudtrail:ListTrails` dan `cloudtrail:ListEventDataStores` tindakan untuk semua prinsipal di semua sumber daya.

JSON

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

```
    "Statement": [
        {
            "Action": ["cloudtrail:ListTrails",
 "cloudtrail:ListEventDataStores"],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Contoh: Tolak semua CloudTrail tindakan

Contoh berikut kebijakan titik akhir VPC menolak akses ke semua CloudTrail tindakan untuk semua prinsip pada semua sumber daya.

JSON

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

Contoh: Tolak CloudTrail tindakan tertentu

Contoh berikut kebijakan titik akhir VPC menyangkal `cloudtrail:CreateTrail` dan `cloudtrail:CreateEventDataStore` tindakan untuk semua prinsip pada semua sumber daya.

JSON

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

```
    "Statement": [
        {
            "Action": ["cloudtrail:CreateTrail",
 "cloudtrail:CreateEventDataStore"],
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan semua CloudTrail tindakan dari VPC tertentu

Contoh kebijakan titik akhir VPC berikut memberikan akses untuk melakukan semua CloudTrail tindakan untuk semua prinsip pada semua sumber daya tetapi hanya jika pemohon menggunakan VPC yang ditentukan untuk membuat permintaan. Ganti *vpc-id* dengan ID VPC Anda.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals": {
        "aws:SourceVpc": "vpc-1234567890abcdef0"
        }
      }
    }
  ]
}
```

Contoh: Izinkan semua CloudTrail tindakan dari titik akhir VPC tertentu

Contoh kebijakan titik akhir VPC berikut memberikan akses untuk melakukan semua CloudTrail tindakan untuk semua prinsip pada semua sumber daya tetapi hanya jika pemohon menggunakan

titik akhir VPC yang ditentukan untuk membuat permintaan. Ganti *vpc-endpoint-id* dengan ID titik akhir VPC Anda.

JSON

```
{
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": "cloudtrail:*",
         "Resource": "*",
         "Condition": {
             "StringEquals": {
                "aws:SourceVpce": "vpce-1a2b3c4d"
             }
         }
       }
    ]
  }
```

Subnet bersama

Titik akhir CloudTrail VPC, seperti titik akhir VPC lainnya, hanya dapat dibuat oleh akun pemilik di subnet bersama. Namun, akun peserta dapat menggunakan titik akhir CloudTrail VPC di subnet yang dibagikan dengan akun peserta. Untuk informasi selengkapnya tentang berbagi VPC Amazon, lihat Bagikan VPC Anda dengan akun lain di Panduan Pengguna Amazon VPC.

Persyaratan penamaan untuk CloudTrail sumber daya, bucket S3, dan kunci KMS

Bagian ini memberikan informasi tentang persyaratan penamaan untuk CloudTrail sumber daya, bucket Amazon S3, dan kunci KMS.

Topik

- CloudTrail persyaratan penamaan sumber daya
- Persyaratan penamaan ember Amazon S3

- AWS KMS persyaratan penamaan alias

CloudTrail persyaratan penamaan sumber daya

CloudTrail nama sumber daya harus memenuhi persyaratan berikut:

- Hanya berisi huruf ASCII (a-z, A-Z), angka (0-9), titik (.), garis bawah (_), atau tanda hubung (-).
- Mulailah dengan huruf atau angka, dan akhiri dengan huruf atau angka.
- Berada di antara 3 dan 128 karakter.
- Tidak memiliki titik, garis bawah, atau tanda hubung yang berdampingan. Nama seperti my-_namespace dan my-\ -namespace tidak valid.
- Tidak dalam format alamat IP (misalnya,`192.168.5.4`).

Persyaratan penamaan ember Amazon S3

Bucket Amazon S3 yang Anda gunakan untuk menyimpan file CloudTrail log harus memiliki nama yang sesuai dengan persyaratan penamaan untuk wilayah Standar non-AS. Amazon S3 mendefinisikan nama bucket sebagai serangkaian satu atau lebih label, dipisahkan oleh titik. Untuk daftar lengkap aturan penamaan, lihat Aturan penamaan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Berikut ini adalah beberapa aturan:

- Nama bucket dapat memiliki panjang antara 3 dan 63 karakter, dan hanya dapat berisi karakter huruf kecil, angka, titik, dan tanda hubung.
- Setiap label dalam nama bucket harus dimulai dengan huruf kecil atau angka.
- Nama bucket tidak dapat berisi garis bawah, diakhiri dengan tanda hubung, memiliki periode berturut-turut, atau menggunakan tanda hubung yang berdekatan dengan titik.
- Nama bucket tidak dapat diformat sebagai alamat IP (198.51.100.24).

> **Warning**
>
> Karena S3 memungkinkan bucket Anda digunakan sebagai URL yang dapat diakses publik, nama bucket yang Anda pilih harus unik secara global. Jika beberapa akun lain telah membuat bucket dengan nama yang Anda pilih, Anda harus menggunakan nama lain.

Untuk informasi selengkapnya, lihat Pembatasan dan batasan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

AWS KMS persyaratan penamaan alias

Saat Anda membuat AWS KMS key, Anda dapat memilih alias untuk mengidentifikasinya. Misalnya, Anda dapat memilih alias “KMS- CloudTrail -us-west-2" untuk mengenkripsi log untuk jejak tertentu.

Alias harus memenuhi persyaratan berikut:

- Antara 1 dan 256 karakter, inklusif
- Berisi karakter alfanumerik (A-Z, a-z, 0-9), tanda hubung (-), garis miring maju (/), dan garis bawah (_)
- Tidak bisa dimulai dengan aws

Untuk informasi selengkapnya, lihat Membuat Kunci di Panduan Developer AWS Key Management Service .

Akun AWS penutupan dan jalan setapak

AWS CloudTrail terus memantau dan mencatat peristiwa untuk aktivitas akun yang dihasilkan oleh pengguna, peran, atau Layanan AWS untuk akun Akun AWS. Pengguna dapat membuat CloudTrail jejak untuk menerima salinan peristiwa ini dalam bucket S3 yang mereka miliki.

CloudTrail adalah layanan keamanan dasar, oleh karena itu, jejak yang dibuat oleh pengguna terus ada dan mengirimkan peristiwa bahkan setelah Akun AWS ditutup, kecuali pengguna secara eksplisit menghapus jejak di mereka sebelum menutupnya. Akun AWS Ini memastikan bahwa jika pengguna membuka kembali akun tertutup, pengguna memiliki catatan aktivitas akun yang tidak terputus. Ini juga memberi pengguna visibilitas ke aktivitas akun akhir apa pun, termasuk penghapusan dan penghentian sumber daya dan layanan akun yang tersisa.

Sebelum Anda menutup Akun AWS, pertimbangkan hal berikut:

- Jalur terus ada bahkan setelah periode pasca-penutupan telah berlalu. Periode pasca-penutupan mengacu pada 90 hari antara saat Anda menutup akun dan saat menutup akun Anda AWS secara permanen. Akun AWS

- Perilaku ini juga berlaku untuk jejak organisasi yang dibuat oleh akun manajemen atau administrator yang didelegasikan, dan untuk jejak organisasi multi-wilayah yang dibuat di akun anggota organisasi.
- Untuk jejak yang mengirimkan peristiwa ke bucket S3 di akun yang sama, jejak tetap ada bahkan setelah akun ditutup. Namun, karena bucket S3 dihapus saat akun ditutup, jejak tidak terus mengirimkan acara.
- Untuk jejak yang mengirimkan peristiwa ke bucket S3 di akun yang berbeda, jejak tetap ada bahkan setelah akun ditutup. Trails juga terus mengirimkan acara ke bucket S3 jika acara dapat dikirimkan. Misalnya, jejak organisasi terus mengirimkan acara ke bucket S3 jika Anda menutup akun anggota di organisasi, tetapi Anda tidak menutup akun manajemen.
- Untuk jalur yang dienkripsi dengan AWS KMS keys, jejak terus ada setelah akun ditutup selain kunci KMS.

Pengguna memiliki opsi untuk menghapus jejak sebelum menutupnya Akun AWS, atau menghubungi AWS Dukunganuntuk meminta penghapusan jejak setelah ditutup. Akun AWS

Untuk informasi tentang menutup Akun AWS, lihat Menutup Akun AWS di Panduan AWS Account Management Referensi.

> **Note**
>
> Jika validasi file CloudTrail log diaktifkan, pengguna akan terus menerima file intisari per jam yang menunjukkan apakah ada CloudTrail log yang dibuat atau tidak.
> CloudTrail Penyimpanan data peristiwa Lake, saluran CloudTrail Lake untuk integrasi, saluran CloudTrail terkait layanan, dan sumber daya yang dibuat untuk jalur (misalnya, grup CloudWatch log Amazon Logs dan bucket Amazon S3 yang ada di akun tertutup), mengikuti AWS perilaku standar untuk penutupan akun dan dihapus secara permanen setelah periode pasca-penutupan (biasanya 90 hari).

Konfigurasikan CloudTrail pengaturan

Anda dapat menggunakan halaman Pengaturan di CloudTrail konsol untuk mengonfigurasi dan meninjau CloudTrail pengaturan, seperti mengelola administrator yang didelegasikan untuk AWS Organizations organisasi dan melihat saluran terkait layanan yang dibuat untuk akun Anda.

Untuk mengakses halaman Pengaturan

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pilih Pengaturan di panel navigasi kiri CloudTrail konsol.
3. Tinjau dan perbarui pengaturan Anda sesuai kebutuhan.

   Pengaturan berikut tersedia:

   - Administrator yang didelegasikan organisasi — Jika memiliki AWS Organizations organisasi, Anda dapat melihat administrator yang CloudTrail didelegasikan, menambahkan administrator yang didelegasikan (maksimal tiga maksimum), dan menghapus administrator yang didelegasikan. Hanya akun manajemen organisasi yang dapat menambah atau menghapus administrator yang didelegasikan.

     Akun manajemen organisasi dapat menetapkan akun apa pun dalam organisasi untuk bertindak sebagai administrator yang CloudTrail didelegasikan untuk mengelola jejak organisasi dan penyimpanan data acara atas nama organisasi.
   - Melihat saluran terkait layanan— Anda dapat melihat saluran terkait layanan apa pun yang dibuat untuk akun Anda.

     Layanan AWS dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWS Layanan yang membuat saluran terkait layanan mengonfigurasi penyeleksi peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semua Wilayah AWS, atau satu saluran. Wilayah AWS

Administrator delegasi dalam organisasi

Saat Anda menggunakan CloudTrail AWS Organizations organisasi, Anda dapat menetapkan akun apa pun dalam organisasi untuk bertindak sebagai administrator yang CloudTrail didelegasikan untuk mengelola jejak organisasi dan penyimpanan data peristiwa atas nama organisasi. Administrator

yang didelegasikan adalah akun anggota dalam organisasi yang dapat melakukan tugas administratif yang sama (kecuali sebagaimana disebutkan) CloudTrail sebagai akun manajemen.

Jika Anda memilih administrator yang didelegasikan, akun anggota ini memiliki izin administratif pada semua jejak organisasi dan penyimpanan data acara di organisasi. Menambahkan administrator yang didelegasikan tidak mengubah manajemen atau pengoperasian jejak organisasi atau penyimpanan data acara.

Saat pertama kali menambahkan administrator yang didelegasikan di CloudTrail konsol, atau menggunakan CloudTrail API AWS CLI atau, CloudTrail memeriksa apakah akun manajemen organisasi memiliki peran terkait layanan. Jika akun manajemen tidak memiliki peran terkait layanan, CloudTrail buat peran terkait layanan untuk akun manajemen. Untuk mengetahui informasi selengkapnya tentang peran terkait layanan, lihat Menggunakan peran terkait layanan untuk CloudTrail.

> **Note**
>
> Saat Anda menambahkan administrator yang didelegasikan menggunakan operasi AWS Organizations CLI atau API CloudTrail , peran terkait layanan tidak akan dibuat secara otomatis jika tidak ada. Peran terkait layanan hanya dibuat saat Anda melakukan panggilan dari akun manajemen langsung ke layanan. CloudTrail Misalnya, saat Anda menambahkan administrator yang didelegasikan atau membuat jejak organisasi atau penyimpanan data peristiwa menggunakan CloudTrail konsol, AWS CLI atau CloudTrail API, peran AWSServiceRoleForCloudTrail terkait layanan akan dibuat.
> Saat Anda menambahkan administrator yang didelegasikan menggunakan AWS CloudTrail; CLI atau operasi API CloudTrail , akan membuat peran dan AWSServiceRoleForCloudTrailEventContext peran AWSServiceRoleForCloudTrail terkait layanan. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk CloudTrail.

Perhatikan faktor-faktor berikut yang menentukan bagaimana administrator yang didelegasikan beroperasi CloudTrail.

Akun manajemen tetap menjadi pemilik sumber daya CloudTrail organisasi apa pun yang dibuat oleh administrator yang didelegasikan.

Akun manajemen organisasi tetap menjadi pemilik sumber daya CloudTrail organisasi apa pun yang dibuat oleh administrator yang didelegasikan, seperti jejak dan penyimpanan data peristiwa. Ini memberikan kontinuitas bagi organisasi jika administrator yang didelegasikan berubah.

Menghapus akun administrator yang didelegasikan tidak akan menghapus sumber daya CloudTrail organisasi apa pun yang mereka buat.

Jejak organisasi dan penyimpanan data peristiwa yang dibuat oleh administrator yang didelegasikan tidak akan dihapus saat Anda menghapus administrator yang didelegasikan, karena akun manajemen selalu berfungsi sebagai pemilik sumber daya CloudTrail organisasi terlepas dari apakah mereka dibuat oleh administrator yang didelegasikan atau akun manajemen.

Sebuah organisasi dapat memiliki maksimal tiga administrator yang CloudTrail didelegasikan.

Anda dapat memiliki maksimal tiga administrator yang CloudTrail didelegasikan per organisasi. Untuk informasi selengkapnya tentang menghapus administrator yang didelegasikan, lihatMenghapus administrator yang CloudTrail didelegasikan.

Tabel berikut menunjukkan kemampuan akun manajemen, akun administrator yang didelegasikan, dan akun yang menjadi anggota dalam AWS Organizations organisasi.

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan	Akun anggota
Menambahkan atau menghapus akun administrator yang didelegasikan.	Ya	Tidak	Tidak
Buat jejak organisasi.	Ya	Ya [1]	Tidak
Lihat daftar jejak organisasi.	Ya	Ya	Ya
Perbarui jejak organisasi.	Ya	Ya [1, 2]	Tidak
Hapus jejak organisasi.	Ya	Ya	Tidak

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan	Akun anggota
Buat penyimpanan data acara organisasi untuk CloudTrail acara atau item AWS Config konfigurasi.	Ya	Ya	Tidak
Aktifkan Wawasan tentang penyimpanan data acara organisasi.	Ya	Tidak	Tidak
Perbarui penyimpanan data acara organisasi.	Ya	Ya [2]	Tidak
Mulai dan hentikan konsumsi acara di penyimpanan data acara organisasi.	Ya	Ya	Tidak
Aktifkan federasi kueri Danau di penyimpanan data acara organisasi [3].	Ya	Ya	Tidak
Nonaktifkan federasi kueri Danau di penyimpanan data acara organisasi.	Ya	Ya	Tidak
Hapus penyimpanan data acara organisasi.	Ya	Ya	Tidak
Salin peristiwa jejak ke penyimpanan data acara organisasi.	Ya	Tidak	Tidak
Jalankan kueri pada penyimpanan data acara organisasi.	Ya	Ya	Tidak
Melihat dasbor terkelola untuk penyimpanan data acara organisasi.	Ya	Tidak	Tidak
Aktifkan dasbor Sorotan untuk penyimpanan data acara organisasi.	Ya	Tidak	Tidak

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan	Akun anggota
Buat widget untuk dasbor kustom yang menanyakan penyimpanan data acara organisasi.	Ya	Tidak	Tidak

[1] Administrator yang didelegasikan hanya dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API. Grup CloudWatch log Log dan peran log harus ada di akun panggilan.

[2] Hanya akun manajemen yang dapat mengonversi jejak organisasi atau penyimpanan data acara ke jejak tingkat akun atau penyimpanan data acara, atau mengonversi jejak tingkat akun atau penyimpanan data acara ke jejak organisasi atau penyimpanan data acara. Tindakan ini tidak diizinkan untuk administrator yang didelegasikan karena jejak organisasi dan penyimpanan data peristiwa hanya ada di akun manajemen. Ketika jejak organisasi atau penyimpanan data peristiwa dikonversi ke jejak tingkat akun atau penyimpanan data peristiwa, hanya akun manajemen yang memiliki akses ke penyimpanan data jejak atau peristiwa.

[3] Hanya satu akun administrator yang didelegasikan atau akun manajemen yang dapat mengaktifkan federasi pada penyimpanan data acara organisasi. Akun administrator lain yang didelegasikan dapat menanyakan dan berbagi informasi menggunakan fitur berbagi data Lake Formation. Setiap akun administrator yang didelegasikan serta akun manajemen organisasi dapat menonaktifkan federasi.

Topik

- Izin yang diperlukan untuk menetapkan administrator yang didelegasikan
- Menambahkan administrator yang CloudTrail didelegasikan
- Menghapus administrator yang CloudTrail didelegasikan

Izin yang diperlukan untuk menetapkan administrator yang didelegasikan

Saat menetapkan administrator yang CloudTrail didelegasikan, Anda harus memiliki izin untuk menambahkan dan menghapus administrator yang didelegasikan CloudTrail, serta tindakan AWS Organizations API tertentu dan izin IAM yang tercantum dalam pernyataan kebijakan berikut.

Anda dapat menambahkan pernyataan berikut di akhir kebijakan IAM untuk memberikan izin ini:

```
{
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

Pertimbangan saat menggunakan kunci kondisi dengan pernyataan kebijakan untuk izin administrator yang didelegasikan

Anda dapat mempertimbangkan untuk menggunakan kunci kondisi global IAM saat menambahkan pernyataan kebijakan untuk menambah dan menghapus administrator yang didelegasikan CloudTrail untuk keamanan tambahan. Saat melakukannya, ingatlah untuk menyertakan kedua nama utama layanan (SPNs) ke kondisi tersebut. Contoh:

```
{
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "context.cloudtrail.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      },
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow"
}
```

Untuk informasi selengkapnya, lihat Identity and Access Management untuk AWS CloudTrail.

Menambahkan administrator yang CloudTrail didelegasikan

Anda dapat menambahkan administrator yang didelegasikan untuk mengelola CloudTrail sumber daya organisasi, seperti jejak dan penyimpanan data peristiwa.

Anda dapat menambahkan administrator yang CloudTrail didelegasikan untuk AWS organisasi Anda menggunakan CloudTrail konsol atau. AWS CLI

Sebelum menambahkan administrator yang didelegasikan, pastikan mereka memiliki akun di organisasi Anda dan Anda masuk dengan akun manajemen untuk organisasi Anda. Untuk informasi tentang cara membuat AWS akun baru untuk organisasi Anda, lihat Membuat AWS akun di organisasi Anda. Untuk informasi tentang cara mengundang AWS akun yang ada ke organisasi Anda, lihat Mengundang AWS akun untuk bergabung dengan organisasi Anda.

CloudTrail console

Prosedur berikut menunjukkan cara menambahkan administrator yang CloudTrail didelegasikan menggunakan CloudTrail konsol.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pilih Pengaturan di panel navigasi kiri CloudTrail konsol.
3. Di bagian Administrator yang didelegasikan organisasi, pilih Daftarkan administrator.
4. Masukkan ID AWS akun dua belas digit dari akun yang ingin Anda tetapkan sebagai administrator yang CloudTrail didelegasikan untuk jejak organisasi dan penyimpanan data peristiwa.
5. Pilih Daftarkan administrator.

AWS CLI

Contoh berikut menambahkan administrator yang CloudTrail didelegasikan.

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

Perintah ini tidak menghasilkan output jika berhasil.

Menghapus administrator yang CloudTrail didelegasikan

Anda dapat menghapus administrator yang CloudTrail didelegasikan menggunakan CloudTrail konsol atau file. AWS CLI

CloudTrail console

Prosedur berikut menunjukkan cara menghapus administrator yang CloudTrail didelegasikan menggunakan CloudTrail konsol.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pilih Pengaturan di panel navigasi kiri CloudTrail konsol.
3. Di bagian Administrator yang didelegasikan organisasi, pilih administrator yang didelegasikan yang ingin Anda hapus.
4. Pilih Hapus administrator.
5. Konfirmasikan bahwa Anda ingin menghapus administrator yang didelegasikan dan kemudian pilih Hapus administrator.

AWS CLI

Perintah berikut menghapus administrator yang CloudTrail didelegasikan.

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

Perintah ini tidak menghasilkan output jika berhasil.

Melihat saluran terkait layanan

AWS layanan dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWS Layanan yang membuat saluran terkait layanan mengonfigurasi penyeleksi peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semua Wilayah AWS, atau satu saluran. Wilayah AWS

Topik

- Melihat saluran terkait layanan dengan menggunakan konsol

- Melihat saluran terkait layanan dengan menggunakan AWS CLI

Melihat saluran terkait layanan dengan menggunakan konsol

Menggunakan CloudTrail konsol, Anda dapat melihat informasi tentang saluran CloudTrail terkait layanan apa pun yang dibuat oleh AWS layanan. Tabel kosong jika akun Anda tidak memiliki saluran terkait layanan.

Gunakan prosedur berikut untuk melihat informasi tentang saluran terkait layanan.

1. Pilih Pengaturan di panel navigasi kiri CloudTrail konsol.
2. Dari saluran terkait layanan, pilih saluran terkait layanan untuk melihat detailnya.
3. Pada halaman detail, tinjau pengaturan yang dikonfigurasi untuk saluran terkait layanan.

   Anda dapat melihat informasi berikut di halaman detail.

   - Nama saluran - Nama lengkap saluran. Format nama saluran adalah `aws-service-channel/`*`AWS_service_name`*`/slc` tempat *`AWS_service_name`* mewakili nama AWS layanan yang mengelola saluran.
   - Saluran ARN - ARN saluran, yang dapat Anda gunakan dalam permintaan API untuk mendapatkan detail tentang saluran tersebut.
   - Semua wilayah - Nilainya adalah `Yes` jika saluran dikonfigurasi untuk semua Wilayah AWS.
   - AWS layanan - Nama AWS layanan yang mengelola saluran.
   - Acara manajemen - Menampilkan peristiwa manajemen apa pun yang dikonfigurasi untuk saluran.
   - Peristiwa data - Menampilkan peristiwa data apa pun yang dikonfigurasi untuk saluran.

Melihat saluran terkait layanan dengan menggunakan AWS CLI

Dengan menggunakan AWS CLI, Anda dapat melihat informasi tentang saluran CloudTrail terkait layanan apa pun yang dibuat oleh AWS layanan.

Topik

- Dapatkan saluran CloudTrail terkait layanan
- Daftar semua saluran CloudTrail terkait layanan
- AWS acara layanan di saluran terkait layanan

Dapatkan saluran CloudTrail terkait layanan

Contoh AWS CLI perintah berikut menampilkan informasi tentang saluran CloudTrail terkait layanan tertentu, termasuk nama AWS layanan tujuan, pemilih lanjutan yang dikonfigurasi untuk saluran, dan apakah saluran tersebut berlaku untuk semua Wilayah atau satu Wilayah.

Anda harus menentukan ARN atau akhiran ID dari ARN untuk. `--channel`

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

Berikut ini adalah contoh respons. Dalam contoh ini, `AWS_service_name` mewakili nama AWS layanan yang membuat saluran.

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

Daftar semua saluran CloudTrail terkait layanan

AWS CLI Perintah contoh berikut mengembalikan informasi tentang semua saluran CloudTrail terkait layanan yang dibuat atas nama Anda. Parameter opsional termasuk`--max-results`, untuk menentukan jumlah maksimum hasil yang Anda inginkan perintah untuk kembali pada satu halaman. Jika ada lebih banyak hasil daripada `--max-results` nilai yang Anda tentukan, jalankan perintah lagi dengan menambahkan `NextToken` nilai yang dikembalikan untuk mendapatkan halaman hasil berikutnya.

```
aws cloudtrail list-channels
```

Berikut ini adalah contoh respons. Dalam contoh ini, `AWS_service_name` mewakili nama AWS layanan yang membuat saluran.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS acara layanan di saluran terkait layanan

AWS Layanan yang mengelola saluran terkait layanan dapat memulai tindakan pada saluran terkait layanan (misalnya, membuat atau memperbarui saluran terkait layanan). CloudTrail mencatat tindakan ini sebagai peristiwa AWS layanan, dan mengirimkan peristiwa ini ke riwayat Acara, dan setiap jejak aktif dan penyimpanan data peristiwa yang dikonfigurasi untuk acara manajemen. Untuk acara-acara ini, `eventType` bidangnya adalah`AwsServiceEvent`.

Berikut ini adalah contoh entri file log dari acara AWS layanan untuk pembuatan saluran terkait layanan.

```
{
```

```
    "eventVersion":"1.08",
    "userIdentity":{
       "accountId":"111122223333",
       "invokedBy":"AWS Internal"
    },
    "eventTime":"2022-08-18T17:11:22Z",
    "eventSource":"cloudtrail.amazonaws.com",
    "eventName":"CreateServiceLinkedChannel",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"AWS Internal",
    "userAgent":"AWS Internal",
    "requestParameters":null,
    "responseElements":null,
    "requestID":"564f004c-EXAMPLE",
    "eventID":"234f004b-EXAMPLE",
    "readOnly":false,
    "resources":[
       {
          "accountId":"184434908391",
          "type":"AWS::CloudTrail::Channel",
          "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
       }
    ],
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "recipientAccountId":"111122223333",
    "eventCategory":"Management"
}
```

Memahami CloudTrail peristiwa

Peristiwa di CloudTrail adalah catatan aktivitas dalam AWS akun. Kegiatan ini dapat berupa tindakan yang diambil oleh identitas IAM, atau layanan yang dapat dipantau oleh. CloudTrail CloudTrail event menyediakan riwayat aktivitas akun API dan non-API yang dibuat melalui Konsol Manajemen AWS, AWS SDK, alat baris perintah, dan lainnya. Layanan AWS

CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga peristiwa tidak muncul dalam urutan tertentu.

Ada empat jenis CloudTrail acara:

- Acara manajemen
- Peristiwa data
- Acara aktivitas jaringan
- Insights acara

Secara default, data jejak dan peristiwa menyimpan peristiwa manajemen log, tetapi bukan peristiwa data, peristiwa aktivitas jaringan, atau peristiwa Wawasan.

Semua jenis acara menggunakan format log CloudTrail JSON. Log berisi informasi tentang permintaan sumber daya di akun Anda, seperti siapa yang membuat permintaan, layanan yang digunakan, tindakan yang dilakukan, dan parameter untuk tindakan tersebut. Data peristiwa terlampir dalam `Records` array.

Untuk informasi tentang bidang catatan CloudTrail peristiwa untuk peristiwa manajemen, data, dan aktivitas jaringan, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

Untuk informasi tentang bidang catatan CloudTrail peristiwa untuk acara Insights untuk jejak, lihat. CloudTrail merekam konten untuk acara Insights untuk jalur

Untuk informasi tentang bidang catatan CloudTrail peristiwa untuk peristiwa Wawasan untuk penyimpanan data acara, lihatCloudTrail merekam konten untuk acara Wawasan untuk penyimpanan data acara.

Peristiwa manajemen

Acara manajemen memberikan informasi tentang operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi pesawat kontrol.

Contoh acara manajemen meliputi:

- Mengkonfigurasi keamanan (misalnya, operasi AWS Identity and Access Management `AttachRolePolicy` API).
- Mendaftarkan perangkat (misalnya, operasi `CreateDefaultVpc` API Amazon EC2).
- Mengkonfigurasi aturan untuk merutekan data (misalnya, operasi Amazon `CreateSubnet` EC2 API).
- Menyiapkan logging (misalnya, operasi AWS CloudTrail `CreateTrail` API).

Peristiwa manajemen juga dapat mencakup peristiwa non-API yang terjadi di akun Anda. Misalnya, saat pengguna masuk ke akun Anda, CloudTrail mencatat `ConsoleLogin` peristiwa tersebut. Untuk informasi selengkapnya, lihat Peristiwa non-API yang ditangkap oleh CloudTrail.

Secara default, CloudTrail jejak dan data acara CloudTrail Lake menyimpan peristiwa manajemen log. Untuk informasi selengkapnya tentang peristiwa manajemen logging, lihatMencatat log peristiwa manajemen.

Contoh berikut menunjukkan catatan log tunggal dari peristiwa manajemen. Dalam peristiwa ini, pengguna IAM bernama `Mary_Major` menjalankan aws cloudtrail start-logging perintah untuk memanggil CloudTrail `StartLogging`tindakan untuk memulai proses logging pada jejak bernamamy`Trail`.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
```

```
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Dalam contoh berikut ini, pengguna pengguna IAM bernama `Paulo_Santos` menjalankan aws cloudtrail start-event-data-store-ingestion perintah untuk memanggil `StartEventDataStoreIngestion`tindakan untuk memulai konsumsi pada penyimpanan data peristiwa.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
```

```
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


Peristiwa data

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya. Ini juga dikenal sebagai operasi pesawat data. Peristiwa data sering kali merupakan aktivitas bervolume tinggi.

Contoh peristiwa data meliputi:

- Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject`, `DeleteObject`, dan operasi `PutObject` API) pada objek di bucket S3.
- AWS Lambda aktivitas eksekusi fungsi (`Invoke`API).
- CloudTrail `PutAuditEvents`aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS.
- Operasi Amazon SNS `Publish`dan `PublishBatch`API pada topik.

Tabel berikut menunjukkan jenis sumber daya yang tersedia untuk jejak dan penyimpanan data peristiwa. Kolom tipe sumber daya (konsol) menunjukkan pilihan yang sesuai di konsol. Kolom nilai resources.type menunjukkan `resources.type` nilai yang akan Anda tentukan untuk menyertakan peristiwa data dari jenis tersebut di penyimpanan data jejak atau peristiwa Anda menggunakan API atau. AWS CLI CloudTrail

Untuk jejak, Anda dapat menggunakan pemilih peristiwa dasar atau lanjutan untuk mencatat peristiwa data untuk objek Amazon S3 di bucket tujuan umum, fungsi Lambda, dan tabel DynamoDB (ditampilkan dalam tiga baris pertama tabel). Anda hanya dapat menggunakan pemilih acara lanjutan untuk mencatat jenis sumber daya yang ditampilkan di baris yang tersisa.

Untuk penyimpanan data acara, Anda hanya dapat menggunakan pemilih acara lanjutan untuk menyertakan peristiwa data.

Peristiwa data yang didukung oleh AWS CloudTrail

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
OMWDevice CommunicationService	Aktivitas API pada `AWS::Account::ControlledDomain` sumber daya.	AWS: :Akun:: ControlledDomain	`AWS::Account::ControlledDomain`
WorkSpaces Aplikasi Amazon	Agen mengakses acara alat MCP WorkSpaces Aplikasi	Alat MCP Akses Agen	`AWS::AgentAccessMCP::Tools`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Registri Agen	Aktivitas API pada `AWS::AgentRegistry::Registry` sumber daya.	AWS Registri Agen	`AWS::AgentRegistry::Registry`
Amazon AIDevOps	AIDevOps Aktivitas API pada ruang agen.	Agen Ruang	`AWS::AIDevOps::AgentSpace`
Amazon AIDevOps	AIDevOps Aktivitas API pada asosiasi.	AIDevOps asosiasi	`AWS::AIDevOps::Association`
Amazon AIDevOps	AIDevOps Aktivitas API di tim aplikasi operator.	AIDevOps tim aplikasi operator	`AWS::AIDevOps::OperatorAppTeam`
Amazon AIDevOps	AIDevOps Aktivitas API pada metadata pipeline.	AIDevOps Metadata Pipa	`AWS::AIDevOps::PipelineMetadata`
Amazon AIDevOps	AIDevOps Aktivitas API pada layanan.	AIDevOps layanan	`AWS::AIDevOps::Service`
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada investigasi operasional. Untuk informasi selengkapnya, lihat Pengembang Amazon Q.	Grup Investigasi AIOps	`AWS::AIOps::InvestigationGroup`
Amazon Tanpa OpenSearch Server	Aktivitas API pada `AWS::AOSS::Collection` sumber daya.	AWS: :AOSS: :I	`AWS::AOSS::Collection`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS AppConfig	AWS AppConfig Aktivitas API untuk operasi konfigurasi seperti panggilan ke StartConfigurationSession dan GetLatestConfiguration. Untuk informasi selengkapnya, lihat AWS AppConfig.	AWS AppConfig	`AWS::AppConfig::Configuration`
CloudWatch Sinyal Aplikasi	Aktivitas API pada `AWS::ApplicationSignals::InstrumentationConfig` sumber daya.	AWS::ApplicationSignals::InstrumentationConfig	`AWS::ApplicationSignals::InstrumentationConfig`
AWS AppSync	AWS AppSync Aktivitas API pada AppSync GraphQL API. Untuk informasi selengkapnya, lihat AWS AppSync.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`
Ruang kerja antropik eksternal	Aktivitas API pada `AWS::AWSExternalAnthropic::Workspace` sumber daya.	Ruang kerja antropik eksternal	`AWS::AWSExternalAnthropic::Workspace`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Pertukaran Data B2B	Aktivitas API Pertukaran Data B2B untuk operasi Transformer seperti panggilan ke dan. GetTransformerJob StartTransformerJob	Pertukaran Data B2B	`AWS::B2BI::Transformer`
AWS Titik akses Backup	Aktivitas API pada `AWS::Backup::BackupAccessPoint` sumber daya.	AWS Titik akses Backup	`AWS::Backup::BackupAccessPoint`
AWS Backup	AWS Aktivitas Backup Search Data API pada pekerjaan pencarian.	AWS API Data Pencarian Cadangan	`AWS::Backup::SearchJob`
Amazon Bedrock	Aktivitas API dasar pada pekerjaan prompt optimasi lanjutan.	AdvancedOptimizePromptJob	`AWS::Bedrock::AdvancedOptimizePromptJob`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias agen. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Alias agen batuan dasar	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada pemanggilan asinkron.	Panggilan asinkron batuan dasar	`AWS::Bedrock::AsyncInvoke`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock API pada kebijakan penalaran otomatis.	Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada versi kebijakan penalaran otomatis.	Versi Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicyVersion`
Amazon Bedrock	Aktivitas API cetak biru Amazon Bedrock.	Cetak biru batuan dasar	`AWS::Bedrock::Blueprint`
Amazon Bedrock	Aktivitas API pemanggilan otomatisasi data batuan dasar.	Pemanggilan Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationInvocation`
Amazon Bedrock	Aktivitas API profil otomatisasi data Amazon Bedrock.	Profil Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProfile`
Amazon Bedrock	Aktivitas API proyek otomatisasi data Amazon Bedrock.	Proyek Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProject`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias flow.	Alias aliran batuan dasar	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada eksekusi aliran.	Eksekusi Aliran	`AWS::Bedrock::FlowExecution`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock API di pagar pembatas.	Pagar pembatas batuan dasar	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada agen inline.	Memohon Batuan Dasar Inline-Agent	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada basis pengetahuan. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Basis pengetahuan batuan dasar	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada model.	Model batuan dasar	`AWS::Bedrock::Model`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada prompt.	Permintaan batuan dasar	`AWS::Bedrock::PromptVersion`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada sesi.	Sesi batuan dasar	`AWS::Bedrock::Session`
Amazon Bedrock	Aktivitas API Amazon Bedrock Tool.	Alat Batuan Dasar	`AWS::Bedrock::Tool`
Bedrock-AgentCore ABTest	Aktivitas API pada `AWS::BedrockAgentCore::ABTest` sumber daya.	Bedrock-AgentCore ABTest	`AWS::BedrockAgentCore::ABTest`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Amazon Bedrock ApiKey CredentialProvider .	Bedrock-AgentCore apiKey CredentialProvider	`AWS::BedrockAgentCore::APIKeyCredentialProvider`
BedrockAgentCore evaluasi batch	Aktivitas API pada `AWS::BedrockAgentCore::BatchEvaluate` sumber daya.	BedrockAgentCore evaluasi batch	`AWS::BedrockAgentCore::BatchEvaluate`
Amazon Bedrock	Aktivitas API Browser Amazon Bedrock.	Bedrock-AgentCore Browser	`AWS::BedrockAgentCore::Browser`
Amazon Bedrock	Aktivitas Amazon Bedrock Browser-Custom API.	Bedrock-AgentCore Browser-Custom	`AWS::BedrockAgentCore::BrowserCustom`
Bedrock-AgentCore Profil Browser	Aktivitas API pada `AWS::BedrockAgentCore::BrowserProfile` sumber daya.	Bedrock-AgentCore Profil Browser	`AWS::BedrockAgentCore::BrowserProfile`
BedrockAgentCore CapacityProvider	Aktivitas API pada `AWS::BedrockAgentCore::CapacityProvider` sumber daya.	BedrockAgentCore CapacityProvider	`AWS::BedrockAgentCore::CapacityProvider`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter API.	Bedrock-AgentCore Code-Interpreter	`AWS::BedrockAgentCore::CodeInterpreter`
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter-Custom API.	Bedrock-AgentCore Code-Interpreter-Custom	`AWS::BedrockAgentCore::CodeInterpreterCustom`
Batuan Dasar Amazon AgentCore	Aktivitas AgentCore API batuan dasar pada evaluator.	Bedrock-AgentCore Penilai	`AWS::BedrockAgentCore::Evaluator`
Amazon Bedrock	Aktivitas API Amazon Bedrock Gateway.	Bedrock-AgentCore Gerbang	`AWS::BedrockAgentCore::Gateway`
Amazon Bedrock	Aktivitas API Memori Amazon Bedrock.	Bedrock-AgentCore Memori	`AWS::BedrockAgentCore::Memory`
Amazon Bedrock	Aktivitas API Amazon Bedrock Oauth2 CredentialProvider .	Bedrock-AgentCore Oauth2 CredentialProvider	`AWS::BedrockAgentCore::OAuth2CredentialProvider`
Bedrock-AgentCore pembayaran	Aktivitas API pada `AWS::BedrockAgentCore::Payments` sumber daya.	Bedrock-AgentCore pembayaran	`AWS::BedrockAgentCore::Payments`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Bedrock-AgentCore kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::Policy` sumber daya.	Bedrock-AgentCore kebijakan	`AWS::BedrockAgentCore::Policy`
Bedrock-AgentCore mesin kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::PolicyEngine` sumber daya.	Bedrock-AgentCore mesin kebijakan	`AWS::BedrockAgentCore::PolicyEngine`
Bedrock-AgentCore Rekomendasi	Aktivitas API pada `AWS::BedrockAgentCore::Recommendation` sumber daya.	Bedrock-AgentCore Rekomendasi	`AWS::BedrockAgentCore::Recommendation`
Bedrock-AgentCore Registri	Aktivitas API pada `AWS::BedrockAgentCore::Registry` sumber daya.	Bedrock-AgentCore Registri	`AWS::BedrockAgentCore::Registry`
Amazon Bedrock	Aktivitas API Amazon Bedrock Runtime.	Bedrock-AgentCore Runtime	`AWS::BedrockAgentCore::Runtime`
Amazon Bedrock	Aktivitas Amazon Bedrock Runtime-Endpoint API.	Bedrock-AgentCore Runtime-Endpoint	`AWS::BedrockAgentCore::RuntimeEndpoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Amazon Bedrock Token Vault.	Bedrock-AgentCore Brankas Token	`AWS::BedrockAgentCore::TokenVault`
Amazon Bedrock	Aktivitas API Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentity`
Amazon Bedrock	Aktivitas API Direktori Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Direktori Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentityDirectory`
Proyek Mantel Batuan Dasar	Aktivitas API pada `AWS::BedrockMantle::Project` sumber daya.	Proyek Mantel Batuan Dasar	`AWS::BedrockMantle::Project`
Alat Pencarian Web Bedrock	Aktivitas API pada `AWS::BedrockWebSearch::Tool` sumber daya.	Alat Pencarian Web Bedrock	`AWS::BedrockWebSearch::Tool`
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces (untuk Apache Cassandra) di aliran Cassandra CDC.	Aliran CDC Cassandra	`AWS::Cassandra::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces di atas meja. Untuk informasi selengkapnya, lihat Amazon Keyspaces (untuk Apache Cassandra).	Meja Cassandra	`AWS::Cassandra::Table`
Certificate Manager	Aktivitas API pada `AWS::CertificateManager::AcmeEndpoint` sumber daya.	AWS::CertificateManager::AcmeEndpoint	`AWS::CertificateManager::AcmeEndpoint`
Uji Klinis Daftar kode teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Codelist` sumber daya.	Uji Klinis Daftar kode teknologi	`AWS::ClinicalTrialsTech::Codelist`
Dataset Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Dataset` sumber daya.	Dataset Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Dataset`
Uji Klinis Eksekusi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Execution` sumber daya.	Uji Klinis Eksekusi teknologi	`AWS::ClinicalTrialsTech::Execution`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Contoh Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Instance` sumber daya.	Contoh Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Instance`
Uji Klinis Pemetaan teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Mapping` sumber daya.	Uji Klinis Pemetaan teknologi	`AWS::ClinicalTrialsTech::Mapping`
Jadwal Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Schedule` sumber daya.	Jadwal Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Schedule`
Uji Klinis Studi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Study` sumber daya.	Uji Klinis Studi teknologi	`AWS::ClinicalTrialsTech::Study`
Amazon CloudFront	CloudFront Aktivitas API pada a KeyValueStore. Untuk informasi selengkapnya, lihat Amazon CloudFront.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API pada profil.	AWS::CloudOptimization: :Profil	`AWS::CloudOptimization::Profile`
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API berdasarkan rekomendasi.	AWS::CloudOptimization: :Rekomendasi	`AWS::CloudOptimization::Recommendation`
AWS CloudTrail	CloudTrail PutAuditEvents aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS. Untuk informasi selengkapnya, lihat AWS CloudTrail.	CloudTrail saluran	`AWS::CloudTrail::Channel`
CloudWatch dataset	Aktivitas API pada `AWS::CloudWatch::Dataset` sumber daya.	CloudWatch dataset	`AWS::CloudWatch::Dataset`
Titik akhir konsumsi observabilitas	Aktivitas API pada `AWS::CloudWatch::IngestionEndpoint` sumber daya.	Titik akhir konsumsi observabilitas	`AWS::CloudWatch::IngestionEndpoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon CloudWatch	Aktivitas Amazon CloudWatch API pada metrik. Untuk informasi selengkap nya, lihat Amazon CloudWatch.	CloudWatch metrik	`AWS::CloudWatch::Metric`
Amazon CodeGuru Profiler	CodeGuru Aktivitas API profiler pada grup profil.	CodeGuru Grup profil profiler	`AWS::CodeGuruProfiler::ProfilingGroup`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API pada kustomisasi.	CodeWhisperer kustomisasi	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API di profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Aktivitas API Amazon Cognito di kumpulan identitas Amazon Cognito. Untuk informasi lebih lanjut, lihat Amazon Cognito.	Kolam Identitas Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Aktivitas API Data Exchange pada aset.	Aset Data Exchange	`AWS::DataExchange::Asset`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada armada. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Armada Cloud	`AWS::Deadline::Fleet`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerjaan. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Lowongan kerja Deadline Cloud	`AWS::Deadline::Job`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada antrian. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu antrian Cloud	`AWS::Deadline::Queue`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerja. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Pekerja Cloud	`AWS::Deadline::Worker`
Peringatan Diode Alerting terkait	Aktivitas API pada `AWS::DiodeAlerting::LinkedAlert` sumber daya.	Peringatan Diode Alerting terkait	`AWS::DiodeAlerting::LinkedAlert`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Aurora DSQL	Aktivitas Amazon Aurora DSQL API pada sumber daya cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
Amazon DynamoDB	Aktivitas Amazon DynamoDB API di stream. Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB Streams	`AWS::DynamoDB::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon DynamoDB	Aktivitas API tingkat item Amazon DynamoDB pada tabel (misalnya, PutItem,, DeleteItem dan operasi API). UpdateItem Untuk tabel dengan aliran diaktifkan, bidang sumber daya dalam peristiwa data berisi: :DynamoDB : :Stream dan AWS AWS: :DynamoDB : :Table. Jika Anda menentukan AWS: :DynamoDB : :Table untuk resources.type, itu akan mencatat tabel DynamoDB dan peristiwa aliran DynamoDB secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter pada bidang EventName . Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB	`AWS::DynamoDB::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Elastic Compute Cloud	Instans Amazon EC2 menghubungkan aktivitas API titik akhir.	Instans EC2 menghubungkan titik akhir	`AWS::EC2::InstanceConnectEndpoint`
Amazon Elastic Block Store	API langsung Amazon Elastic Block Store (EBS), seperti, PutSnapshotBlock, GetSnapshotBlock dan pada snapshot ListChangedBlocks Amazon EBS. Untuk informasi selengkapnya, lihat Amazon Elastic Block Store.	API langsung EBS	`AWS::EC2::Snapshot`
Amazon Elastic Container Service	Aktivitas API Amazon Elastic Container Service pada instance container.	Contoh kontainer ECS	`AWS::ECS::ContainerInstance`
LAYANAN AMAZON ELASTIC KUBERNETES	Aktivitas API Amazon Elastic Kubernetes Service di dasbor.	Dasbor EKS	`AWS::EKS::Dashboard`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon EMR	Aktivitas Amazon EMR API di ruang kerja log tulis di depan. Untuk informasi selengkapnya, lihat Amazon EMR.	Ruang kerja log tulis ke depan EMR	`AWS::EMRWAL::Workspace`
pesan pengguna akhir	Aktivitas API pada `AWS::EndUserMessaging::NotifyCodeVerification` sumber daya.	AWS::EndUserMessaging::NotifyCodeVerification	`AWS::EndUserMessaging::NotifyCodeVerification`
EventBridge titik akhir	Aktivitas API pada `AWS::Events::Endpoint` sumber daya.	EventBridge titik akhir	`AWS::Events::Endpoint`
EventBridge Bus acara khusus - klasik	Aktivitas API pada `AWS::Events::EventBus` sumber daya.	EventBridge Bus acara khusus - klasik	`AWS::Events::EventBus`
EventBridge sumber acara mitra	Aktivitas API pada `AWS::Events::EventSource` sumber daya.	EventBridge sumber acara mitra	`AWS::Events::EventSource`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
EventBridge aturan	Aktivitas API pada `AWS::Events::Rule` sumber daya.	EventBridge aturan	`AWS::Events::Rule`
EventBridge Bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventBus` sumber daya.	EventBridge Bus peristiwa kustom	`AWS::EventsV2::EventBus`
EventBridge Sumber acara bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventSource` sumber daya.	EventBridge Sumber acara bus acara khusus	`AWS::EventsV2::EventSource`
Amazon FinSpace	Aktivitas Amazon FinSpace API di lingkungan. Untuk informasi selengkapnya, lihat Amazon FinSpace.	FinSpace	`AWS::FinSpace::Environment`
Amazon FSx	Aktivitas Amazon FSx API pada volume.	Volume FSx	`AWS::FSx::Volume`
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada aplikasi. Untuk informasi selengkapnya, lihat Amazon GameLift Streams.	GameLift Aplikasi Streams	`AWS::GameLiftStreams::Application`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada grup streaming. Untuk informasi selengkap nya, lihat Amazon GameLift Streams.	GameLift Streaming grup aliran	`AWS::GameLiftStreams::StreamGroup`
Peta Lokasi Amazon	Aktivitas API Peta Lokasi Amazon.	Peta Geo	`AWS::GeoMaps::Provider`
Tempat Lokasi Amazon	Aktivitas API Tempat Lokasi Amazon.	Tempat Geo	`AWS::GeoPlaces::Provider`
Rute Lokasi Amazon	Aktivitas API Rute Lokasi Amazon.	Rute Geo	`AWS::GeoRoutes::Provider`
AWS Glue	AWS Aktivitas Glue API pada tabel yang dibuat oleh Lake Formation.	Formasi Danau	`AWS::Glue::Table`
AWS IoT Greengrass Versi 2	Aktivitas API Greengrass dari perangkat inti Greengrass pada versi komponen. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Versi komponen Greengrass IoT	`AWS::GreengrassV2::ComponentVersion`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT Greengrass Versi 2	Greengrass aktivitas API dari perangkat inti Greengrass pada penerapan. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Penyebaran Greengrass IoT	`AWS::GreengrassV2::Deployment`
Amazon GuardDuty	Aktivitas Amazon GuardDuty API untuk detektor. Untuk informasi selengkapnya, lihat Amazon GuardDuty.	GuardDuty detektor	`AWS::GuardDuty::Detector`
Amazon GuardDuty	GuardDuty Aktivitas API pada pemindaian malware.	GuardDuty pemindaian malware	`AWS::GuardDuty::MalwareScan`
Domain agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Domain` sumber daya.	Domain agen kesehatan	`AWS::HealthAgent::Domain`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Integration` sumber daya.	AWS::HealthAgent: :Integri	`AWS::HealthAgent::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::PatientInsightsJob` sumber daya.	health-agent.amazonaws.com	`AWS::HealthAgent::PatientInsightsJob`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Session` sumber daya.	AWS::HealthAgent: :Sesi	`AWS::HealthAgent::Session`
Berlangganan agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Subscription` sumber daya.	Berlangganan agen kesehatan	`AWS::HealthAgent::Subscription`
Profil transformasi data Health Lake	Aktivitas API pada `AWS::HealthLake::DataTransformationProfile` sumber daya.	Profil transformasi data Health Lake	`AWS::HealthLake::DataTransformationProfile`
AWS IoT	AWS Aktivitas API IoT pada sertifikat. Untuk informasi selengkapnya, lihat AWS IoT.	Sertifikat IoT	`AWS::IoT::Certificate`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT	AWS Aktivitas API IoT pada berbagai hal. Untuk informasi selengkapnya, lihat AWS IoT.	Hal IoT	`AWS::IoT::Thing`
AWS Terowongan IoT	Aktivitas API pada `AWS::IoT::Tunnel` sumber daya.	AWS Terowongan IoT	`AWS::IoT::Tunnel`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada aset. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Aset IoT SiteWise	`AWS::IoTSiteWise::Asset`
Dataset IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Dataset` sumber daya.	Dataset IoT SiteWise	`AWS::IoTSiteWise::Dataset`
Pipa IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Pipeline` sumber daya.	Pipa IoT SiteWise	`AWS::IoTSiteWise::Pipeline`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada deret waktu. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Deret waktu IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Ruang kerja IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Workspace` sumber daya.	Ruang kerja IoT SiteWise	`AWS::IoTSiteWise::Workspace`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT pada entitas. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Entitas IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT di ruang kerja. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Ruang kerja IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Peringkat Cerdas Amazon Kendra	Aktivitas API Amazon Kendra Intelligent Ranking pada rencana eksekusi skor ulang. Untuk informasi selengkapnya, lihat Peringkat Cerdas Amazon Kendra.	Peringkat Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Kinesis Data Streams	Aktivitas API Kinesis Data Streams pada stream. Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Aliran kinesis	`AWS::Kinesis::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Kinesis Data Streams	Kinesis Data Streams aktivitas API pada konsumen streaming . Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Konsumen aliran kinesis	`AWS::Kinesis::StreamConsumer`
Amazon Data Firehose	Aktivitas API aliran pengiriman Amazon Data Firehose.	Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`
Amazon Kinesis Video Streams	Kinesis Video Streams aktivitas API saluran pensinyalan video.	Saluran pensinyalan video Kinesis	`AWS::KinesisVideo::SignalingChannel`
Amazon Kinesis Video Streams	Aktivitas API Kinesis Video Streams pada aliran video, seperti panggilan ke dan. GetMedia PutMedia	Aliran video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Aktivitas eksekusi fungsi Lambda (API Invoke).	Lambda	`AWS::Lambda::Function`
Gambar microvm Lambda	Aktivitas API pada `AWS::Lambda::MicrovmImage` sumber daya.	Gambar microvm Lambda	`AWS::Lambda::MicrovmImage`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Fungsi Web Lambda	Aktivitas API pada `AWS::Lambda::WebFunction` sumber daya.	Lambda WebFunction	`AWS::Lambda::WebFunction`
Lex Bot	Aktivitas API pada `AWS::Lex::Bot` sumber daya.	Lex Bot	`AWS::Lex::Bot`
AWS Lex Bot Alias	Aktivitas API pada `AWS::Lex::BotAlias` sumber daya.	AWS Lex Bot Alias	`AWS::Lex::BotAlias`
CloudWatch Otorisasi grup log log	Aktivitas API pada `AWS::Logs::LogGroupAuthorization` sumber daya.	CloudWatch Otorisasi grup log log	`AWS::Logs::LogGroupAuthorization`
Log Scheduled Query	Aktivitas API pada `AWS::Logs::ScheduledQuery` sumber daya.	Log Scheduled Query	`AWS::Logs::ScheduledQuery`
Amazon Machine Learning	Aktivitas Machine Learning API pada model ML.	Machine Learning MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	Aktivitas API Amazon Managed Blockchain di jaringan.	Jaringan Blockchain yang dikelola	`AWS::ManagedBlockchain::Network`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Managed Blockchain	Amazon Managed Blockchain JSON-RPC memanggil node Ethereum, seperti ETH_getBalance atau eth_get. BlockByNumber Untuk informasi selengkapnya, lihat Amazon Managed Blockchain.	Blockchain yang Dikelola	`AWS::ManagedBlockchain::Node`
Kueri Blockchain yang Dikelola Amazon	Aktivitas API Kueri Blockchain Terkelola Amazon.	Kueri Blockchain Terkelola	`AWS::ManagedBlockchainQuery::QueryAPI`
AWS HealthImaging	AWS HealthImaging Aktivitas API pada penyimpanan data.	MedicalImaging penyimpanan data	`AWS::MedicalImaging::Datastore`
AWS HealthImaging	AWS HealthImaging image set aktivitas API.	MedicalImaging set gambar	`AWS::MedicalImaging::ImageSet`
Amazon Managed Workflows for Apache Airflow	Aktivitas API Amazon MWAA di lingkungan.	Apache Airflow yang Dikelola	`AWS::MWAA::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Grafik Amazon Neptunus	Aktivitas API data, misalnya kueri, algoritme , atau pencarian vektor, pada Grafik Neptunus.	Grafik Neptunus	`AWS::NeptuneGraph::Graph`
Monitor Aliran CloudWatch Jaringan Amazon	Aktivitas API Monitor Aliran CloudWatch Jaringan Amazon pada monitor.	Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Monitor`
Monitor Aliran CloudWatch Jaringan Amazon	Amazon CloudWatch Network Flow Monitor aktivitas API pada cakupan.	Lingkup Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Scope`
Amazon NovaAct	Aktivitas Amazon NovaAct API pada definisi alur kerja.	Definisi alur kerja	`AWS::NovaAct::WorkflowDefinition`
Amazon NovaAct	Aktivitas NovaAct API Amanzon pada alur kerja berjalan.	Alur kerja berjalan	`AWS::NovaAct::WorkflowRun`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise di UKey.	Amazon Satu uKey	`AWS::One::UKey`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise pada pengguna.	Amazon Satu Pengguna	`AWS::One::User`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada alias.	Alias Kriptografi Pembayaran	`AWS::PaymentCryptography::Alias`
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada kunci.	Kunci Kriptografi Pembayaran	`AWS::PaymentCryptography::Key`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API Direktori Aktif.	Konektor CA Pribadi untuk Direktori Aktif	`AWS::PCAConnectorAD::Connector`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API SCEP.	Konektor CA Pribadi untuk SCEP	`AWS::PCAConnectorSCEP::Connector`
Amazon Pinpoint	Amazon Pinpoint aktivitas API pada aplikasi penargetan seluler.	Aplikasi Penargetan Seluler	`AWS::Pinpoint::App`
Aplikasi Amazon Q	Aktivitas API data di Amazon Q Apps. Untuk informasi selengkapnya, lihat Amazon Q Apps.	Aplikasi Amazon Q	`AWS::QApps::QApp`
Aplikasi Amazon Q	Aktivitas API data di sesi Amazon Q App.	Sesi Aplikasi Amazon Q	`AWS::QApps::QAppSession`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada aplikasi. Untuk informasi selengkapnya, lihat Amazon Q Business.	Aplikasi Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada sumber data. Untuk informasi selengkapnya, lihat Amazon Q Business.	Sumber data Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Bisnis	Aktivitas API Amazon Q Business pada indeks. Untuk informasi selengkapnya, lihat Amazon Q Business.	Amazon Q Indeks Bisnis	`AWS::QBusiness::Index`
Amazon Q Bisnis	Aktivitas API integrasi Amazon Q Business.	Integrasi Amazon Q Bisnis	`AWS::QBusiness::Integration`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada pengalaman web. Untuk informasi selengkapnya, lihat Amazon Q Business.	Pengalaman web Amazon Q Bisnis	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada integrasi.	Q Integrasi pengembang	`AWS::QDeveloper::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Cepat Amazon pada konektor tindakan.	AWS QuickSuite Tindakan	`AWS::Quicksight::ActionConnector`
QuickSight Aplikasi Amazon	Aktivitas API pada `AWS::QuickSight::App` sumber daya.	QuickSight Aplikasi Amazon	`AWS::QuickSight::App`
QuickSight otomatisasi	Aktivitas API pada `AWS::QuickSight::Automation` sumber daya.	QuickSight otomatisasi	`AWS::QuickSight::Automation`
QuickSight pekerjaan otomatisasi	Aktivitas API pada `AWS::QuickSight::AutomationJob` sumber daya.	QuickSight pekerjaan otomatisasi	`AWS::QuickSight::AutomationJob`
AWS QuickSight Ekstensi	Aktivitas API pada `AWS::QuickSight::Extension` sumber daya.	AWS QuickSight Ekstensi	`AWS::QuickSight::Extension`
AWS QuickSight Akses Ekstensi	Aktivitas API pada `AWS::QuickSight::ExtensionAccess` sumber daya.	AWS QuickSight Akses Ekstensi	`AWS::QuickSight::ExtensionAccess`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Aliran Cepat Amazon.	AWS QuickSight aliran	`AWS::QuickSight::Flow`
Amazon Quick	Aktivitas FlowSession API Cepat Amazon.	AWS QuickSight sesi aliran	`AWS::QuickSight::FlowSession`
QuickSight Halaman Amazon	Aktivitas API pada `AWS::QuickSight::Page` sumber daya.	QuickSight Halaman Amazon	`AWS::QuickSight::Page`
QuickSight Tugas	Aktivitas API pada `AWS::QuickSight::Task` sumber daya.	QuickSight Tugas	`AWS::QuickSight::Task`
Amazon RDS	Aktivitas Amazon RDS API di Cluster DB. Untuk informasi selengkapnya, lihat Amazon RDS.	API Data RDS - Kluster DB	`AWS::RDS::DBCluster`
Amazon Redshift	Aktivitas Redshift API pada cluster.	Gugus Pergeseran Merah	`AWS::Redshift::Cluster`
AWS Tampilan terkelola Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::ManagedView` sumber daya.	AWS Tampilan terkelola Resource Explorer	`AWS::ResourceExplorer2::ManagedView`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Tampilan Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::View` sumber daya.	AWS Tampilan Resource Explorer	`AWS::ResourceExplorer2::View`
Amazon CloudWatch RUM	Aktivitas Amazon CloudWatch RUM API di monitor aplikasi.	Monitor aplikasi RUM	`AWS::RUM::AppMonitor`
Amazon S3	Aktivitas API Amazon S3 pada titik akses. Untuk informasi selengkapnya, lihat Amazon S3.	Titik Akses S3	`AWS::S3::AccessPoint`
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket tujuan umum. Untuk informasi selengkapnya, lihat Amazon S3.	S3	`AWS::S3::Object`
Titik Akses Ekspres S3	Aktivitas API pada `AWS::S3Express::AccessPoint` sumber daya.	Titik Akses Ekspres S3	`AWS::S3Express::AccessPoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket direktori . Untuk informasi selengkapnya, lihat Amazon S3.	S3 Ekspres	`AWS::S3Express::Object`
Amazon S3	Aktivitas API titik akses Objek Lambda Amazon S3, seperti panggilan ke dan. CompleteMultipartU pload GetObject Untuk informasi selengkapnya, lihat Amazon S3.	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 pada aktivitas API tingkat objek Outposts. Untuk informasi selengkap nya, lihat Amazon S3 on Outposts.	Outposts S3	`AWS::S3Outposts::Object`
Tabel Amazon S3	Aktivitas API Amazon S3 pada tabel. Untuk informasi selengkap nya, lihat Tabel Amazon S3.	Tabel S3	`AWS::S3Tables::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Tabel Amazon S3	Aktivitas API Amazon S3 pada bucket meja. Untuk informasi selengkapnya, lihat Tabel Amazon S3.	Ember meja S3	`AWS::S3Tables::TableBucket`
Vektor Amazon S3	Aktivitas API Amazon S3 pada indeks vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Indeks vektor S3	`AWS::S3Vectors::Index`
Vektor Amazon S3	Aktivitas API Amazon S3 pada bucket vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Ember vektor S3	`AWS::S3Vectors::VectorBucket`
Amazon SageMaker AI	InvokeEndpointWithResponseStream Aktivitas Amazon SageMaker AI di titik akhir. Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker titik akhir	`AWS::SageMaker::Endpoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API pada komponen percobaan percobaan . Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker komponen uji coba eksperimen metrik	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API di toko fitur.	SageMaker Toko Fitur	`AWS::SageMaker::FeatureGroup`
SageMaker hub	Aktivitas API pada `AWS::SageMaker::Hub` sumber daya.	SageMaker hub	`AWS::SageMaker::Hub`
SageMaker Lowongan	Aktivitas API pada `AWS::SageMaker::Job` sumber daya.	SageMaker Lowongan	`AWS::SageMaker::Job`
AWS SageMaker MlflowApp	Aktivitas API pada `AWS::SageMaker::MlflowApp` sumber daya.	AWS SageMaker MlflowApp	`AWS::SageMaker::MlflowApp`
Amazon SageMaker AI	Aktivitas API Amazon SageMaker AI MLFlow.	SageMaker MLFlow	`AWS::SageMaker::MlflowTrackingServer`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
SageMaker sesi pelatihan	Aktivitas API pada `AWS::SageMaker::TrainingSession` sumber daya.	SageMaker sesi pelatihan	`AWS::SageMaker::TrainingSession`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::BusinessRule` sumber daya.	AWS: :SCN:: BusinessRule	`AWS::SCN::BusinessRule`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::DataLakeException` sumber daya.	AWS: :SCN:: DataLakeException	`AWS::SCN::DataLakeException`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionInvestigation` sumber daya.	AWS: :SCN:: Exception Investigation	`AWS::SCN::ExceptionInvestigation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionRule` sumber daya.	AWS: :SCN:: Exception Rule	`AWS::SCN::ExceptionRule`
AWS Rantai Pasokan	Aktivitas API Rantai Pasokan pada sebuah instance.	Keputusan Amazon Connect	`AWS::SCN::Instance`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Metric` sumber daya.	AWS: :SCN: :M	`AWS::SCN::Metric`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::MetricEvaluation` sumber daya.	AWS: :SCN:: MetricEvaluation	`AWS::SCN::MetricEvaluation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Outcome` sumber daya.	AWS: :SCN: :H	`AWS::SCN::Outcome`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::OutcomeTemplate` sumber daya.	AWS: :SCN:: OutcomeTemplate	`AWS::SCN::OutcomeTemplate`
Amazon SimpleDB	Aktivitas API Amazon SimpleDB di domain.	Domain SimpleDB	`AWS::SDB::Domain`
AWS Cloud Map	AWS Aktivitas Cloud Map API pada namespace. Untuk informasi selengkapnya, lihat AWS Cloud Map.	AWS Ruang nama Cloud Map	`AWS::ServiceDiscovery::Namespace`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Cloud Map	AWS Aktivitas Cloud Map API pada suatu layanan. Untuk informasi selengkapnya, lihat AWS Cloud Map.	AWS Layanan Cloud Map	`AWS::ServiceDiscovery::Service`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada set konfigurasi.	Set konfigurasi SES	`AWS::SES::ConfigurationSet`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada identitas email.	Identitas SES	`AWS::SES::EmailIdentity`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada template.	Templat SES	`AWS::SES::Template`
AWS Penandatangan	Aktivitas API penandatangan saat menandatangani pekerjaan.	Pekerjaan penandatanganan penandatangan	`AWS::Signer::SigningJob`
AWS Penandatangan	Aktivitas API penandatangan pada profil penandatanganan.	Profil penandatanganan penandatangan	`AWS::Signer::SigningProfile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Asisten IoT SiteWise	Aktivitas API Asisten Sitewise pada percakapan.	Percakapan Asisten Sitewise	`AWS::SitewiseAssistant::Conversation`
Pencarian Operator	Aktivitas API pada `AWS::SMSVoice::CarrierLookup` sumber daya.	Pencarian Operator	`AWS::SMSVoice::CarrierLookup`
Set Konfigurasi	Aktivitas API pada `AWS::SMSVoice::ConfigurationSet` sumber daya.	Set Konfigurasi	`AWS::SMSVoice::ConfigurationSet`
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada pesan. Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Pesan Suara SMS	`AWS::SMSVoice::Message`
Beritahu Konfigurasi	Aktivitas API pada `AWS::SMSVoice::NotifyConfiguration` sumber daya.	Beritahu Konfigurasi	`AWS::SMSVoice::NotifyConfiguration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada identitas originasi . Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Identitas originasi SMS Voice	`AWS::SMSVoice::OriginationIdentity`
Amazon SNS	Amazon SNS Publikasikan operasi API pada titik akhir platform. Untuk informasi selengkapnya, lihat Amazon SNS.	Titik akhir platform SNS	`AWS::SNS::PlatformEndpoint`
Amazon SNS	Amazon SNS Publish dan operasi PublishBatch API pada topik. Untuk informasi selengkapnya, lihat Amazon SNS.	Topik SNS	`AWS::SNS::Topic`
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID nomor telepon. Untuk informasi selengkapnya, lihat AWS End User Messaging Sosial.	Social-Messaging ID Nomor Telepon	`AWS::SocialMessaging::PhoneNumberId`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID Waba.	Social-Messaging ID Waba	`AWS::SocialMessaging::WabaId`
Amazon SQS	Aktivitas Amazon SQS API pada pesan. Untuk informasi selengkapnya, lihat Amazon SQS.	SQS	`AWS::SQS::Queue`
AWS Systems Manager	Aktivitas API Systems Manager pada penilaian dampak.	Penilaian Dampak SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Aktivitas API Systems Manager pada node terkelola. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Node terkelola Systems Manager	`AWS::SSM::ManagedNode`
AWS Systems Manager	Aktivitas API Systems Manager pada saluran kontrol. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Step Functions	Aktivitas Step Functions API pada aktivitas. Untuk informasi selengkapnya, lihat AWS Step Functions.	Aktivitas Step Functions	`AWS::StepFunctions::Activity`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Step Functions	Aktivitas Step Functions API pada mesin state. Untuk informasi selengkapnya, lihat AWS Step Functions.	Mesin status Step Functions	`AWS::StepFunctions::StateMachine`
Amazon Support	SupportAccess Aktivitas API pada penyewa.	SupportAccess penyewa	`AWS::SupportAccess::Tenant`
Amazon Support	SupportAccess Aktivitas API pada akun yang mempercayai.	SupportAccess akun kepercayaan	`AWS::SupportAccess::TrustingAccount`
Amazon Support	SupportAccess Aktivitas API tentang peran kepercayaan.	SupportAccess peran percaya	`AWS::SupportAccess::TrustingRole`
Amazon SWF	Aktivitas API Amazon SWF di domain. Untuk informasi selengkapnya, lihat Amazon SWF.	Domain SWF	`AWS::SWF::Domain`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Perangkat.	Perangkat Klien Tipis	`AWS::ThinClient::Device`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Lingkungan.	Lingkungan Klien Tipis	`AWS::ThinClient::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Token stempel waktu	Aktivitas API pada `AWS::Timestamp::TimestampToken` sumber daya.	Token stempel waktu	`AWS::Timestamp::TimestampToken`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream di database. Untuk informasi selengkapnya, lihat Amazon Timestream.	Database Timestream	`AWS::Timestream::Database`
Amazon Timestream	Aktivitas API Amazon Timestream di titik akhir regional.	Titik akhir regional Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream pada tabel. Untuk informasi selengkapnya, lihat Amazon Timestream.	Tabel Timestream	`AWS::Timestream::Table`
Transformasi Amazon	Mengubah aktivitas API pada instance agen.	Contoh agen transformasi	`AWS::Transform::AgentInstance`
Amazon Q Transform AKA AWS Transformasi	Aktivitas API pada `AWS::Transform::Profile` sumber daya.	mengubah	`AWS::Transform::Profile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada kampanye.	Transform -Custom kampanye	`AWS::TransformCustom::Campaign`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada percakapan.	Transform -Custom percakapan	`AWS::TransformCustom::Conversation`
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada item pengetahuan.	Transform- Custom item pengetahuan	`AWS::TransformCustom::KnowledgeItem`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada paket.	Transform- Custom paket	`AWS::TransformCustom::Package`
Kustomisasi akun UXC	Aktivitas API pada `AWS::UXC::AccountCustomization` sumber daya.	Kustomisasi akun UXC	`AWS::UXC::AccountCustomization`
Izin Terverifikasi Amazon	Aktivitas API Izin Terverifikasi Amazon di toko kebijakan.	Izin Terverifikasi Amazon	`AWS::VerifiedPermissions::PolicyStore`
Well-Architected rekomendasi agen	Aktivitas API pada `AWS::WellArchitected::AgentRecommendation` sumber daya.	Well-Architected rekomendasi agen	`AWS::WellArchitected::AgentRecommendation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS X-Ray	X-Ray Aktivitas API pada jejak. Untuk informasi selengkapnya, lihat AWS X-Ray.	X-Ray jejak	`AWS::XRay::Trace`

Peristiwa data tidak dicatat secara default saat Anda membuat penyimpanan data jejak atau peristiwa. Untuk merekam peristiwa CloudTrail data, Anda harus secara eksplisit menambahkan sumber daya atau jenis sumber daya yang didukung yang ingin Anda kumpulkan aktivitasnya. Untuk informasi selengkapnya, lihat Membuat jejak dengan CloudTrail konsol dan Membuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Contoh berikut menunjukkan catatan log tunggal peristiwa data untuk tindakan Amazon SNS`Publish`.

```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

Contoh berikutnya menunjukkan catatan log tunggal dari peristiwa data untuk tindakan Amazon Cognito`GetCredentialsForIdentity`.

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```

Acara aktivitas jaringan

CloudTrail peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Peristiwa aktivitas jaringan memberikan visibilitas ke dalam operasi sumber daya yang dilakukan dalam VPC.

Anda dapat mencatat peristiwa aktivitas jaringan untuk layanan berikut:

- Amazon Aurora DSQL
- Amazon Bedrock
- ID Suara Amazon Connect
- EventBridge Penjadwal Amazon
- Amazon Fraud Detector
- Amazon HealthLake
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Langganan Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Layanan Streaming Amazon Transcribe
- Izin Terverifikasi Amazon
- Amazon WorkMail
- Platform Pengembang Anthropic Claude di AWS
- Athena
- AWS Registri Agen
- AWS AppConfig
- jaminan aws
- AWS Pertukaran Data B2B
- AWS Kalkulator Harga BCM

- AWS Penagihan
- AWS Cloud Map
- AWS Peringatan Dioda
- AWS Glue
- AWS IdentityStore Layanan
- AWS Faktur
- AWS IoT FleetWise
- AWS Terowongan Aman IoT
- AWS IoT SiteWise
- AWS License Manager
- AWS Pengukuran Pendapatan Pusat Mitra
- AWS Secrets Manager
- AWS SSO
- AWS Step Functions
- AWS Transfer Family
- AWS Transformasi
- AWSBillingAndCostManagementDataExports
- AWSLakeFormation
- Gerbang Cadangan
- Inti Agen Batuan Dasar
- API Kontrol Awan
- CloudFormation
- CloudHSM
- CloudTrail
- CodeDeploy
- Comprehend medis
- Otomatisasi Compute Optimizer
- DynamoDB
- Penskalaan Otomatis EC2
- Elastic Compute Cloud (EC2)

- Sistem File Elastis (EFS)
- pesan pengguna akhir
- IoT
- Layanan Manajemen Kunci (KMS)
- Lambda
- Relational Database Service (RDS) Core Control Plane
- Route 53 DNS Publik
- Vektor S3
- Layanan Token Keamanan (STS)
- Sign-In Portal
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- LAYANAN ANTRIAN SEDERHANA (SQS)
- Simple Storage Service (S3)
- Layanan Alur Kerja Sederhana (SWF)
- Kontak SSM
- Storage Gateway

Peristiwa aktivitas jaringan tidak dicatat secara default saat Anda membuat penyimpanan data jejak atau peristiwa. Untuk merekam peristiwa aktivitas CloudTrail jaringan, Anda harus secara eksplisit menetapkan sumber acara yang ingin Anda kumpulkan aktivitasnya. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.

Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Contoh berikut menunjukkan AWS KMS `ListKeys` peristiwa sukses yang melintasi titik akhir VPC. `vpcEndpointId`Bidang menunjukkan ID titik akhir VPC. `vpcEndpointAccountId`Kolom menunjukkan ID akun pemilik titik akhir VPC. Dalam contoh ini, permintaan dibuat oleh pemilik endpoint VPC.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE:role-name",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/role-name",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-06-04T23:10:46Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-06-04T23:12:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "requestID": "16bcc089-ac49-43f1-9177-EXAMPLE23731",
    "eventID": "228ca3c8-5f95-4a8a-9732-EXAMPLE60ed9",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "a1f3720c-ef19-47e9-a5d5-EXAMPLE8099f",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```

Contoh berikutnya menunjukkan AWS KMS `ListKeys` peristiwa yang gagal dengan pelanggaran kebijakan titik akhir VPC. Karena pelanggaran kebijakan VPC terjadi, baik `errorMessage` bidang `errorCode` dan bidang hadir. ID akun di `vpcEndpointAccountId` bidang `recipientAccountId` dan sama, yang menunjukkan peristiwa dikirim ke pemilik titik akhir VPC. `accountId`Di `userIdentity` elemen bukan`vpcEndpointAccountId`, yang menunjukkan bahwa pengguna yang membuat permintaan bukan pemilik titik akhir VPC.

```
{
```

```
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "777788889999"
    },
    "eventTime": "2024-07-15T23:57:12Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "errorCode": "VpceAccessDenied",
    "errorMessage": "The request was denied due to a VPC endpoint policy",
    "requestID": "899003b8-abc4-42bb-ad95-EXAMPLE0c374",
    "eventID": "7c6e3d04-0c3b-42f2-8589-EXAMPLE826c0",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "702f74c4-f692-4bfd-8491-EXAMPLEb1ac4",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```


Insights acara

CloudTrail Peristiwa Insights menangkap tingkat panggilan API atau aktivitas tingkat kesalahan yang tidak biasa di AWS akun Anda dengan menganalisis aktivitas CloudTrail manajemen. Peristiwa wawasan memberikan informasi yang relevan, seperti API terkait, kode kesalahan, waktu kejadian, dan statistik, yang membantu Anda memahami dan bertindak berdasarkan aktivitas yang tidak biasa. Tidak seperti jenis peristiwa lain yang ditangkap dalam penyimpanan data CloudTrail jejak atau peristiwa, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda atau pencatatan tingkat kesalahan yang berbeda secara signifikan dari pola penggunaan biasa akun. Untuk informasi selengkapnya, lihat Bekerja dengan CloudTrail Wawasan.

Contoh aktivitas yang mungkin menghasilkan peristiwa Insights meliputi:

- Akun Anda biasanya mencatat tidak lebih dari 20 panggilan `deleteBucket` API Amazon S3 per menit, tetapi akun Anda mulai mencatat rata-rata 100 panggilan `deleteBucket` API per menit. Peristiwa Insights dicatat pada awal aktivitas yang tidak biasa, dan peristiwa Insights lainnya dicatat untuk menandai akhir dari aktivitas yang tidak biasa.

- Akun Anda biasanya mencatat 20 panggilan per menit ke Amazon EC2 `AuthorizeSecurityGroupIngress` API, tetapi akun Anda mulai mencatat nol panggilan. `AuthorizeSecurityGroupIngress` Peristiwa Insights dicatat pada awal aktivitas yang tidak biasa, dan sepuluh menit kemudian, ketika aktivitas yang tidak biasa berakhir, peristiwa Insights lain dicatat untuk menandai akhir dari aktivitas yang tidak biasa.
- Akun Anda biasanya mencatat kurang dari satu `AccessDeniedException` kesalahan dalam periode tujuh hari di API. AWS Identity and Access Management `DeleteInstanceProfile` Akun Anda mulai mencatat rata-rata 12 `AccessDeniedException` kesalahan per menit pada panggilan `DeleteInstanceProfile` API. Peristiwa Insights dicatat pada awal aktivitas tingkat kesalahan yang tidak biasa, dan peristiwa Insights lainnya dicatat untuk menandai akhir aktivitas yang tidak biasa.

Contoh-contoh ini disediakan untuk tujuan ilustrasi saja. Hasil Anda dapat bervariasi tergantung pada kasus penggunaan Anda.

Untuk mencatat peristiwa CloudTrail Insights, Anda harus secara eksplisit mengaktifkan peristiwa Insights di penyimpanan data jejak atau peristiwa baru atau yang sudah ada. Untuk informasi selengkapnya tentang membuat jejak, lihatMembuat jejak dengan CloudTrail konsol. Untuk informasi selengkapnya tentang membuat penyimpanan data acara, lihatMembuat penyimpanan data acara untuk acara Insights dengan konsol.

Biaya tambahan berlaku untuk acara Insights. Anda akan dikenakan biaya secara terpisah jika Anda mengaktifkan Wawasan untuk penyimpanan data jalur dan acara. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Ada dua peristiwa yang dicatat untuk menunjukkan aktivitas yang tidak biasa di CloudTrail Wawasan: acara mulai dan acara akhir. Contoh berikut menunjukkan catatan log tunggal dari peristiwa Wawasan awal yang terjadi ketika Application Auto Scaling `CompleteLifecycleAction` API dipanggil beberapa kali yang tidak biasa. Untuk acara Wawasan, nilainya `eventCategory` adalah`Insight`. `insightDetails`Blok mengidentifikasi status peristiwa, sumber, nama, jenis Wawasan, dan konteks, termasuk statistik dan atribusi. Untuk informasi lebih lanjut tentang `insightDetails` blok, lihatCloudTrail merekam konten untuk acara Insights untuk jalur.


```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
```

```
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
```

```
                }],
                "baseline": [{
                    "value": "codedeploy.amazonaws.com",
                    "average": 9.82222E-5
                }]
            }, {
                "attribute": "errorCode",
                "insight": [{
                    "value": "null",
                    "average": 5.0
                }],
                "baseline": [{
                    "value": "null",
                    "average": 9.82222E-5
                }]
            }]
        }
    },
    "eventCategory": "Insight"
}
```

Mencatat log peristiwa manajemen

Secara default, jejak dan data peristiwa menyimpan peristiwa manajemen log dan tidak menyertakan data atau peristiwa Wawasan.

Biaya tambahan berlaku untuk data atau acara Wawasan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Daftar Isi

- Peristiwa manajemen
- Membaca dan menulis acara
- Pencatatan acara manajemen dengan Konsol Manajemen AWS
  - Memperbarui pengaturan acara manajemen untuk jejak yang ada
  - Memperbarui pengaturan acara manajemen untuk penyimpanan data acara yang ada
- Pencatatan acara manajemen dengan AWS CLI
  - Contoh: Acara manajemen pencatatan untuk jalur
    - Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan penyeleksi acara tingkat lanjut

    - Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan pemilih acara dasar
  - Contoh: Logging acara manajemen untuk penyimpanan data acara
    - Contoh: Kecualikan AWS KMS acara manajemen
    - Contoh: Kecualikan acara manajemen Amazon RDS
    - Contoh: Kecualikan Layanan AWS peristiwa dan peristiwa dari Konsol Manajemen AWS sidang
    - Contoh: Kecualikan peristiwa manajemen untuk identitas IAM tertentu
- Pencatatan acara manajemen dengan AWS SDK

Peristiwa manajemen

Acara manajemen memberikan visibilitas ke dalam operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi bidang kontrol. Contoh acara manajemen meliputi:

- Mengkonfigurasi keamanan (misalnya, operasi `AttachRolePolicy` API IAM)
- Mendaftarkan perangkat (misalnya, operasi `CreateDefaultVpc` API Amazon EC2)
- Mengonfigurasi aturan untuk merutekan data (misalnya, operasi Amazon `CreateSubnet` EC2 API)
- Menyiapkan logging (misalnya, operasi AWS CloudTrail `CreateTrail` API)

Peristiwa manajemen juga dapat mencakup peristiwa non-API yang terjadi di akun Anda. Misalnya, ketika pengguna masuk ke akun Anda, CloudTrail mencatat `ConsoleLogin` peristiwa tersebut. Untuk informasi selengkapnya, lihat Peristiwa non-API yang ditangkap oleh CloudTrail.

Secara default, jejak dan penyimpanan data peristiwa dikonfigurasi untuk mencatat peristiwa manajemen.

> **Note**
>
> Fitur Riwayat CloudTrail acara hanya mendukung acara manajemen. Anda tidak dapat mengecualikan AWS KMS atau peristiwa Amazon RDS Data API dari riwayat Peristiwa; pengaturan yang Anda terapkan ke penyimpanan data jejak atau peristiwa tidak berlaku

untuk riwayat Peristiwa. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.

Membaca dan menulis acara

Saat mengonfigurasi penyimpanan data jejak atau peristiwa untuk mencatat peristiwa manajemen, Anda dapat menentukan apakah Anda menginginkan peristiwa hanya-baca, peristiwa hanya-tulis, atau keduanya.

- Baca

  Read-only event mencakup operasi API yang membaca sumber daya Anda, tetapi tidak membuat perubahan. Misalnya, peristiwa hanya-baca mencakup operasi API `DescribeSecurityGroups` dan `DescribeSubnets` Amazon EC2. Operasi ini hanya menampilkan informasi tentang sumber daya Amazon EC2 Anda dan tidak mengubah konfigurasi Anda.

- Menulis

  Write-only event mencakup operasi API yang memodifikasi (atau mungkin memodifikasi) sumber daya Anda. Misalnya, operasi API `RunInstances` dan `TerminateInstances` Amazon EC2 memodifikasi instans Anda.

Contoh: Mencatat peristiwa baca dan tulis untuk jalur terpisah

Contoh berikut menunjukkan cara mengonfigurasi jejak untuk membagi aktivitas log untuk akun menjadi bucket S3 terpisah: satu bucket menerima peristiwa hanya-baca dan bucket kedua menerima peristiwa hanya-tulis.

1. Anda membuat jejak dan memilih bucket S3 bernama `amzn-s3-demo-bucket1` untuk menerima file log. Anda kemudian memperbarui jejak untuk menentukan bahwa Anda ingin Baca acara manajemen.
2. Anda membuat jejak kedua dan memilih bucket S3 bernama `amzn-s3-demo-bucket2` untuk menerima file log. Anda kemudian memperbarui jejak untuk menentukan bahwa Anda ingin menulis acara manajemen.
3. Operasi Amazon EC2 `DescribeInstances` dan `TerminateInstances` API terjadi di akun Anda.

4. Operasi `DescribeInstances` API adalah peristiwa hanya-baca dan cocok dengan pengaturan untuk jejak pertama. Jejak mencatat dan mengirimkan acara keamzn-s3-demo-bucket1.
5. Operasi `TerminateInstances` API adalah acara khusus tulis dan cocok dengan pengaturan untuk jejak kedua. Jejak mencatat dan mengirimkan acara keamzn-s3-demo-bucket2.

Pencatatan acara manajemen dengan Konsol Manajemen AWS

Bagian ini menjelaskan cara memperbarui pengaturan acara manajemen untuk penyimpanan data jejak atau peristiwa yang ada.

Topik

- Memperbarui pengaturan acara manajemen untuk jejak yang ada
- Memperbarui pengaturan acara manajemen untuk penyimpanan data acara yang ada

Memperbarui pengaturan acara manajemen untuk jejak yang ada

Gunakan prosedur berikut untuk memperbarui pengaturan acara manajemen untuk jejak yang ada.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Buka halaman Trails CloudTrail konsol dan pilih nama jejak.
3. Untuk acara Manajemen, pilih Edit.
   - Pilih apakah Anda ingin mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.
   - Pilih Kecualikan AWS KMS acara untuk memfilter AWS Key Management Service (AWS KMS) peristiwa dari Trail Anda. Pengaturan default adalah untuk memasukkan semua AWS KMS acara.

     Opsi untuk mencatat atau mengecualikan AWS KMS peristiwa hanya tersedia jika Anda mencatat peristiwa manajemen di jejak Anda. Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan AWS KMS peristiwa.

     AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Low-volume, AWS KMS tindakan yang relevan seperti`Disable`,`Delete`,

dan `ScheduleKey` (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

Untuk mengecualikan peristiwa bervolume tinggi seperti`Encrypt`,`Decrypt`, dan`GenerateDataKey`, tetapi masih mencatat peristiwa yang relevan seperti`Disable`, `Delete` dan`ScheduleKey`, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa.

- Pilih Kecualikan peristiwa Amazon RDS Data API untuk memfilter peristiwa Amazon Relational Database Service Data Data API dari jejak Anda. Pengaturan default adalah untuk menyertakan semua peristiwa Amazon RDS Data API. Untuk informasi selengkapnya tentang peristiwa Amazon RDS Data API, lihat Pencatatan panggilan API Data dengan AWS CloudTrail di Panduan Pengguna Amazon RDS untuk Aurora.

4. Pilih Simpan perubahan setelah Anda selesai.

Memperbarui pengaturan acara manajemen untuk penyimpanan data acara yang ada

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Buka halaman penyimpanan data acara CloudTrail konsol dan pilih nama penyimpanan data acara.
3. Untuk acara Manajemen, pilih Edit lalu konfigurasikan pengaturan berikut:

   a. Pilih antara koleksi acara Simple atau Advanced event collection:

      - Pilih koleksi acara sederhana jika Anda ingin mencatat semua peristiwa, hanya mencatat peristiwa yang dibaca, atau hanya mencatat peristiwa tulis. Anda dapat memilih juga untuk mengecualikan AWS Key Management Service dan peristiwa manajemen Amazon RDS Data API.
      - Pilih Koleksi acara lanjutan jika Anda ingin menyertakan atau mengecualikan acara manajemen berdasarkan nilai bidang pemilih acara lanjutan, termasuk,`eventName`, `eventTypeeventSource`, dan `userIdentity.arn` bidang.

   b. Jika Anda memilih koleksi acara sederhana, pilih apakah Anda ingin mencatat semua peristiwa, hanya mencatat peristiwa yang dibaca, atau hanya mencatat peristiwa tulis. Anda juga dapat memilih untuk mengecualikan AWS KMS dan acara manajemen Amazon RDS.

   c. Jika Anda memilih koleksi acara lanjutan, buat pilihan berikut:

i. Di template pemilih Log, pilih templat yang telah ditentukan sebelumnya, atau Kustom untuk membuat konfigurasi khusus berdasarkan nilai bidang pemilih acara lanjutan.

   Anda dapat memilih dari template yang telah ditentukan berikut:

   - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
   - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
   - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa.
   - Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
   - Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` of`AwsServiceEvent`, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).

ii. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih acara lanjutan, seperti “Acara manajemen log dari Konsol Manajemen AWS sesi”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

iii. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih acara lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

   A. Pilih dari bidang berikut.

- **`readOnly`**— `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Ketika disetel ke`false`, data peristiwa menyimpan peristiwa Write-only manajemen log. Read-only peristiwa manajemen adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa. Untuk mencatat peristiwa Baca dan Tulis, jangan tambahkan `readOnly` pemilih.
- **`eventName`**— `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara manajemen apa pun, seperti `CreateAccessPoint` atau`GetAccessPoint`.
- **`userIdentity.arn`**— Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`sessionCredentialFromConsole`**— Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- **`eventSource`**— Anda dapat menggunakannya untuk memasukkan atau mengecualikan sumber acara tertentu. `eventSource`Ini biasanya merupakan bentuk pendek dari nama layanan tanpa spasi plus`.amazonaws.com`. Misalnya, Anda dapat `eventSource` menyetel sama dengan `ec2.amazonaws.com` untuk hanya mencatat peristiwa pengelolaan Amazon EC2.
- **`eventType`**- EventType untuk menyertakan atau mengecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk mengecualikan Layanan AWS peristiwa.

B. Untuk setiap bidang, pilih + Kondisi untuk menambahkan kondisi sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua kondisi.

   Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua

pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

C. Pilih + Bidang untuk menambahkan bidang tambahan sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

iv. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

d. Pilih Aktifkan tangkapan peristiwa Wawasan untuk mengaktifkan Wawasan. Untuk mengaktifkan Wawasan, Anda perlu menyiapkan penyimpanan data acara tujuan untuk mengumpulkan peristiwa Wawasan berdasarkan aktivitas acara manajemen di penyimpanan data acara ini.

Jika Anda memilih untuk mengaktifkan Wawasan, lakukan hal berikut.

i. Pilih toko acara tujuan yang akan mencatat peristiwa Wawasan. Penyimpanan data acara tujuan akan mengumpulkan peristiwa Wawasan berdasarkan aktivitas acara manajemen di penyimpanan data acara ini. Untuk informasi tentang cara membuat penyimpanan data acara tujuan, lihatUntuk membuat penyimpanan data peristiwa tujuan yang mencatat peristiwa Insights.

ii. Pilih jenis Wawasan. Anda dapat memilih API call rate, API error rate, atau keduanya. Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Insights untuk tingkat panggilan API. Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.

4. Pilih Simpan perubahan setelah Anda selesai.

Pencatatan acara manajemen dengan AWS CLI

Anda dapat mengonfigurasi jejak atau penyimpanan data peristiwa untuk mencatat peristiwa manajemen menggunakan file. AWS CLI

Topik

- Contoh: Acara manajemen pencatatan untuk jalur
- Contoh: Logging acara manajemen untuk penyimpanan data acara

Contoh: Acara manajemen pencatatan untuk jalur

Untuk melihat apakah jejak Anda mencatat peristiwa manajemen, jalankan `get-event-selectors` perintah.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

Contoh berikut mengembalikan pengaturan default untuk jejak. Secara default, jejak mencatat semua peristiwa manajemen, mencatat peristiwa dari semua sumber peristiwa, dan tidak mencatat peristiwa data.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

Anda dapat menggunakan pemilih acara dasar atau lanjutan untuk mencatat peristiwa manajemen. Anda tidak dapat menerapkan pemilih peristiwa dan pemilih peristiwa lanjutan untuk satu jejak. Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa. Bagian berikut memberikan contoh cara mencatat peristiwa manajemen menggunakan pemilih acara lanjutan dan pemilih acara dasar.

Topik

- Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan penyeleksi acara tingkat lanjut
- Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan pemilih acara dasar

Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan penyeleksi acara tingkat lanjut

Contoh berikut membuat pemilih peristiwa lanjutan untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen hanya-baca dan hanya tulis (dengan menghilangkan `readOnly` pemilih), tetapi untuk mengecualikan () peristiwa. AWS Key Management Service AWS KMS Karena AWS KMS peristiwa diperlakukan sebagai peristiwa manajemen, dan mungkin ada volume yang tinggi, mereka dapat memiliki dampak besar pada CloudTrail tagihan Anda jika Anda memiliki lebih dari satu jejak yang menangkap peristiwa manajemen.

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, AWS KMS peristiwa tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan AWS KMS peristiwa.

Untuk mulai mencatat AWS KMS peristiwa ke jejak lagi, hapus `eventSource` pemilih, dan jalankan perintah lagi.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
```

```
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat peristiwa yang dikecualikan ke jejak lagi, hapus `eventSource` pemilih, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Contoh berikutnya membuat pemilih peristiwa lanjutan untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen hanya-baca dan hanya-tulis (dengan menghilangkan `readOnly` pemilih), tetapi untuk mengecualikan peristiwa manajemen Amazon RDS Data API. Untuk mengecualikan peristiwa pengelolaan Amazon RDS Data API, tentukan sumber peristiwa Amazon RDS Data API dalam nilai string untuk `eventSource` bidang:. `rdsdata.amazonaws.com`

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, peristiwa manajemen Amazon RDS Data API tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan peristiwa Amazon RDS Data API.

Untuk mulai mencatat peristiwa pengelolaan Amazon RDS Data API ke jejak lagi, hapus `eventSource` pemilih, dan jalankan perintah lagi.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
```

```
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk mulai mencatat peristiwa yang dikecualikan ke jejak lagi, hapus `eventSource` pemilih, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

Contoh: Mencatat peristiwa manajemen untuk jalur menggunakan pemilih acara dasar

Untuk mengonfigurasi jejak Anda untuk mencatat peristiwa manajemen, jalankan `put-event-selectors` perintah. Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk

menyertakan semua peristiwa manajemen untuk dua objek S3. Anda dapat menentukan dari 1 hingga 5 penyeleksi acara untuk jejak. Anda dapat menentukan dari 1 hingga 250 sumber daya data untuk jejak.

> **Note**
>
> Jumlah maksimum sumber daya data S3 adalah 250, terlepas dari jumlah pemilih acara.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-demo-bucket/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2"] }] }]'
```

Contoh berikut mengembalikan pemilih acara dikonfigurasi untuk jejak.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

Untuk mengecualikan AWS Key Management Service (AWS KMS) peristiwa dari log jejak, jalankan `put-event-selectors` perintah dan tambahkan atribut `ExcludeManagementEventSources` dengan nilai`kms.amazonaws.com`. Contoh berikut membuat pemilih acara untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen hanya-baca dan hanya tulis, tetapi

mengecualikan peristiwa. AWS KMS Karena AWS KMS dapat menghasilkan volume peristiwa yang tinggi, pengguna dalam contoh ini mungkin ingin membatasi peristiwa untuk mengelola biaya jejak.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

Contoh mengembalikan pemilih acara yang dikonfigurasi untuk jejak.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Untuk mengecualikan peristiwa pengelolaan Amazon RDS Data API dari log jejak, jalankan `put-event-selectors` perintah dan tambahkan atribut `ExcludeManagementEventSources` dengan nilai`rdsdata.amazonaws.com`. Contoh berikut membuat pemilih peristiwa untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen hanya-baca dan hanya-tulis, tetapi mengecualikan peristiwa manajemen Amazon RDS Data API. Karena Amazon RDS Data API dapat menghasilkan volume peristiwa manajemen yang tinggi, pengguna dalam contoh ini mungkin ingin membatasi peristiwa untuk mengelola biaya jejak.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
```

```
        }
    ]
}
```

Untuk memulai logging AWS KMS atau peristiwa pengelolaan Amazon RDS Data API ke jejak lagi, teruskan string kosong sebagai nilai`ExcludeManagementEventSources`, seperti yang ditunjukkan pada perintah berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Untuk mencatat AWS KMS peristiwa yang relevan ke jejak seperti`Disable`, `Delete` dan`ScheduleKey`, tetapi mengecualikan AWS KMS peristiwa volume tinggi seperti`Encrypt`,`Decrypt`, dan`GenerateDataKey`, mencatat peristiwa manajemen khusus tulis, dan menyimpan pengaturan default untuk mencatat AWS KMS peristiwa, seperti yang ditunjukkan pada contoh berikut.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

Contoh: Logging acara manajemen untuk penyimpanan data acara

Anda mencatat peristiwa manajemen untuk penyimpanan data peristiwa dengan mengonfigurasi pemilih acara lanjutan.

Bidang pemilih peristiwa lanjutan berikut didukung untuk peristiwa manajemen pencatatan pada penyimpanan data acara:

- **`eventCategory`**— Anda harus menetapkan `eventCategory` sama `Management` dengan peristiwa manajemen log. Bidang ini harus diisi.
- **`readOnly`**— `readOnly` dapat diatur `Equals` ke nilai `true` atau`false`. Ketika disetel ke`false`, data peristiwa menyimpan peristiwa Write-only manajemen log. Read-only peristiwa manajemen adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,`Delete*`, atau `Write*` peristiwa. Untuk mencatat peristiwa Baca dan Tulis, jangan tambahkan `readOnly` pemilih.

- **`eventName`**— `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara manajemen apa pun, seperti `CreateAccessPoint` atau`GetAccessPoint`. Anda dapat menggunakan operator apa pun dengan bidang ini.
- **`userIdentity.arn`**— Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`sessionCredentialFromConsole`**— Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke Sama atau `NotEquals` dengan nilai. `true`
- **`eventSource`**— Anda dapat menggunakannya untuk memasukkan atau mengecualikan sumber acara tertentu. `eventSource`Ini biasanya merupakan bentuk pendek dari nama layanan tanpa spasi plus`.amazonaws.com`. Misalnya, Anda dapat mengatur `eventSource Equals` `ec2.amazonaws.com` untuk hanya mencatat peristiwa manajemen Amazon EC2.
- **`eventType`**- EventType untuk menyertakan atau mengecualikan. Misalnya, Anda dapat mengatur bidang ini `NotEquals` `AwsServiceEvent` untuk mengecualikan Layanan AWS peristiwa. Anda dapat menggunakan operator apa pun dengan bidang ini.

Untuk melihat apakah penyimpanan data acara Anda menyertakan peristiwa manajemen, jalankan get-event-data-store perintah.

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

Berikut ini adalah contoh respons. Pembuatan dan waktu pembaruan terakhir dalam `timestamp` format.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
```

```
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

Untuk membuat penyimpanan data acara yang mencakup semua peristiwa manajemen, Anda menjalankan create-event-data-store perintah. Anda tidak perlu menentukan pemilih acara lanjutan untuk menyertakan semua acara manajemen.

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

Contoh:

- Contoh: Kecualikan AWS KMS acara manajemen
- Contoh: Kecualikan acara manajemen Amazon RDS
- Contoh: Kecualikan Layanan AWS peristiwa dan peristiwa dari Konsol Manajemen AWS sidang
- Contoh: Kecualikan peristiwa manajemen untuk identitas IAM tertentu

Contoh: Kecualikan AWS KMS acara manajemen

Untuk membuat penyimpanan data peristiwa yang mengecualikan AWS Key Management Service (AWS KMS) peristiwa, jalankan `create-event-data-store` perintah dan tentukan yang `eventSource` tidak sama`kms.amazonaws.com`. Contoh berikut membuat penyimpanan data peristiwa yang mencakup peristiwa manajemen hanya-baca dan hanya tulis, tetapi mengecualikan peristiwa. AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
```

```
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Contoh: Kecualikan acara manajemen Amazon RDS

Untuk membuat penyimpanan data peristiwa yang mengecualikan peristiwa manajemen Amazon RDS Data API, jalankan `create-event-data-store` perintah dan tentukan yang `eventSource` tidak sama. `rdsdata.amazonaws.com` Contoh berikut membuat penyimpanan data peristiwa yang menyertakan peristiwa manajemen hanya-baca dan hanya-tulis, tetapi mengecualikan peristiwa Amazon RDS Data API.

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
```

```
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Contoh: Kecualikan Layanan AWS peristiwa dan peristiwa dari Konsol Manajemen AWS sidang

Contoh berikut membuat penyimpanan data peristiwa yang mencatat peristiwa manajemen tetapi mengecualikan peristiwa dan Layanan AWS peristiwa yang berasal dari Konsol Manajemen AWS sesi.

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude Layanan AWS and console events",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventType","NotEquals": ["AwsServiceEvent"]},
            {"Field": "sessionCredentialFromConsole","NotEquals": ["true"]}
        ]
    }
]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Exclude Layanan AWS and console events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                },
                {
                    "Field": "sessionCredentialFromConsole",
```

```
                    "NotEquals": [
                        "true"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

Contoh: Kecualikan peristiwa manajemen untuk identitas IAM tertentu

Contoh berikut membuat penyimpanan data peristiwa yang mencatat peristiwa manajemen tetapi mengecualikan peristiwa yang dihasilkan oleh. `bucket-scanner-role` `userIdentity`

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude events generated by bucket-scanner-role userIdentity",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "userIdentity.arn","NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

Berikut ini adalah contoh respons.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
```

```
            "Name": "Exclude events generated by bucket-scanner-role userIdentity",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

Pencatatan acara manajemen dengan AWS SDK

Gunakan GetEventSelectorsoperasi untuk melihat apakah jejak Anda mencatat peristiwa manajemen untuk jejak. Anda dapat mengonfigurasi jejak Anda untuk mencatat peristiwa manajemen dengan PutEventSelectorsoperasi. Untuk informasi lebih lanjut, lihat Referensi API AWS CloudTrail.

Jalankan GetEventDataStoreoperasi untuk melihat apakah penyimpanan data acara Anda menyertakan acara manajemen. Anda dapat mengonfigurasi penyimpanan data acara Anda untuk menyertakan peristiwa manajemen dengan menjalankan CreateEventDataStoreatau UpdateEventDataStoreoperasi. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI dan Referensi AWS CloudTrail API.

Mencatat log peristiwa data

Bagian ini menjelaskan cara mencatat peristiwa data menggunakan CloudTrail konsol dan AWS CLI.

Secara default, jejak dan penyimpanan data peristiwa tidak mencatat peristiwa data. Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya. Ini juga dikenal sebagai operasi pesawat data. Peristiwa data sering kali merupakan aktivitas bervolume tinggi.

Contoh peristiwa data meliputi:

- Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject`, `DeleteObject`, dan operasi `PutObject` API) pada objek di bucket S3.
- AWS Lambda aktivitas eksekusi fungsi (`Invoke`API).
- CloudTrail `PutAuditEvents`aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS.
- Operasi Amazon SNS `Publish`dan `PublishBatch`API pada topik.

Anda dapat menggunakan penyeleksi acara lanjutan untuk membuat penyeleksi berbutir halus, yang membantu Anda mengontrol biaya dengan hanya mencatat peristiwa tertentu yang menarik untuk kasus penggunaan Anda. Misalnya, Anda dapat menggunakan pemilih peristiwa lanjutan untuk mencatat panggilan API tertentu dengan menambahkan filter di `eventName` bidang. Untuk informasi selengkapnya, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut.

> **Note**
>
> Peristiwa yang dicatat oleh jejak Anda tersedia di Amazon EventBridge. Misalnya, jika Anda memilih untuk mencatat peristiwa data untuk objek S3 tetapi tidak mengelola peristiwa, jejak Anda memproses dan mencatat peristiwa data hanya untuk objek S3 yang ditentukan. Peristiwa data untuk objek S3 ini tersedia di Amazon EventBridge. Untuk informasi selengkapnya, lihat peristiwa AWS layanan yang dikirimkan melalui CloudTrail Panduan EventBridge Pengguna Amazon dan Referensi AWS Acara.

Daftar Isi

- Peristiwa data
  - Peristiwa data yang didukung oleh AWS CloudTrail
  - Contoh: Mencatat peristiwa data untuk objek Amazon S3

- Mencatat peristiwa data untuk objek S3 di objek lain AWS rekening
- Read-only dan acara khusus tulis
- Mencatat peristiwa data dengan Konsol Manajemen AWS
- Mencatat peristiwa data dengan AWS Command Line Interface
  - Mencatat peristiwa data untuk jejak dengan AWS CLI
    - Log peristiwa data untuk jejak dengan menggunakan pemilih acara tingkat lanjut
    - Catat semua peristiwa Amazon S3 untuk bucket Amazon S3 dengan menggunakan pemilih acara lanjutan
    - Masuk Amazon S3 AWS Outposts acara dengan menggunakan penyeleksi acara tingkat lanjut
    - Log peristiwa dengan menggunakan pemilih acara dasar
  - Pencatatan peristiwa data untuk menyimpan data acara dengan AWS CLI
    - Sertakan semua acara Amazon S3 untuk bucket tertentu
    - Sertakan Amazon S3 di AWS Outposts peristiwa
- Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut
  - Bagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang
    - Contoh yang menunjukkan beberapa kondisi untuk bidang Resources.arn
  - AWS CLI contoh untuk memfilter peristiwa data
    - Contoh 1: Pemfilteran pada bidang EventName
    - Contoh 2: Memfilter pada bidang Resources.arn dan pengguna Identity.arn
    - Contoh 3: Memfilter pada bidang resources.type dan eventName untuk mengecualikan objek individual yang dihapus oleh peristiwa Amazon S3 DeleteObjects
    - Contoh 4: Memfilter pada bidang EventSource untuk mengecualikan peristiwa data siklus hidup Amazon S3
    - Contoh 5: Memfilter pada bidang EventSource untuk mengecualikan peristiwa data kegagalan autentikasi Amazon S3
- Mengagregasikan peristiwa data
  - Mengaktifkan agregasi untuk peristiwa data menggunakan konsol
  - Mengaktifkan agregasi untuk peristiwa data menggunakan AWS CLI
    - Contoh: peristiwa agregat API_ACTIVITY
    - Contoh: RESOURCE_ACCESS peristiwa agregat

- Peristiwa data pencatatan untuk AWS Config kepatuhan
- Mencatat peristiwa data dengan AWS SDK
- Menekan peristiwa rekursif dengan logging rekursif
  - Apa itu logging rekursif?
  - Cara kerja penekanan logging rekursif
  - Mengkonfigurasi logging rekursif
    - Menonaktifkan logging rekursif (menekan peristiwa rekursif)
    - Re-enabling pencatatan rekursif
  - Perilaku default

Peristiwa data

Tabel berikut menunjukkan jenis sumber daya yang tersedia untuk jejak dan penyimpanan data peristiwa. Kolom tipe sumber daya (konsol) menunjukkan pilihan yang sesuai di konsol. Kolom nilai resources.type menunjukkan `resources.type` nilai yang akan Anda tentukan untuk menyertakan peristiwa data dari jenis tersebut di penyimpanan data jejak atau peristiwa Anda menggunakan API atau. AWS CLI CloudTrail

Untuk jejak, Anda dapat menggunakan pemilih peristiwa dasar atau lanjutan untuk mencatat peristiwa data untuk objek Amazon S3 di bucket tujuan umum, fungsi Lambda, dan tabel DynamoDB (ditampilkan dalam tiga baris pertama tabel). Anda hanya dapat menggunakan pemilih acara lanjutan untuk mencatat jenis sumber daya yang ditampilkan di baris yang tersisa.

Untuk penyimpanan data acara, Anda hanya dapat menggunakan pemilih acara lanjutan untuk menyertakan peristiwa data.

Peristiwa data yang didukung oleh AWS CloudTrail

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
OMWDevice CommunicationService	Aktivitas API pada `AWS::Account::ControlledDomain` sumber daya.	AWS: :Akun:: ControlledDomain	`AWS::Account::ControlledDomain`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
WorkSpaces Aplikasi Amazon	Agen mengakses acara alat MCP WorkSpaces Aplikasi	Alat MCP Akses Agen	`AWS::AgentAccessMCP::Tools`
AWS Registri Agen	Aktivitas API pada `AWS::AgentRegistry::Registry` sumber daya.	AWS Registri Agen	`AWS::AgentRegistry::Registry`
Amazon AIDevOps	AIDevOps Aktivitas API pada ruang agen.	Agen Ruang	`AWS::AIDevOps::AgentSpace`
Amazon AIDevOps	AIDevOps Aktivitas API pada asosiasi.	AIDevOps asosiasi	`AWS::AIDevOps::Association`
Amazon AIDevOps	AIDevOps Aktivitas API di tim aplikasi operator.	AIDevOps tim aplikasi operator	`AWS::AIDevOps::OperatorAppTeam`
Amazon AIDevOps	AIDevOps Aktivitas API pada metadata pipeline.	AIDevOps Metadata Pipa	`AWS::AIDevOps::PipelineMetadata`
Amazon AIDevOps	AIDevOps Aktivitas API pada layanan.	AIDevOps layanan	`AWS::AIDevOps::Service`
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada investigasi operasional. Untuk informasi selengkapnya, lihat Pengembang Amazon Q.	Grup Investigasi AIOps	`AWS::AIOps::InvestigationGroup`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Tanpa OpenSearch Server	Aktivitas API pada `AWS::AOSS::Collection` sumber daya.	AWS: :AOSS: :I	`AWS::AOSS::Collection`
AWS AppConfig	AWS AppConfig Aktivitas API untuk operasi konfigurasi seperti panggilan ke StartConfigurationSession dan GetLatestConfiguration. Untuk informasi selengkapnya, lihat AWS AppConfig.	AWS AppConfig	`AWS::AppConfig::Configuration`
CloudWatch Sinyal Aplikasi	Aktivitas API pada `AWS::ApplicationSignals::InstrumentationConfig` sumber daya.	AWS::ApplicationSignals::InstrumentationConfig	`AWS::ApplicationSignals::InstrumentationConfig`
AWS AppSync	AWS AppSync Aktivitas API pada AppSync GraphQL API. Untuk informasi selengkapnya, lihat AWS AppSync.	AppSync GraphQL	`AWS::AppSync::GraphQLApi`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Ruang kerja antropik eksternal	Aktivitas API pada `AWS::AWSExternalAnthropic::Workspace` sumber daya.	Ruang kerja antropik eksternal	`AWS::AWSExternalAnthropic::Workspace`
AWS Pertukaran Data B2B	Aktivitas API Pertukaran Data B2B untuk operasi Transformer seperti panggilan ke dan. GetTransformerJob StartTransformerJob	Pertukaran Data B2B	`AWS::B2BI::Transformer`
AWS Titik akses Backup	Aktivitas API pada `AWS::Backup::BackupAccessPoint` sumber daya.	AWS Titik akses Backup	`AWS::Backup::BackupAccessPoint`
AWS Backup	AWS Aktivitas Backup Search Data API pada pekerjaan pencarian.	AWS API Data Pencarian Cadangan	`AWS::Backup::SearchJob`
Amazon Bedrock	Aktivitas API dasar pada pekerjaan prompt optimasi lanjutan.	AdvancedOptimizePromptJob	`AWS::Bedrock::AdvancedOptimizePromptJob`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias agen. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Alias agen batuan dasar	`AWS::Bedrock::AgentAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada pemanggilan asinkron.	Pemanggilan asinkron batuan dasar	`AWS::Bedrock::AsyncInvoke`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada kebijakan penalaran otomatis.	Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicy`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada versi kebijakan penalaran otomatis.	Versi Kebijakan Penalaran Otomatis Batuan Dasar	`AWS::Bedrock::AutomatedReasoningPolicyVersion`
Amazon Bedrock	Aktivitas API cetak biru Amazon Bedrock.	Cetak biru batuan dasar	`AWS::Bedrock::Blueprint`
Amazon Bedrock	Aktivitas API pemanggilan otomatisasi data batuan dasar.	Pemanggilan Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationInvocation`
Amazon Bedrock	Aktivitas API profil otomatisasi data Amazon Bedrock.	Profil Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProfile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API proyek otomatisasi data Amazon Bedrock.	Proyek Otomasi Data Batuan Dasar	`AWS::Bedrock::DataAutomationProject`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias flow.	Alias aliran batuan dasar	`AWS::Bedrock::FlowAlias`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada eksekusi aliran.	Eksekusi Aliran	`AWS::Bedrock::FlowExecution`
Amazon Bedrock	Aktivitas Amazon Bedrock API di pagar pembatas.	Pagar pembatas batuan dasar	`AWS::Bedrock::Guardrail`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada agen inline.	Memohon Batuan Dasar Inline-Agent	`AWS::Bedrock::InlineAgent`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada basis pengetahuan. Untuk informasi selengkapnya, lihat Amazon Bedrock.	Basis pengetahuan batuan dasar	`AWS::Bedrock::KnowledgeBase`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada model.	Model batuan dasar	`AWS::Bedrock::Model`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada prompt.	Permintaan batuan dasar	`AWS::Bedrock::PromptVersion`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas Amazon Bedrock API pada sesi.	Sesi batuan dasar	`AWS::Bedrock::Session`
Amazon Bedrock	Aktivitas API Amazon Bedrock Tool.	Alat Batuan Dasar	`AWS::Bedrock::Tool`
Bedrock-AgentCore ABTest	Aktivitas API pada `AWS::BedrockAgentCore::ABTest` sumber daya.	Bedrock-AgentCore ABTest	`AWS::BedrockAgentCore::ABTest`
Amazon Bedrock	Aktivitas API Amazon Bedrock ApiKey CredentialProvider .	Bedrock-AgentCore apiKey CredentialProvider	`AWS::BedrockAgentCore::APIKeyCredentialProvider`
BedrockAgentCore evaluasi batch	Aktivitas API pada `AWS::BedrockAgentCore::BatchEvaluate` sumber daya.	BedrockAgentCore evaluasi batch	`AWS::BedrockAgentCore::BatchEvaluate`
Amazon Bedrock	Aktivitas API Browser Amazon Bedrock.	Bedrock-AgentCore Browser	`AWS::BedrockAgentCore::Browser`
Amazon Bedrock	Aktivitas Amazon Bedrock Browser-Custom API.	Bedrock-AgentCore Browser-Custom	`AWS::BedrockAgentCore::BrowserCustom`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Bedrock-AgentCore Profil Browser	Aktivitas API pada `AWS::BedrockAgentCore::BrowserProfile` sumber daya.	Bedrock-AgentCore Profil Browser	`AWS::BedrockAgentCore::BrowserProfile`
BedrockAgentCore CapacityProvider	Aktivitas API pada `AWS::BedrockAgentCore::CapacityProvider` sumber daya.	BedrockAgentCore CapacityProvider	`AWS::BedrockAgentCore::CapacityProvider`
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter API.	Bedrock-AgentCore Code-Interpreter	`AWS::BedrockAgentCore::CodeInterpreter`
Amazon Bedrock	Aktivitas Amazon Bedrock Code-Interpreter-Custom API.	Bedrock-AgentCore Code-Interpreter-Custom	`AWS::BedrockAgentCore::CodeInterpreterCustom`
Batuan Dasar Amazon AgentCore	Aktivitas AgentCore API batuan dasar pada evaluator.	Bedrock-AgentCore Penilai	`AWS::BedrockAgentCore::Evaluator`
Amazon Bedrock	Aktivitas API Amazon Bedrock Gateway.	Bedrock-AgentCore Gerbang	`AWS::BedrockAgentCore::Gateway`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Memori Amazon Bedrock.	Bedrock-AgentCore Memori	`AWS::BedrockAgentCore::Memory`
Amazon Bedrock	Aktivitas API Amazon Bedrock Oauth2 CredentialProvider .	Bedrock-AgentCore Oauth2 CredentialProvider	`AWS::BedrockAgentCore::OAuth2CredentialProvider`
Bedrock-AgentCore pembayaran	Aktivitas API pada `AWS::BedrockAgentCore::Payments` sumber daya.	Bedrock-AgentCore pembayaran	`AWS::BedrockAgentCore::Payments`
Bedrock-AgentCore kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::Policy` sumber daya.	Bedrock-AgentCore kebijakan	`AWS::BedrockAgentCore::Policy`
Bedrock-AgentCore mesin kebijakan	Aktivitas API pada `AWS::BedrockAgentCore::PolicyEngine` sumber daya.	Bedrock-AgentCore mesin kebijakan	`AWS::BedrockAgentCore::PolicyEngine`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Bedrock-AgentCore Rekomendasi	Aktivitas API pada `AWS::BedrockAgentCore::Recommendation` sumber daya.	Bedrock-AgentCore Rekomendasi	`AWS::BedrockAgentCore::Recommendation`
Bedrock-AgentCore Registri	Aktivitas API pada `AWS::BedrockAgentCore::Registry` sumber daya.	Bedrock-AgentCore Registri	`AWS::BedrockAgentCore::Registry`
Amazon Bedrock	Aktivitas API Amazon Bedrock Runtime.	Bedrock-AgentCore Runtime	`AWS::BedrockAgentCore::Runtime`
Amazon Bedrock	Aktivitas Amazon Bedrock Runtime-Endpoint API.	Bedrock-AgentCore Runtime-Endpoint	`AWS::BedrockAgentCore::RuntimeEndpoint`
Amazon Bedrock	Aktivitas API Amazon Bedrock Token Vault.	Bedrock-AgentCore Brankas Token	`AWS::BedrockAgentCore::TokenVault`
Amazon Bedrock	Aktivitas API Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentity`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Bedrock	Aktivitas API Direktori Identitas Beban Kerja Amazon Bedrock.	Bedrock-AgentCore Direktori Identitas Beban Kerja	`AWS::BedrockAgentCore::WorkloadIdentityDirectory`
Proyek Mantel Batuan Dasar	Aktivitas API pada `AWS::BedrockMantle::Project` sumber daya.	Proyek Mantel Batuan Dasar	`AWS::BedrockMantle::Project`
Alat Pencarian Web Bedrock	Aktivitas API pada `AWS::BedrockWebSearch::Tool` sumber daya.	Alat Pencarian Web Bedrock	`AWS::BedrockWebSearch::Tool`
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces (untuk Apache Cassandra) di aliran Cassandra CDC.	Aliran CDC Cassandra	`AWS::Cassandra::Stream`
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces di atas meja. Untuk informasi selengkapnya, lihat Amazon Keyspaces (untuk Apache Cassandra).	Meja Cassandra	`AWS::Cassandra::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Certificate Manager	Aktivitas API pada `AWS::CertificateManager::AcmeEndpoint` sumber daya.	AWS::CertificateManager::AcmeEndpoint	`AWS::CertificateManager::AcmeEndpoint`
Uji Klinis Daftar kode teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Codelist` sumber daya.	Uji Klinis Daftar kode teknologi	`AWS::ClinicalTrialsTech::Codelist`
Dataset Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Dataset` sumber daya.	Dataset Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Dataset`
Uji Klinis Eksekusi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Execution` sumber daya.	Uji Klinis Eksekusi teknologi	`AWS::ClinicalTrialsTech::Execution`
Contoh Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Instance` sumber daya.	Contoh Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Instance`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Uji Klinis Pemetaan teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Mapping` sumber daya.	Uji Klinis Pemetaan teknologi	`AWS::ClinicalTrialsTech::Mapping`
Jadwal Teknologi Uji Klinis	Aktivitas API pada `AWS::ClinicalTrialsTech::Schedule` sumber daya.	Jadwal Teknologi Uji Klinis	`AWS::ClinicalTrialsTech::Schedule`
Uji Klinis Studi teknologi	Aktivitas API pada `AWS::ClinicalTrialsTech::Study` sumber daya.	Uji Klinis Studi teknologi	`AWS::ClinicalTrialsTech::Study`
Amazon CloudFront	CloudFront Aktivitas API pada a KeyValueStore. Untuk informasi selengkapnya, lihat Amazon CloudFront.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API pada profil.	AWS::CloudOptimization: :Profil	`AWS::CloudOptimization::Profile`
Optimalisasi Biaya Amazon	CloudOptimization Aktivitas API berdasarkan rekomendasi.	AWS::CloudOptimization: :Rekomendasi	`AWS::CloudOptimization::Recommendation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS CloudTrail	CloudTrail PutAuditEvents aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS. Untuk informasi selengkapnya, lihat AWS CloudTrail.	CloudTrail saluran	`AWS::CloudTrail::Channel`
CloudWatch dataset	Aktivitas API pada `AWS::CloudWatch::Dataset` sumber daya.	CloudWatch dataset	`AWS::CloudWatch::Dataset`
Titik akhir konsumsi observabilitas	Aktivitas API pada `AWS::CloudWatch::IngestionEndpoint` sumber daya.	Titik akhir konsumsi observabilitas	`AWS::CloudWatch::IngestionEndpoint`
Amazon CloudWatch	Aktivitas Amazon CloudWatch API pada metrik. Untuk informasi selengkapnya, lihat Amazon CloudWatch.	CloudWatch metrik	`AWS::CloudWatch::Metric`
Amazon CodeGuru Profiler	CodeGuru Aktivitas API profiler pada grup profil.	CodeGuru Grup profil profiler	`AWS::CodeGuruProfiler::ProfilingGroup`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API pada kustomisasi.	CodeWhisperer kustomisasi	`AWS::CodeWhisperer::Customization`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API di profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Aktivitas API Amazon Cognito di kumpulan identitas Amazon Cognito. Untuk informasi lebih lanjut, lihat Amazon Cognito.	Kolam Identitas Cognito	`AWS::Cognito::IdentityPool`
AWS Data Exchange	AWS Aktivitas API Data Exchange pada aset.	Aset Data Exchange	`AWS::DataExchange::Asset`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada armada. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Armada Cloud	`AWS::Deadline::Fleet`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerjaan. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Lowongan kerja Deadline Cloud	`AWS::Deadline::Job`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada antrian. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu antrian Cloud	`AWS::Deadline::Queue`
AWS Batas Waktu Cloud	Batas waktu aktivitas Cloud API pada pekerja. Untuk informasi selengkapnya, lihat AWS Deadline Cloud.	Batas waktu Pekerja Cloud	`AWS::Deadline::Worker`
Peringatan Diode Alerting terkait	Aktivitas API pada `AWS::DiodeAlerting::LinkedAlert` sumber daya.	Peringatan Diode Alerting terkait	`AWS::DiodeAlerting::LinkedAlert`
Amazon Aurora DSQL	Aktivitas Amazon Aurora DSQL API pada sumber daya cluster.	Amazon Aurora DSQL	`AWS::DSQL::Cluster`
Amazon DynamoDB	Aktivitas Amazon DynamoDB API di stream. Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB Streams	`AWS::DynamoDB::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon DynamoDB	Aktivitas API tingkat item Amazon DynamoDB pada tabel (misalnya, PutItem,, DeleteItem dan operasi API). UpdateItem Untuk tabel dengan aliran diaktifkan, bidang sumber daya dalam peristiwa data berisi: :DynamoDB : :Stream dan AWS AWS: :DynamoDB : :Table. Jika Anda menentukan AWS: :DynamoDB : :Table untuk resources.type, itu akan mencatat tabel DynamoDB dan peristiwa aliran DynamoDB secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter pada bidang EventName . Untuk informasi selengkapnya, lihat Amazon DynamoDB.	DynamoDB	`AWS::DynamoDB::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Elastic Compute Cloud	Instans Amazon EC2 menghubungkan aktivitas API titik akhir.	Instans EC2 menghubungkan titik akhir	`AWS::EC2::InstanceConnectEndpoint`
Amazon Elastic Block Store	API langsung Amazon Elastic Block Store (EBS), seperti, PutSnapshotBlock, GetSnapshotBlock dan snapshot ListChangedBlocks Amazon EBS. Untuk informasi selengkapnya, lihat Amazon Elastic Block Store.	API langsung EBS	`AWS::EC2::Snapshot`
Amazon Elastic Container Service	Aktivitas API Amazon Elastic Container Service pada instance container.	Contoh kontainer ECS	`AWS::ECS::ContainerInstance`
LAYANAN AMAZON ELASTIC KUBERNETES	Aktivitas API Amazon Elastic Kubernetes Service di dasbor.	Dasbor EKS	`AWS::EKS::Dashboard`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon EMR	Aktivitas Amazon EMR API di ruang kerja log tulis di depan. Untuk informasi selengkapnya, lihat Amazon EMR.	Ruang kerja log tulis ke depan EMR	`AWS::EMRWAL::Workspace`
pesan pengguna akhir	Aktivitas API pada `AWS::EndUserMessaging::NotifyCodeVerification` sumber daya.	AWS::EndUserMessaging::NotifyCodeVerification	`AWS::EndUserMessaging::NotifyCodeVerification`
EventBridge titik akhir	Aktivitas API pada `AWS::Events::Endpoint` sumber daya.	EventBridge titik akhir	`AWS::Events::Endpoint`
EventBridge Bus acara khusus - klasik	Aktivitas API pada `AWS::Events::EventBus` sumber daya.	EventBridge Bus acara khusus - klasik	`AWS::Events::EventBus`
EventBridge sumber acara mitra	Aktivitas API pada `AWS::Events::EventSource` sumber daya.	EventBridge sumber acara mitra	`AWS::Events::EventSource`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
EventBridge aturan	Aktivitas API pada `AWS::Events::Rule` sumber daya.	EventBridge aturan	`AWS::Events::Rule`
EventBridge Bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventBus` sumber daya.	EventBridge Bus peristiwa kustom	`AWS::EventsV2::EventBus`
EventBridge Sumber acara bus acara khusus	Aktivitas API pada `AWS::EventsV2::EventSource` sumber daya.	EventBridge Sumber acara bus acara khusus	`AWS::EventsV2::EventSource`
Amazon FinSpace	Aktivitas Amazon FinSpace API di lingkungan. Untuk informasi selengkapnya, lihat Amazon FinSpace.	FinSpace	`AWS::FinSpace::Environment`
Amazon FSx	Aktivitas Amazon FSx API pada volume.	Volume FSx	`AWS::FSx::Volume`
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada aplikasi. Untuk informasi selengkapnya, lihat Amazon GameLift Streams.	GameLift Aplikasi Streams	`AWS::GameLiftStreams::Application`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
GameLift Aliran Amazon	Amazon GameLift Streaming aktivitas API streaming pada grup streaming. Untuk informasi selengkap nya, lihat Amazon GameLift Streams.	GameLift Streaming grup aliran	`AWS::GameLiftStreams::StreamGroup`
Peta Lokasi Amazon	Aktivitas API Peta Lokasi Amazon.	Peta Geo	`AWS::GeoMaps::Provider`
Tempat Lokasi Amazon	Aktivitas API Tempat Lokasi Amazon.	Tempat Geo	`AWS::GeoPlaces::Provider`
Rute Lokasi Amazon	Aktivitas API Rute Lokasi Amazon.	Rute Geo	`AWS::GeoRoutes::Provider`
AWS Glue	AWS Aktivitas Glue API pada tabel yang dibuat oleh Lake Formation.	Formasi Danau	`AWS::Glue::Table`
AWS IoT Greengrass Versi 2	Aktivitas API Greengrass dari perangkat inti Greengrass pada versi komponen. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Versi komponen Greengrass IoT	`AWS::GreengrassV2::ComponentVersion`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT Greengrass Versi 2	Greengrass aktivitas API dari perangkat inti Greengrass pada penerapan. Greengrass tidak mencatat peristiwa yang ditolak akses. Untuk informasi lebih lanjut, lihat AWS IoT Greengrass Versi 2.	Penyebaran Greengrass IoT	`AWS::GreengrassV2::Deployment`
Amazon GuardDuty	Aktivitas Amazon GuardDuty API untuk detektor. Untuk informasi selengkapnya, lihat Amazon GuardDuty.	GuardDuty detektor	`AWS::GuardDuty::Detector`
Amazon GuardDuty	GuardDuty Aktivitas API pada pemindaian malware.	GuardDuty pemindaian malware	`AWS::GuardDuty::MalwareScan`
Domain agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Domain` sumber daya.	Domain agen kesehatan	`AWS::HealthAgent::Domain`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Integration` sumber daya.	AWS::HealthAgent: :Integri	`AWS::HealthAgent::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::PatientInsightsJob` sumber daya.	health-agent.amazonaws.com	`AWS::HealthAgent::PatientInsightsJob`
Amazon Connect Health	Aktivitas API pada `AWS::HealthAgent::Session` sumber daya.	AWS::HealthAgent: :Sesi	`AWS::HealthAgent::Session`
Berlangganan agen kesehatan	Aktivitas API pada `AWS::HealthAgent::Subscription` sumber daya.	Berlangganan agen kesehatan	`AWS::HealthAgent::Subscription`
Profil transformasi data Health Lake	Aktivitas API pada `AWS::HealthLake::DataTransformationProfile` sumber daya.	Profil transformasi data Health Lake	`AWS::HealthLake::DataTransformationProfile`
AWS IoT	AWS Aktivitas API IoT pada sertifikat. Untuk informasi selengkapnya, lihat AWS IoT.	Sertifikat IoT	`AWS::IoT::Certificate`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS IoT	AWS Aktivitas API IoT pada berbagai hal. Untuk informasi selengkapnya, lihat AWS IoT.	Hal IoT	`AWS::IoT::Thing`
AWS Terowongan IoT	Aktivitas API pada `AWS::IoT::Tunnel` sumber daya.	AWS Terowongan IoT	`AWS::IoT::Tunnel`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada aset. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Aset IoT SiteWise	`AWS::IoTSiteWise::Asset`
Dataset IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Dataset` sumber daya.	Dataset IoT SiteWise	`AWS::IoTSiteWise::Dataset`
Pipa IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Pipeline` sumber daya.	Pipa IoT SiteWise	`AWS::IoTSiteWise::Pipeline`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada deret waktu. Untuk informasi selengkapnya, lihat AWS IoT SiteWise.	Deret waktu IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Ruang kerja IoT SiteWise	Aktivitas API pada `AWS::IoTSiteWise::Workspace` sumber daya.	Ruang kerja IoT SiteWise	`AWS::IoTSiteWise::Workspace`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT pada entitas. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Entitas IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT di ruang kerja. Untuk informasi selengkapnya, lihat AWS IoT TwinMaker.	Ruang kerja IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Peringkat Cerdas Amazon Kendra	Aktivitas API Peringkat Cerdas Amazon Kendra pada rencana eksekusi skor ulang. Untuk informasi selengkapnya, lihat Peringkat Cerdas Amazon Kendra.	Peringkat Kendra	`AWS::KendraRanking::ExecutionPlan`
Amazon Kinesis Data Streams	Aktivitas API Kinesis Data Streams pada stream. Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Aliran kinesis	`AWS::Kinesis::Stream`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Kinesis Data Streams	Kinesis Data Streams aktivitas API pada konsumen streaming . Untuk informasi selengkapnya, lihat Amazon Kinesis Data Streams.	Konsumen aliran kinesis	`AWS::Kinesis::StreamConsumer`
Amazon Data Firehose	Aktivitas API aliran pengiriman Amazon Data Firehose.	Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`
Amazon Kinesis Video Streams	Kinesis Video Streams aktivitas API saluran pensinyalan video.	Saluran pensinyalan video Kinesis	`AWS::KinesisVideo::SignalingChannel`
Amazon Kinesis Video Streams	Aktivitas API Kinesis Video Streams pada aliran video, seperti panggilan ke dan. GetMedia PutMedia	Aliran video Kinesis	`AWS::KinesisVideo::Stream`
AWS Lambda	AWS Aktivitas eksekusi fungsi Lambda (API Invoke).	Lambda	`AWS::Lambda::Function`
Gambar microvm Lambda	Aktivitas API pada `AWS::Lambda::MicrovmImage` sumber daya.	Gambar microvm Lambda	`AWS::Lambda::MicrovmImage`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Fungsi Web Lambda	Aktivitas API pada `AWS::Lambda::WebFunction` sumber daya.	Lambda WebFunction	`AWS::Lambda::WebFunction`
Lex Bot	Aktivitas API pada `AWS::Lex::Bot` sumber daya.	Lex Bot	`AWS::Lex::Bot`
AWS Lex Bot Alias	Aktivitas API pada `AWS::Lex::BotAlias` sumber daya.	AWS Lex Bot Alias	`AWS::Lex::BotAlias`
CloudWatch Otorisasi grup log log	Aktivitas API pada `AWS::Logs::LogGroupAuthorization` sumber daya.	CloudWatch Otorisasi grup log log	`AWS::Logs::LogGroupAuthorization`
Log Scheduled Query	Aktivitas API pada `AWS::Logs::ScheduledQuery` sumber daya.	Log Scheduled Query	`AWS::Logs::ScheduledQuery`
Amazon Machine Learning	Aktivitas Machine Learning API pada model ML.	Machine Learning MlModel	`AWS::MachineLearning::MlModel`
Amazon Managed Blockchain	Aktivitas API Amazon Managed Blockchain di jaringan.	Jaringan Blockchain yang dikelola	`AWS::ManagedBlockchain::Network`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Managed Blockchain	Amazon Managed Blockchain JSON-RPC memanggil node Ethereum, seperti ETH_getBalance atau eth_get. BlockByNumber Untuk informasi selengkapnya, lihat Amazon Managed Blockchain.	Blockchain yang Dikelola	`AWS::ManagedBlockchain::Node`
Kueri Blockchain yang Dikelola Amazon	Aktivitas API Kueri Blockchain Terkelola Amazon.	Kueri Blockchain Terkelola	`AWS::ManagedBlockchainQuery::QueryAPI`
AWS HealthImaging	AWS HealthImaging Aktivitas API pada penyimpanan data.	MedicalImaging penyimpanan data	`AWS::MedicalImaging::Datastore`
AWS HealthImaging	AWS HealthImaging image set aktivitas API.	MedicalImaging set gambar	`AWS::MedicalImaging::ImageSet`
Amazon Managed Workflows for Apache Airflow	Aktivitas API Amazon MWAA di lingkungan.	Apache Airflow yang Dikelola	`AWS::MWAA::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Grafik Amazon Neptunus	Aktivitas API data, misalnya kueri, algoritme , atau pencarian vektor, pada Grafik Neptunus.	Grafik Neptunus	`AWS::NeptuneGraph::Graph`
Monitor Aliran CloudWatch Jaringan Amazon	Aktivitas API Monitor Aliran CloudWatch Jaringan Amazon pada monitor.	Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Monitor`
Monitor Aliran CloudWatch Jaringan Amazon	Amazon CloudWatch Network Flow Monitor aktivitas API pada cakupan.	Lingkup Monitor Aliran Jaringan	`AWS::NetworkFlowMonitor::Scope`
Amazon NovaAct	Aktivitas Amazon NovaAct API pada definisi alur kerja.	Definisi alur kerja	`AWS::NovaAct::WorkflowDefinition`
Amazon NovaAct	Aktivitas NovaAct API Amanzon pada alur kerja berjalan.	Alur kerja berjalan	`AWS::NovaAct::WorkflowRun`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise di UKey.	Amazon Satu uKey	`AWS::One::UKey`
Amazon Satu Perusahaan	Aktivitas API Amazon One Enterprise pada pengguna.	Amazon Satu Pengguna	`AWS::One::User`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada alias.	Alias Kriptografi Pembayaran	`AWS::PaymentCryptography::Alias`
AWS Kriptografi Pembayaran	AWS Aktivitas API Kriptografi Pembayaran pada kunci.	Kunci Kriptografi Pembayaran	`AWS::PaymentCryptography::Key`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API Direktori Aktif.	Konektor CA Pribadi untuk Direktori Aktif	`AWS::PCAConnectorAD::Connector`
AWS CA pribadi	AWS Konektor CA Pribadi untuk aktivitas API SCEP.	Konektor CA Pribadi untuk SCEP	`AWS::PCAConnectorSCEP::Connector`
Amazon Pinpoint	Amazon Pinpoint aktivitas API pada aplikasi penargetan seluler.	Aplikasi Penargetan Seluler	`AWS::Pinpoint::App`
Aplikasi Amazon Q	Aktivitas API data di Amazon Q Apps. Untuk informasi selengkapnya, lihat Amazon Q Apps.	Aplikasi Amazon Q	`AWS::QApps::QApp`
Aplikasi Amazon Q	Aktivitas API data di sesi Amazon Q App.	Sesi Aplikasi Amazon Q	`AWS::QApps::QAppSession`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada aplikasi. Untuk informasi selengkapnya, lihat Amazon Q Business.	Aplikasi Amazon Q Business	`AWS::QBusiness::Application`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada sumber data. Untuk informasi selengkapnya, lihat Amazon Q Business.	Sumber data Amazon Q Business	`AWS::QBusiness::DataSource`
Amazon Q Bisnis	Aktivitas API Amazon Q Business pada indeks. Untuk informasi selengkapnya, lihat Amazon Q Business.	Amazon Q Indeks Bisnis	`AWS::QBusiness::Index`
Amazon Q Bisnis	Aktivitas API integrasi Amazon Q Business.	Integrasi Amazon Q Bisnis	`AWS::QBusiness::Integration`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada pengalaman web. Untuk informasi selengkapnya, lihat Amazon Q Business.	Pengalaman web Amazon Q Bisnis	`AWS::QBusiness::WebExperience`
Amazon Q Developer	Aktivitas API Pengembang Amazon Q pada integrasi.	Q Integrasi pengembang	`AWS::QDeveloper::Integration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Cepat Amazon pada konektor tindakan.	AWS QuickSuite Tindakan	`AWS::Quicksight::ActionConnector`
QuickSight Aplikasi Amazon	Aktivitas API pada `AWS::QuickSight::App` sumber daya.	QuickSight Aplikasi Amazon	`AWS::QuickSight::App`
QuickSight otomatisasi	Aktivitas API pada `AWS::QuickSight::Automation` sumber daya.	QuickSight otomatisasi	`AWS::QuickSight::Automation`
QuickSight pekerjaan otomatisasi	Aktivitas API pada `AWS::QuickSight::AutomationJob` sumber daya.	QuickSight pekerjaan otomatisasi	`AWS::QuickSight::AutomationJob`
AWS QuickSight Ekstensi	Aktivitas API pada `AWS::QuickSight::Extension` sumber daya.	AWS QuickSight Ekstensi	`AWS::QuickSight::Extension`
AWS QuickSight Akses Ekstensi	Aktivitas API pada `AWS::QuickSight::ExtensionAccess` sumber daya.	AWS QuickSight Akses Ekstensi	`AWS::QuickSight::ExtensionAccess`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Quick	Aktivitas API Aliran Cepat Amazon.	AWS QuickSight aliran	`AWS::QuickSight::Flow`
Amazon Quick	Aktivitas FlowSession API Cepat Amazon.	AWS QuickSight sesi aliran	`AWS::QuickSight::FlowSession`
QuickSight Halaman Amazon	Aktivitas API pada `AWS::QuickSight::Page` sumber daya.	QuickSight Halaman Amazon	`AWS::QuickSight::Page`
QuickSight Tugas	Aktivitas API pada `AWS::QuickSight::Task` sumber daya.	QuickSight Tugas	`AWS::QuickSight::Task`
Amazon RDS	Aktivitas Amazon RDS API di Cluster DB. Untuk informasi selengkapnya, lihat Amazon RDS.	API Data RDS - Kluster DB	`AWS::RDS::DBCluster`
Amazon Redshift	Aktivitas Redshift API pada cluster.	Gugus Pergeseran Merah	`AWS::Redshift::Cluster`
AWS Tampilan terkelola Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::ManagedView` sumber daya.	AWS Tampilan terkelola Resource Explorer	`AWS::ResourceExplorer2::ManagedView`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Tampilan Resource Explorer	Aktivitas API pada `AWS::ResourceExplorer2::View` sumber daya.	AWS Tampilan Resource Explorer	`AWS::ResourceExplorer2::View`
Amazon CloudWatch RUM	Aktivitas Amazon CloudWatch RUM API di monitor aplikasi.	Monitor aplikasi RUM	`AWS::RUM::AppMonitor`
Amazon S3	Aktivitas API Amazon S3 pada titik akses. Untuk informasi selengkapnya, lihat Amazon S3.	Titik Akses S3	`AWS::S3::AccessPoint`
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket tujuan umum. Untuk informasi selengkapnya, lihat Amazon S3.	S3	`AWS::S3::Object`
Titik Akses Ekspres S3	Aktivitas API pada `AWS::S3Express::AccessPoint` sumber daya.	Titik Akses Ekspres S3	`AWS::S3Express::AccessPoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, GetObject DeleteObject, dan operasi PutObject API) pada objek dalam bucket direktori . Untuk informasi selengkapnya, lihat Amazon S3.	S3 Ekspres	`AWS::S3Express::Object`
Amazon S3	Aktivitas API titik akses Objek Lambda Amazon S3, seperti panggilan ke dan. CompleteMultipartU pload GetObject Untuk informasi selengkapnya, lihat Amazon S3.	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 pada aktivitas API tingkat objek Outposts. Untuk informasi selengkap nya, lihat Amazon S3 on Outposts.	Outposts S3	`AWS::S3Outposts::Object`
Tabel Amazon S3	Aktivitas API Amazon S3 pada tabel. Untuk informasi selengkap nya, lihat Tabel Amazon S3.	Tabel S3	`AWS::S3Tables::Table`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Tabel Amazon S3	Aktivitas API Amazon S3 pada bucket meja. Untuk informasi selengkapnya, lihat Tabel Amazon S3.	Ember meja S3	`AWS::S3Tables::TableBucket`
Vektor Amazon S3	Aktivitas API Amazon S3 pada indeks vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Indeks vektor S3	`AWS::S3Vectors::Index`
Vektor Amazon S3	Aktivitas API Amazon S3 pada bucket vektor. Untuk informasi selengkapnya, lihat Vektor Amazon S3.	Ember vektor S3	`AWS::S3Vectors::VectorBucket`
Amazon SageMaker AI	InvokeEndpointWithResponseStream Aktivitas Amazon SageMaker AI di titik akhir. Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker titik akhir	`AWS::SageMaker::Endpoint`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API pada komponen percobaan percobaan . Untuk informasi lebih lanjut, lihat Amazon SageMaker AI.	SageMaker komponen uji coba eksperimen metrik	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SageMaker AI	Aktivitas Amazon SageMaker AI API di toko fitur.	SageMaker Toko Fitur	`AWS::SageMaker::FeatureGroup`
SageMaker hub	Aktivitas API pada `AWS::SageMaker::Hub` sumber daya.	SageMaker hub	`AWS::SageMaker::Hub`
SageMaker Lowongan	Aktivitas API pada `AWS::SageMaker::Job` sumber daya.	SageMaker Lowongan kerja	`AWS::SageMaker::Job`
AWS SageMaker MlflowApp	Aktivitas API pada `AWS::SageMaker::MlflowApp` sumber daya.	AWS SageMaker MlflowApp	`AWS::SageMaker::MlflowApp`
Amazon SageMaker AI	Aktivitas API Amazon SageMaker AI MLFlow.	SageMaker MLFlow	`AWS::SageMaker::MlflowTrackingServer`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
SageMaker sesi pelatihan	Aktivitas API pada `AWS::SageMaker::TrainingSession` sumber daya.	SageMaker sesi pelatihan	`AWS::SageMaker::TrainingSession`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::BusinessRule` sumber daya.	AWS: :SCN:: BusinessRule	`AWS::SCN::BusinessRule`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::DataLakeException` sumber daya.	AWS: :SCN:: DataLakeException	`AWS::SCN::DataLakeException`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionInvestigation` sumber daya.	AWS: :SCN:: Exception Investigation	`AWS::SCN::ExceptionInvestigation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::ExceptionRule` sumber daya.	AWS: :SCN:: Exception Rule	`AWS::SCN::ExceptionRule`
AWS Rantai Pasokan	Aktivitas API Rantai Pasokan pada sebuah instance.	Keputusan Amazon Connect	`AWS::SCN::Instance`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Metric` sumber daya.	AWS: :SCN: :M	`AWS::SCN::Metric`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::MetricEvaluation` sumber daya.	AWS: :SCN:: MetricEvaluation	`AWS::SCN::MetricEvaluation`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::Outcome` sumber daya.	AWS: :SCN: :H	`AWS::SCN::Outcome`
AWS Rantai Pasokan	Aktivitas API pada `AWS::SCN::OutcomeTemplate` sumber daya.	AWS: :SCN:: OutcomeTemplate	`AWS::SCN::OutcomeTemplate`
Amazon SimpleDB	Aktivitas API Amazon SimpleDB di domain.	Domain SimpleDB	`AWS::SDB::Domain`
AWS Cloud Map	AWS Aktivitas Cloud Map API pada namespace. Untuk informasi selengkapnya, lihat AWS Cloud Map.	AWS Ruang nama Cloud Map	`AWS::ServiceDiscovery::Namespace`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Cloud Map	AWS Aktivitas Cloud Map API pada suatu layanan. Untuk informasi selengkapnya, lihat AWS Cloud Map.	AWS Layanan Cloud Map	`AWS::ServiceDiscovery::Service`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada set konfigurasi.	Set konfigurasi SES	`AWS::SES::ConfigurationSet`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada identitas email.	Identitas SES	`AWS::SES::EmailIdentity`
Layanan Email Sederhana Amazon	Aktivitas API Amazon Simple Email Service (Amazon SES) pada template.	Templat SES	`AWS::SES::Template`
AWS Penandatangan	Aktivitas API penandatangan saat menandatangani pekerjaan.	Pekerjaan penandatanganan penandatangan	`AWS::Signer::SigningJob`
AWS Penandatangan	Aktivitas API penandatangan pada profil penandatanganan.	Profil penandatanganan penandatangan	`AWS::Signer::SigningProfile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Asisten IoT SiteWise	Aktivitas API Asisten Sitewise pada percakapan.	Percakapan Asisten Sitewise	`AWS::SitewiseAssistant::Conversation`
Pencarian Operator	Aktivitas API pada `AWS::SMSVoice::CarrierLookup` sumber daya.	Pencarian Operator	`AWS::SMSVoice::CarrierLookup`
Set Konfigurasi	Aktivitas API pada `AWS::SMSVoice::ConfigurationSet` sumber daya.	Set Konfigurasi	`AWS::SMSVoice::ConfigurationSet`
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada pesan. Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Pesan Suara SMS	`AWS::SMSVoice::Message`
Beritahu Konfigurasi	Aktivitas API pada `AWS::SMSVoice::NotifyConfiguration` sumber daya.	Beritahu Konfigurasi	`AWS::SMSVoice::NotifyConfiguration`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS SMS Pesan Pengguna Akhir	AWS Aktivitas API SMS Pesan Pengguna Akhir pada identitas originasi . Untuk informasi selengkapnya, lihat SMS Pesan Pengguna AWS Akhir.	Identitas originasi SMS Voice	`AWS::SMSVoice::OriginationIdentity`
Amazon SNS	Amazon SNS Publikasikan operasi API pada titik akhir platform. Untuk informasi selengkapnya, lihat Amazon SNS.	Titik akhir platform SNS	`AWS::SNS::PlatformEndpoint`
Amazon SNS	Amazon SNS Publish dan operasi PublishBatch API pada topik. Untuk informasi selengkapnya, lihat Amazon SNS.	Topik SNS	`AWS::SNS::Topic`
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID nomor telepon. Untuk informasi selengkapnya, lihat AWS End User Messaging Sosial.	Social-Messaging ID Nomor Telepon	`AWS::SocialMessaging::PhoneNumberId`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Pesan Pengguna Akhir Sosial	AWS Aktivitas API Sosial Pesan Pengguna Akhir pada ID Waba.	Social-Messaging ID Waba	`AWS::SocialMessaging::WabaId`
Amazon SQS	Aktivitas Amazon SQS API pada pesan. Untuk informasi selengkapnya, lihat Amazon SQS.	SQS	`AWS::SQS::Queue`
AWS Systems Manager	Aktivitas API Systems Manager pada penilaian dampak.	Penilaian Dampak SSM	`AWS::SSM::ExecutionPreview`
AWS Systems Manager	Aktivitas API Systems Manager pada node terkelola. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Node terkelola Systems Manager	`AWS::SSM::ManagedNode`
AWS Systems Manager	Aktivitas API Systems Manager pada saluran kontrol. Untuk informasi selengkapnya, lihat AWS Systems Manager.	Systems Manager	`AWS::SSMMessages::ControlChannel`
AWS Step Functions	Aktivitas Step Functions API pada aktivitas. Untuk informasi selengkapnya, lihat AWS Step Functions.	Aktivitas Step Functions	`AWS::StepFunctions::Activity`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS Step Functions	Aktivitas Step Functions API pada mesin state. Untuk informasi selengkapnya, lihat AWS Step Functions.	Mesin status Step Functions	`AWS::StepFunctions::StateMachine`
Amazon Support	SupportAccess Aktivitas API pada penyewa.	SupportAccess penyewa	`AWS::SupportAccess::Tenant`
Amazon Support	SupportAccess Aktivitas API pada akun yang mempercayai.	SupportAccess akun kepercayaan	`AWS::SupportAccess::TrustingAccount`
Amazon Support	SupportAccess Aktivitas API tentang peran kepercayaan.	SupportAccess peran percaya	`AWS::SupportAccess::TrustingRole`
Amazon SWF	Aktivitas API Amazon SWF di domain. Untuk informasi selengkapnya, lihat Amazon SWF.	Domain SWF	`AWS::SWF::Domain`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Perangkat.	Perangkat Klien Tipis	`AWS::ThinClient::Device`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Lingkungan.	Lingkungan Klien Tipis	`AWS::ThinClient::Environment`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Token stempel waktu	Aktivitas API pada `AWS::Timestamp::TimestampToken` sumber daya.	Token stempel waktu	`AWS::Timestamp::TimestampToken`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream di database. Untuk informasi selengkapnya, lihat Amazon Timestream.	Database Timestream	`AWS::Timestream::Database`
Amazon Timestream	Aktivitas API Amazon Timestream di titik akhir regional.	Titik akhir regional Timestream	`AWS::Timestream::RegionalEndpoint`
Amazon Timestream	Aktivitas API Kueri Amazon Timestream pada tabel. Untuk informasi selengkapnya, lihat Amazon Timestream.	Tabel Timestream	`AWS::Timestream::Table`
Transformasi Amazon	Mengubah aktivitas API pada instance agen.	Contoh agen transformasi	`AWS::Transform::AgentInstance`
Amazon Q Transform AKA AWS Transformasi	Aktivitas API pada `AWS::Transform::Profile` sumber daya.	mengubah	`AWS::Transform::Profile`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada kampanye.	Transform -Custom kampanye	`AWS::TransformCustom::Campaign`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada percakapan.	Transform -Custom percakapan	`AWS::TransformCustom::Conversation`
Amazon Transform Kustom	Mengubah aktivitas API Kustom pada item pengetahuan.	Transform- Custom item pengetahuan	`AWS::TransformCustom::KnowledgeItem`
Amazon Transform Kustom	Ubah aktivitas API Kustom pada paket.	Transform- Custom paket	`AWS::TransformCustom::Package`
Kustomisasi akun UXC	Aktivitas API pada `AWS::UXC::AccountCustomization` sumber daya.	Kustomisasi akun UXC	`AWS::UXC::AccountCustomization`
Izin Terverifikasi Amazon	Aktivitas API Izin Terverifikasi Amazon di toko kebijakan.	Izin Terverifikasi Amazon	`AWS::VerifiedPermissions::PolicyStore`
Well-Architected rekomendasi agen	Aktivitas API pada `AWS::WellArchitected::AgentRecommendation` sumber daya.	Well-Architected rekomendasi agen	`AWS::WellArchitected::AgentRecommendation`

Layanan AWS	Deskripsi	Jenis sumber daya (konsol)	nilai resources.type
AWS X-Ray	X-Ray Aktivitas API pada jejak. Untuk informasi selengkapnya, lihat AWS X-Ray.	X-Ray jejak	`AWS::XRay::Trace`

Untuk merekam peristiwa CloudTrail data, Anda harus secara eksplisit menambahkan setiap jenis sumber daya yang ingin Anda kumpulkan aktivitasnya. Untuk informasi selengkapnya, lihat Membuat jejak dengan CloudTrail konsol dan Membuat penyimpanan data acara untuk CloudTrail acara dengan konsol.

Pada jejak wilayah tunggal atau penyimpanan data peristiwa, Anda dapat mencatat peristiwa data hanya untuk sumber daya yang dapat Anda akses di Wilayah tersebut. Meskipun bucket S3 bersifat global, AWS Lambda fungsi dan tabel DynamoDB bersifat regional.

Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Contoh: Mencatat peristiwa data untuk objek Amazon S3

Mencatat peristiwa data untuk semua objek S3 dalam bucket S3

Contoh berikut menunjukkan cara kerja logging saat Anda mengonfigurasi logging semua kejadian data untuk bucket S3 bernama `amzn-s3-demo-bucket`. Dalam contoh ini, CloudTrail pengguna menentukan awalan kosong, dan opsi untuk mencatat peristiwa data Baca dan Tulis.

1. Seorang pengguna mengunggah objek ke`amzn-s3-demo-bucket`.
2. Operasi API `PutObject` adalah API tingkat objek Amazon S3. Ini dicatat sebagai peristiwa data di CloudTrail. Karena CloudTrail pengguna menetapkan bucket S3 dengan awalan kosong, peristiwa yang terjadi pada objek apa pun di bucket tersebut dicatat. Data jejak atau peristiwa menyimpan proses dan mencatat acara.
3. Pengguna lain mengunggah objek ke`amzn-s3-demo-bucket2`.
4. Operasi `PutObject` API terjadi pada objek dalam bucket S3 yang tidak ditentukan untuk penyimpanan data jejak atau peristiwa. Penyimpanan data jejak atau peristiwa tidak mencatat acara.

Mencatat peristiwa data untuk objek S3 tertentu

Contoh berikut menunjukkan cara kerja logging saat Anda mengonfigurasi penyimpanan data jejak atau peristiwa untuk mencatat peristiwa untuk objek S3 tertentu. Dalam contoh ini, CloudTrail pengguna menentukan bucket S3 bernamaamzn-s3-demo-bucket3, dengan awalan*my-images*, dan opsi untuk hanya mencatat peristiwa Write data.

1. Pengguna menghapus objek yang dimulai dengan `my-images` awalan di bucket, seperti. `arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`
2. Operasi API `DeleteObject` adalah API tingkat objek Amazon S3. Ini dicatat sebagai peristiwa data Tulis di CloudTrail. Peristiwa terjadi pada objek yang cocok dengan bucket S3 dan awalan yang ditentukan dalam penyimpanan data jejak atau peristiwa. Data jejak atau peristiwa menyimpan proses dan mencatat acara.
3. Pengguna lain menghapus objek dengan awalan berbeda di bucket S3, seperti. `arn:aws:s3:::amzn-s3-demo-bucket3/my-videos/example.avi`
4. Peristiwa terjadi pada objek yang tidak cocok dengan awalan yang ditentukan dalam penyimpanan data jejak atau peristiwa Anda. Penyimpanan data jejak atau peristiwa tidak mencatat acara.
5. Seorang pengguna memanggil operasi `GetObject` API untuk objek,`arn:aws:s3:::amzn-s3-demo-bucket3/my-images/example.jpg`.
6. Peristiwa terjadi pada bucket dan awalan yang ditentukan dalam penyimpanan data jejak atau peristiwa, tetapi `GetObject` merupakan API tingkat objek Amazon S3 tipe baca. Ini direkam sebagai peristiwa data Baca di CloudTrail, dan penyimpanan data jejak atau peristiwa tidak dikonfigurasi untuk mencatat peristiwa Baca. Penyimpanan data jejak atau peristiwa tidak mencatat acara.

> **Note**
>
> Untuk jejak, jika Anda mencatat peristiwa data untuk bucket Amazon S3 tertentu, kami sarankan Anda tidak menggunakan bucket Amazon S3 tempat Anda mencatat peristiwa data untuk menerima file log yang telah Anda tentukan di bagian peristiwa data untuk jejak Anda. Menggunakan bucket Amazon S3 yang sama menyebabkan jejak Anda mencatat peristiwa data setiap kali file log dikirim ke bucket Amazon S3 Anda. File log adalah peristiwa agregat yang dikirimkan pada interval, jadi ini bukan rasio peristiwa 1:1 untuk file log; peristiwa dicatat di file log berikutnya. Misalnya, saat CloudTrail mengirimkan log, `PutObject` peristiwa terjadi pada bucket S3. Jika bucket S3 juga ditentukan di bagian peristiwa data, jejak akan

memproses dan mencatat `PutObject` peristiwa sebagai peristiwa data. Tindakan itu adalah `PutObject` peristiwa lain, dan jejak memproses dan mencatat peristiwa itu lagi. Untuk menghindari peristiwa data pencatatan untuk bucket Amazon S3 tempat Anda menerima file log jika Anda mengonfigurasi jejak untuk mencatat semua peristiwa data Amazon S3 di akun AWS Anda, pertimbangkan salah satu opsi berikut:

- Atur `RecursiveLogging` ke `false` on the trail untuk menekan peristiwa yang dihasilkan oleh operasi CloudTrail pengiriman. Untuk informasi selengkapnya, lihat Menekan peristiwa rekursif dengan logging rekursif.
- Konfigurasikan pengiriman file log ke bucket Amazon S3 milik akun lain AWS . Untuk informasi selengkapnya, lihat Menerima file CloudTrail log dari beberapa akun.

Mencatat peristiwa data untuk objek S3 di objek lain AWS rekening

Saat mengonfigurasi jejak untuk mencatat peristiwa data, Anda juga dapat menentukan objek S3 milik AWS akun lain. Ketika suatu peristiwa terjadi pada objek tertentu, CloudTrail mengevaluasi apakah acara tersebut cocok dengan jejak apa pun di setiap akun. Jika acara cocok dengan pengaturan untuk jejak, jejak akan memproses dan mencatat peristiwa untuk akun tersebut. Umumnya, penelepon API dan pemilik sumber daya dapat menerima peristiwa.

Jika Anda memiliki objek S3 dan Anda menentukannya di jejak Anda, jejak Anda mencatat peristiwa yang terjadi pada objek di akun Anda. Karena Anda memiliki objek, jejak Anda juga mencatat peristiwa ketika akun lain memanggil objek.

Jika Anda menentukan objek S3 di jejak Anda, dan akun lain memiliki objek tersebut, jejak Anda hanya mencatat peristiwa yang terjadi pada objek tersebut di akun Anda. Jejak Anda tidak mencatat peristiwa yang terjadi di akun lain.

Contoh: Mencatat peristiwa data untuk objek Amazon S3 untuk dua AWS rekening

Contoh berikut menunjukkan bagaimana dua AWS akun mengkonfigurasi CloudTrail untuk mencatat peristiwa untuk objek S3 yang sama.

1. Di akun Anda, Anda ingin jejak Anda mencatat peristiwa data untuk semua objek di bucket S3 yang diberi nama`amzn-s3-demo-bucket`. Anda mengonfigurasi jejak dengan menentukan bucket S3 dengan awalan objek kosong.

2. Bob memiliki akun terpisah yang telah diberikan akses ke bucket S3. Bob juga ingin mencatat peristiwa data untuk semua objek di bucket S3 yang sama. Untuk jejaknya, ia mengkonfigurasi jejaknya dan menentukan ember S3 yang sama dengan awalan objek kosong.
3. Bob mengunggah objek ke bucket S3 dengan operasi `PutObject` API.
4. Peristiwa ini terjadi di akunnya dan cocok dengan pengaturan jejaknya. Jejak Bob memproses dan mencatat acara tersebut.
5. Karena Anda memiliki bucket S3 dan acara cocok dengan pengaturan untuk jejak Anda, jejak Anda juga memproses dan mencatat peristiwa yang sama. Karena sekarang ada dua salinan acara (satu masuk di jejak Bob, dan satu masuk ke milik Anda), CloudTrail dikenakan biaya untuk dua salinan peristiwa data.
6. Anda mengunggah objek ke bucket S3.
7. Acara ini terjadi di akun Anda dan cocok dengan pengaturan untuk jejak Anda. Jejak Anda memproses dan mencatat acara.
8. Karena peristiwa itu tidak terjadi di akun Bob, dan dia tidak memiliki ember S3, jejak Bob tidak mencatat acara tersebut. CloudTrail biaya hanya untuk satu salinan peristiwa data ini.

Contoh: Mencatat peristiwa data untuk semua bucket, termasuk bucket S3 yang digunakan oleh dua AWS rekening

Contoh berikut menunjukkan perilaku logging saat Pilih semua bucket S3 di akun Anda diaktifkan untuk jejak yang mengumpulkan peristiwa data di akun. AWS

1. Di akun Anda, Anda ingin jejak Anda mencatat peristiwa data untuk semua bucket S3. Anda mengonfigurasi jejak dengan memilih acara Baca, Menulis peristiwa, atau keduanya untuk Semua bucket S3 saat ini dan masa depan dalam peristiwa Data.
2. Bob memiliki akun terpisah yang telah diberikan akses ke bucket S3 di akun Anda. Dia ingin mencatat peristiwa data untuk ember yang dia akses. Dia mengonfigurasi jejaknya untuk mendapatkan peristiwa data untuk semua bucket S3.
3. Bob mengunggah objek ke bucket S3 dengan operasi `PutObject` API.
4. Peristiwa ini terjadi di akunnya dan cocok dengan pengaturan jejaknya. Jejak Bob memproses dan mencatat acara tersebut.
5. Karena Anda memiliki bucket S3 dan acara cocok dengan pengaturan untuk jejak Anda, jejak Anda juga memproses dan mencatat acara. Karena sekarang ada dua salinan acara (satu masuk di jejak Bob, dan satu masuk ke milik Anda), CloudTrail menagih setiap akun untuk salinan peristiwa data.

6. Anda mengunggah objek ke bucket S3.
7. Acara ini terjadi di akun Anda dan cocok dengan pengaturan untuk jejak Anda. Jejak Anda memproses dan mencatat acara.
8. Karena peristiwa itu tidak terjadi di akun Bob, dan dia tidak memiliki ember S3, jejak Bob tidak mencatat acara tersebut. CloudTrail mengenakan biaya hanya untuk satu salinan peristiwa data ini di akun Anda.
9. Pengguna ketiga, Mary, memiliki akses ke bucket S3, dan menjalankan `GetObject` operasi di ember. Dia memiliki jejak yang dikonfigurasi untuk mencatat peristiwa data di semua bucket S3 di akunnya. Karena dia adalah pemanggil API, CloudTrail mencatat peristiwa data di jejaknya. Meskipun Bob memiliki akses ke ember, dia bukan pemilik sumber daya, jadi tidak ada acara yang dicatat di jejaknya kali ini. Sebagai pemilik sumber daya, Anda menerima acara di jalan Anda tentang `GetObject` operasi yang dipanggil Mary. CloudTrailmenagih akun Anda dan akun Mary untuk setiap salinan peristiwa data: satu di jejak Mary, dan satu di milik Anda.

Read-only dan acara khusus tulis

Saat mengonfigurasi penyimpanan data jejak atau peristiwa untuk mencatat data dan peristiwa manajemen, Anda dapat menentukan apakah Anda menginginkan peristiwa hanya-baca, peristiwa hanya-tulis, atau keduanya.

- Baca

  Peristiwa baca mencakup operasi API yang membaca sumber daya Anda, tetapi tidak membuat perubahan. Misalnya, peristiwa hanya-baca mencakup operasi API `DescribeSecurityGroups` dan `DescribeSubnets` Amazon EC2. Operasi ini hanya menampilkan informasi tentang sumber daya Amazon EC2 Anda dan tidak mengubah konfigurasi Anda.
- Menulis

  Peristiwa tulis mencakup operasi API yang memodifikasi (atau mungkin memodifikasi) sumber daya Anda. Misalnya, operasi API `RunInstances` dan `TerminateInstances` Amazon EC2 memodifikasi instans Anda.

Contoh: Mencatat peristiwa baca dan tulis untuk jalur terpisah

Contoh berikut menunjukkan bagaimana Anda dapat mengonfigurasi jejak untuk membagi aktivitas log untuk akun menjadi bucket S3 terpisah: satu bucket bernama amzn-s3-demo-bucket1 menerima peristiwa hanya-baca dan amzn-s3-demo-bucket2 kedua menerima peristiwa hanya-tulis.

1. Anda membuat jejak dan memilih bucket S3 bernama `amzn-s3-demo-bucket1` untuk menerima file log. Anda kemudian memperbarui jejak untuk menentukan bahwa Anda ingin Baca peristiwa manajemen dan peristiwa data.
2. Anda membuat jejak kedua dan memilih bucket S3 `amzn-s3-demo-bucket2` untuk menerima file log. Anda kemudian memperbarui jejak untuk menentukan bahwa Anda ingin Menulis peristiwa manajemen dan peristiwa data.
3. Operasi Amazon EC2 `DescribeInstances` dan `TerminateInstances` API terjadi di akun Anda.
4. Operasi `DescribeInstances` API adalah peristiwa hanya-baca dan cocok dengan pengaturan untuk jejak pertama. Jejak mencatat dan mengirimkan acara ke. `amzn-s3-demo-bucket1`
5. Operasi `TerminateInstances` API adalah acara khusus tulis dan cocok dengan pengaturan untuk jejak kedua. Jejak mencatat dan mengirimkan acara ke. `amzn-s3-demo-bucket2`

Mencatat peristiwa data dengan Konsol Manajemen AWS

Prosedur berikut menjelaskan cara memperbarui penyimpanan data peristiwa yang ada atau jejak untuk mencatat peristiwa data dengan menggunakan Konsol Manajemen AWS. Untuk informasi tentang cara membuat penyimpanan data peristiwa untuk mencatat peristiwa data, lihatMembuat penyimpanan data acara untuk CloudTrail acara dengan konsol. Untuk informasi tentang cara membuat jejak untuk mencatat peristiwa data, lihatMembuat jejak dengan konsol.

Untuk jejak, langkah-langkah untuk mencatat peristiwa data berbeda berdasarkan apakah Anda menggunakan penyeleksi peristiwa lanjutan atau pemilih acara dasar. Anda dapat mencatat peristiwa data untuk semua jenis sumber daya menggunakan pemilih peristiwa lanjutan, tetapi jika Anda menggunakan pemilih peristiwa dasar, Anda dibatasi untuk mencatat peristiwa data untuk bucket Amazon S3 dan objek bucket, fungsi AWS Lambda , dan tabel Amazon DynamoDB.

Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa data menggunakan konsol

Gunakan prosedur berikut untuk memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa data. Untuk informasi selengkapnya tentang penggunaan pemilih acara tingkat lanjut, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut di topik ini.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Penyimpanan data acara.

3. Pada halaman Penyimpanan data acara, pilih penyimpanan data acara yang ingin Anda perbarui.

> **Note**
>
> Anda hanya dapat mengaktifkan peristiwa data pada penyimpanan data acara yang berisi CloudTrail peristiwa. Anda tidak dapat mengaktifkan peristiwa data pada penyimpanan data CloudTrail peristiwa untuk item AWS Config konfigurasi, peristiwa CloudTrail Wawasan, atau AWS non-peristiwa.

4. Pada halaman detail, dalam peristiwa Data, pilih Edit.
5. Jika Anda belum mencatat peristiwa data, pilih kotak centang Peristiwa data.
6. Untuk tipe Sumber Daya, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data.
7. Pilih templat pemilih log. Anda dapat memilih template yang telah ditentukan, atau memilih Custom untuk menentukan kondisi koleksi acara Anda sendiri.

   Anda dapat memilih dari template yang telah ditentukan berikut:

   - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
   - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
   - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, seperti`Put*`,`Delete*`, atau `Write*` peristiwa.
   - Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
   - Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` of`AwsServiceEvent`, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).
8. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.
9. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,`Delete*`, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan `readOnly` pemilih.
- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk menyertakan atau mengecualikan peristiwa data apa pun yang dicatat CloudTrail, sepertiPutBucket,`GetItem`, atau`GetSnapshotBlock`.
- **`eventSource`**— Sumber acara untuk menyertakan atau mengecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk dikecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType`diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- Sesi CredentialFromConsole — Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- pengguna Identity.arn - Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.`ARN, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai. `resources.type`

> **Note**
>
> Anda tidak dapat menggunakan `resources.ARN` bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Kunci tindakan, sumber daya, dan kondisi Layanan AWS di Referensi Otorisasi Layanan.

b. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data acara, Anda dapat menyetel bidang ke Resources.arn, mengatur operator untuk tidak memulai, lalu menempelkan ARN bucket S3 yang tidak ingin Anda catat peristiwa.

   Untuk menambahkan bucket S3 kedua, pilih + Condition, lalu ulangi instruksi sebelumnya, tempelkan di ARN untuk atau jelajahi bucket yang berbeda.

   Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

c. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan tentukan ARN dalam satu pemilih agar sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

10. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 6 melalui langkah ini untuk mengonfigurasi penyeleksi acara lanjutan untuk jenis sumber daya lain.
11. Setelah Anda meninjau dan memverifikasi pilihan Anda, pilih Simpan perubahan.

Memperbarui jejak yang ada untuk mencatat peristiwa data dengan pemilih acara lanjutan menggunakan konsol

Dalam Konsol Manajemen AWS, jika jejak Anda menggunakan pemilih acara lanjutan, Anda dapat memilih dari templat yang telah ditentukan sebelumnya yang mencatat semua peristiwa data pada sumber daya yang dipilih. Setelah Anda memilih template pemilih log, Anda dapat menyesuaikan template untuk menyertakan hanya peristiwa data yang paling ingin Anda lihat. Untuk informasi selengkapnya tentang penggunaan pemilih acara tingkat lanjut, lihat Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut di topik ini.

1. Pada halaman Dashboard atau Trails CloudTrail konsol, pilih jejak yang ingin Anda perbarui.
2. Pada halaman detail, dalam peristiwa Data, pilih Edit.
3. Jika Anda belum mencatat peristiwa data, pilih kotak centang Peristiwa data.
4. Untuk tipe Sumber Daya, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data.
5. Pilih templat pemilih log. Anda dapat memilih template yang telah ditentukan, atau memilih Custom untuk menentukan kondisi koleksi acara Anda sendiri.

   Anda dapat memilih dari template yang telah ditentukan berikut:

   - Catat semua peristiwa – Pilih templat ini untuk mencatat semua peristiwa.
   - Log hanya membaca peristiwa - Pilih template ini untuk log hanya membaca peristiwa. Read-only peristiwa adalah peristiwa yang tidak mengubah keadaan sumber daya, seperti `Get*` atau `Describe*` peristiwa.
   - Log hanya menulis peristiwa - Pilih template ini untuk log hanya menulis peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau `Write*` peristiwa.
   - Log hanya Konsol Manajemen AWS peristiwa - Pilih template ini untuk log hanya peristiwa yang berasal dari. Konsol Manajemen AWS
   - Kecualikan peristiwa Layanan AWS yang dimulai - Pilih templat ini untuk mengecualikan Layanan AWS peristiwa, yang memiliki `eventType` ofAwsServiceEvent, dan peristiwa yang dimulai dengan peran Layanan AWS-linked (SLR).

   > **Note**
   >
   > Memilih template yang telah ditentukan untuk bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket

apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.

Jika jejak hanya berlaku untuk satu Wilayah, memilih templat yang telah ditentukan sebelumnya yang mencatat semua bucket S3 memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS

Jika Anda membuat jejak untuk semua Wilayah, memilih templat yang telah ditentukan untuk fungsi Lambda memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di akun AWS Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (untuk jalur, ini hanya dapat dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah itu setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.

Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

6. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log peristiwa data hanya untuk dua bucket S3”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.
7. Jika Anda memilih Kustom, di Penyeleksi acara lanjutan membangun ekspresi berdasarkan nilai bidang pemilih peristiwa lanjutan.

> **Note**
>
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Read-onlyperistiwa data adalah peristiwa yang tidak mengubah status sumber daya, seperti `Get*` atau `Describe*` peristiwa. Menulis peristiwa menambah, mengubah, atau menghapus sumber daya, atribut, atau artefak, sepertiPut*,Delete*, atau `Write*` peristiwa. Untuk mencatat keduanya `read` dan `write` peristiwa, jangan tambahkan `readOnly` pemilih.
- **`eventName`**- `eventName` dapat menggunakan operator apa pun. Anda dapat menggunakannya untuk menyertakan atau mengecualikan peristiwa data apa pun yang dicatat CloudTrail, sepertiPutBucket,GetItem, atauGetSnapshotBlock.
- **`eventSource`**— Sumber acara untuk menyertakan atau mengecualikan. Bidang ini dapat menggunakan operator apa pun.
- eventType – Jenis peristiwa yang harus disertakan atau dikecualikan. Misalnya, Anda dapat mengatur bidang ini ke tidak sama dengan `AwsServiceEvent` untuk dikecualikanLayanan AWS acara. Untuk daftar jenis acara, lihat `eventType`diCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.
- Sesi CredentialFromConsole — Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke sama atau tidak sama dengan nilai. `true`
- pengguna Identity.arn - Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.
- **`resources.ARN`**- Anda dapat menggunakan operator apa pun dengan`resources.`ARN, tetapi jika Anda menggunakan sama atau tidak sama, nilainya harus sama persis dengan ARN dari sumber daya yang valid dari jenis yang telah Anda tentukan dalam template sebagai nilai. `resources.type`

> **Note**
>
> Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Kunci tindakan, sumber daya, dan kondisi Layanan AWS di Referensi Otorisasi Layanan.

b. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat. Misalnya, untuk mengecualikan peristiwa data untuk dua bucket S3 dari peristiwa data yang dicatat di penyimpanan data acara, Anda dapat menyetel bidang ke Resources.arn, mengatur operator untuk tidak memulai, lalu menempelkan ARN bucket S3 yang tidak ingin Anda catat peristiwa.

   Untuk menambahkan bucket S3 kedua, pilih + Condition, lalu ulangi instruksi sebelumnya, tempelkan di ARN untuk atau jelajahi bucket yang berbeda.

   Untuk informasi tentang cara CloudTrail mengevaluasi beberapa kondisi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi pada penyimpanan data acara. Ini termasuk array dari beberapa nilai untuk pemilih seperti. `eventName` Jika Anda memiliki nilai tunggal untuk semua pemilih, Anda dapat memiliki maksimum 500 kondisi yang ditambahkan ke pemilih.

c. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang. Misalnya, jangan tentukan ARN dalam satu pemilih agar sama dengan nilai, lalu tentukan bahwa ARN tidak sama dengan nilai yang sama di pemilih lain.

8. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 4 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk jenis sumber daya.
9. Setelah Anda meninjau dan memverifikasi pilihan Anda, pilih Simpan perubahan.

Perbarui jejak yang ada untuk mencatat peristiwa data dengan pemilih acara dasar menggunakan konsol

Gunakan prosedur berikut untuk memperbarui jejak yang ada untuk mencatat peristiwa data menggunakan pemilih acara dasar.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Buka halaman Trails CloudTrail konsol dan pilih nama jejak.

> **Note**
>
> Meskipun Anda dapat mengedit jejak yang ada untuk mencatat peristiwa data, sebagai praktik terbaik, pertimbangkan untuk membuat jejak terpisah khusus untuk mencatat peristiwa data.

3. Untuk peristiwa Data, pilih Edit.
4. Untuk ember Amazon S3:
   a. Untuk sumber peristiwa Data, pilih S3.
   b. Anda dapat memilih untuk mencatat Semua bucket S3 saat ini dan masa depan, atau Anda dapat menentukan masing-masing bucket atau fungsi. Secara default, peristiwa data dicatat untuk semua bucket S3 saat ini dan masa depan.

> **Note**
>
> Menjaga opsi All current and future S3 bucket default memungkinkan pencatatan peristiwa data untuk semua bucket yang saat ini ada di AWS akun Anda dan bucket apa pun yang Anda buat setelah Anda selesai membuat jejak. Ini juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada bucket milik AWS akun lain.
> Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), memilih opsi Pilih semua bucket S3 di akun Anda memungkinkan pencatatan peristiwa data untuk semua bucket di Wilayah yang sama dengan jejak Anda dan bucket apa pun yang Anda buat nanti di Wilayah tersebut. Ini tidak akan mencatat peristiwa data untuk bucket Amazon S3 di Wilayah lain di akun Anda. AWS

   c. Jika Anda meninggalkan default, Semua bucket S3 saat ini dan masa depan, pilih untuk mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.
   d. Untuk memilih bucket individual, kosongkan kotak centang Baca dan Tulis untuk Semua bucket S3 saat ini dan masa depan. Dalam pemilihan bucket Individual, telusuri bucket untuk mencatat peristiwa data. Untuk menemukan bucket tertentu, ketikkan awalan bucket

untuk bucket yang Anda inginkan. Anda dapat memilih beberapa ember di jendela ini. Pilih Tambahkan bucket untuk mencatat peristiwa data untuk bucket lainnya. Pilih untuk mencatat peristiwa Baca, sepertiGetObject, Menulis peristiwa, sepertiPutObject, atau keduanya.

Pengaturan ini lebih diutamakan daripada setelan individual yang Anda konfigurasikan untuk masing-masing bucket. Misalnya, jika Anda menentukan peristiwa Pencatatan Baca untuk semua bucket S3, lalu memilih untuk menambahkan bucket tertentu untuk pencatatan peristiwa data, Baca sudah dipilih untuk bucket yang Anda tambahkan. Anda tidak dapat menghapus pilihan. Anda hanya dapat mengonfigurasi opsi untuk Menulis.

Untuk menghapus ember dari logging, pilih X.

5. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data.
6. Untuk fungsi Lambda:

   a. Untuk sumber peristiwa Data, pilih Lambda.

   b. Dalam fungsi Lambda, pilih Semua wilayah untuk mencatat semua fungsi Lambda, atau Fungsi input sebagai ARN untuk mencatat peristiwa data pada fungsi tertentu.

   Untuk mencatat peristiwa data untuk semua fungsi Lambda di AWS akun Anda, pilih Log semua fungsi saat ini dan masa depan. Pengaturan ini lebih diutamakan daripada pengaturan individual yang Anda konfigurasikan untuk fungsi individual. Semua fungsi dicatat, bahkan jika semua fungsi tidak ditampilkan.

   > **Note**
   >
   > Jika Anda membuat jejak untuk semua Wilayah, pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah mana pun setelah Anda selesai membuat jejak. Jika Anda membuat jejak untuk satu Wilayah (dilakukan dengan menggunakan AWS CLI), pilihan ini memungkinkan pencatatan peristiwa data untuk semua fungsi yang saat ini ada di Wilayah tersebut di AWS akun Anda, dan fungsi Lambda apa pun yang mungkin Anda buat di Wilayah tersebut setelah Anda selesai membuat jejak. Itu tidak mengaktifkan pencatatan peristiwa data untuk fungsi Lambda yang dibuat di Wilayah lain.

Pencatatan peristiwa data untuk semua fungsi juga memungkinkan pencatatan aktivitas peristiwa data yang dilakukan oleh pengguna atau peran apa pun di AWS akun Anda, bahkan jika aktivitas tersebut dilakukan pada fungsi milik AWS akun lain.

c. Jika Anda memilih fungsi Input sebagai ARN, masukkan ARN dari fungsi Lambda.

> **Note**
>
> Jika Anda memiliki lebih dari 15.000 fungsi Lambda di akun Anda, Anda tidak dapat melihat atau memilih semua fungsi di CloudTrail konsol saat membuat jejak. Anda masih dapat memilih opsi untuk mencatat semua fungsi, meskipun tidak ditampilkan. Jika Anda ingin mencatat peristiwa data untuk fungsi tertentu, Anda dapat menambahkan fungsi secara manual jika Anda mengetahui ARN-nya. Anda juga dapat menyelesaikan pembuatan jejak di konsol, lalu menggunakan dan put-event-selectors perintah untuk mengonfigurasi pencatatan peristiwa data untuk fungsi Lambda tertentu. AWS CLI Untuk informasi selengkapnya, lihat Mengelola jalur dengan AWS CLI.

7. Untuk menambahkan jenis sumber daya lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data.
8. Untuk tabel DynamoDB:

   a. Untuk sumber peristiwa Data, pilih DynamoDB.

   b. Dalam pemilihan tabel DynamoDB, pilih Browse untuk memilih tabel, atau tempel di ARN tabel DynamoDB yang dapat Anda akses. Sebuah DynamoDB tabel ARN menggunakan format berikut:

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   Untuk menambahkan tabel lain, pilih Tambah baris, dan telusuri tabel atau tempel di ARN tabel yang dapat Anda akses.
9. Pilih Simpan perubahan.

Mencatat peristiwa data dengan AWS Command Line Interface

Anda dapat mengonfigurasi jejak atau penyimpanan data peristiwa untuk mencatat peristiwa data menggunakan file. AWS CLI

Topik

- Mencatat peristiwa data untuk jejak dengan AWS CLI
- Pencatatan peristiwa data untuk menyimpan data acara dengan AWS CLI

Mencatat peristiwa data untuk jejak dengan AWS CLI

Anda dapat mengonfigurasi jejak Anda untuk mencatat manajemen dan peristiwa data menggunakan file. AWS CLI

Note

- Ketahuilah bahwa jika akun Anda mencatat lebih dari satu salinan acara manajemen, Anda dikenakan biaya. Selalu ada biaya untuk mencatat peristiwa data. Untuk informasi selengkapnya, silakan lihat Harga AWS CloudTrail.
- Anda dapat menggunakan pemilih acara lanjutan atau pemilih acara dasar, tetapi tidak keduanya. Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa.
- Jika jejak Anda menggunakan pemilih acara dasar, Anda hanya dapat mencatat jenis sumber daya berikut:
  - `AWS::DynamoDB::Table`
  - `AWS::Lambda::Function`
  - `AWS::S3::Object`

  Untuk mencatat jenis sumber daya tambahan, Anda harus menggunakan pemilih acara lanjutan. Untuk mengonversi jejak menjadi penyeleksi peristiwa lanjutan, jalankan get-event-selectors perintah untuk mengonfirmasi penyeleksi peristiwa saat ini, lalu konfigurasikan pemilih acara lanjutan agar sesuai dengan cakupan pemilih peristiwa sebelumnya, lalu tambahkan pemilih untuk jenis sumber daya apa pun yang ingin Anda catat peristiwa data log.
- Anda dapat menggunakan pemilih peristiwa lanjutan untuk memfilter berdasarkan nilai bidang pemilih acara lanjutan yang didukung bidang pemilih, sehingga Anda dapat mencatat hanya peristiwa data yang diminati. Untuk informasi selengkapnya tentang mengonfigurasi bidang ini, lihat AdvancedFieldSelectordi Referensi

AWS CloudTrail API dan Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut di panduan ini.

Untuk melihat apakah jejak Anda mencatat manajemen dan peristiwa data, jalankan `get-event-selectors`perintah.

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

Perintah mengembalikan penyeleksi acara untuk jejak.

Topik

- Log peristiwa data untuk jejak dengan menggunakan pemilih acara tingkat lanjut
- Catat semua peristiwa Amazon S3 untuk bucket Amazon S3 dengan menggunakan pemilih acara lanjutan
- Masuk Amazon S3 AWS Outposts acara dengan menggunakan penyeleksi acara tingkat lanjut
- Log peristiwa dengan menggunakan pemilih acara dasar

Log peristiwa data untuk jejak dengan menggunakan pemilih acara tingkat lanjut

> **Note**
>
> Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa. Sebelum mengonfigurasi penyeleksi acara lanjutan, jalankan get-event-selectors perintah untuk mengonfirmasi pemilih peristiwa saat ini, lalu konfigurasikan pemilih acara lanjutan agar sesuai dengan cakupan pemilih acara sebelumnya, lalu tambahkan penyeleksi untuk peristiwa data tambahan yang ingin Anda log.

Contoh berikut membuat pemilih peristiwa lanjutan khusus untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen baca dan tulis (dengan menghilangkan `readOnly` pemilih), `PutObject` dan peristiwa `DeleteObject` data untuk semua bucket/prefix kombinasi Amazon S3 kecuali untuk bucket bernama `amzn-s3-demo-bucket` dan peristiwa data untuk fungsi bernama. AWS Lambda `MyLambdaFunction` Karena ini adalah penyeleksi acara lanjutan khusus, setiap set penyeleksi memiliki nama deskriptif. Perhatikan bahwa garis miring adalah bagian dari nilai ARN untuk bucket S3.

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

Contoh mengembalikan pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
```

```
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::amzn-s3-demo-bucket/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Catat semua peristiwa Amazon S3 untuk bucket Amazon S3 dengan menggunakan pemilih acara lanjutan

> **Note**
>
> Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa.

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan semua peristiwa data untuk semua objek Amazon S3 dalam bucket S3 tertentu. Nilai untuk acara S3 untuk `resources.type` bidang tersebut adalah`AWS::S3::Object`. Karena nilai ARN untuk objek S3 dan bucket S3 sedikit berbeda, Anda harus menambahkan `StartsWith` operator untuk `resources.`ARN menangkap semua peristiwa.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] }
            ]
        }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
```

```
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::amzn-s3-demo-bucket/"
                    ]
                }
            ]
        }
    ]
}
```

Masuk Amazon S3 AWS Outposts acara dengan menggunakan penyeleksi acara tingkat lanjut

> **Note**
>
> Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa.

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan semua peristiwa data untuk semua objek Amazon S3 di Outposts di pos terdepan Anda.

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

Log peristiwa dengan menggunakan pemilih acara dasar

Berikut ini adalah contoh hasil dari get-event-selectors perintah yang menunjukkan pemilih acara dasar. Secara default, saat Anda membuat jejak dengan menggunakan AWS CLI, jejak mencatat semua peristiwa manajemen. Secara default, jejak tidak mencatat peristiwa data.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

Untuk mengonfigurasi jejak Anda ke manajemen log dan peristiwa data, jalankan [put-event-selectors](#)perintah.

Contoh berikut menunjukkan cara menggunakan pemilih peristiwa dasar untuk mengonfigurasi jejak Anda agar menyertakan semua peristiwa manajemen dan data untuk objek S3 dalam dua awalan bucket S3. Anda dapat menentukan dari 1 hingga 5 penyeleksi acara untuk jejak. Anda dapat menentukan dari 1 hingga 250 sumber daya data untuk jejak.

> **Note**
>
> Jumlah maksimum sumber daya data S3 adalah 250, jika Anda memilih untuk membatasi peristiwa data dengan menggunakan pemilih acara dasar.

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-demo-bucket1/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2;/prefix2"] }] }]'
```

Perintah mengembalikan pemilih acara yang dikonfigurasi untuk jejak.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::amzn-s3-demo-bucket1/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

Pencatatan peristiwa data untuk menyimpan data acara dengan AWS CLI

Anda dapat mengonfigurasi penyimpanan data acara Anda untuk menyertakan peristiwa data menggunakan AWS CLI. Gunakan `create-event-data-store`perintah untuk membuat penyimpanan data acara baru untuk mencatat peristiwa data. Gunakan `update-event-data-store`perintah untuk memperbarui pemilih acara lanjutan untuk penyimpanan data peristiwa yang ada.

Anda mengonfigurasi pemilih acara lanjutan untuk mencatat peristiwa data di penyimpanan data acara. Untuk daftar bidang yang didukung, lihatMemfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut.

Untuk melihat apakah penyimpanan data acara Anda menyertakan peristiwa data, jalankan `get-event-data-store`perintah.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

Perintah mengembalikan pengaturan untuk penyimpanan data acara.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

Topik

- Sertakan semua acara Amazon S3 untuk bucket tertentu
- Sertakan Amazon S3 di AWS Outposts peristiwa

Sertakan semua acara Amazon S3 untuk bucket tertentu

Contoh berikut menunjukkan cara membuat penyimpanan data peristiwa untuk menyertakan semua peristiwa data untuk semua objek Amazon S3 dalam bucket S3 tujuan umum tertentu dan mengecualikan Layanan AWS peristiwa dan peristiwa yang dihasilkan oleh. `bucket-scanner-role` `userIdentity` Nilai untuk acara S3 untuk `resources.type` bidang tersebut adalah`AWS::S3::Object`. Karena nilai ARN untuk objek S3 dan bucket S3 sedikit berbeda, Anda harus menambahkan `StartsWith` operator untuk `resources.`ARN menangkap semua peristiwa.

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]},
            { "Field": "eventType","NotEquals": ["AwsServiceEvent"]}
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:partition:s3:::amzn-s3-demo-bucket/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                     ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                }
            ]
        }
    ],
```

```
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2024-11-20T20:49:21.766000+00:00"
}
```

Sertakan Amazon S3 di AWS Outposts peristiwa

Contoh berikut menunjukkan cara membuat penyimpanan data peristiwa yang mencakup semua peristiwa data untuk semua objek Amazon S3 di Outposts di pos terdepan Anda.

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
```

```
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

Memfilter peristiwa data dengan menggunakan pemilih acara tingkat lanjut

Bagian ini menjelaskan bagaimana Anda dapat menggunakan penyeleksi peristiwa tingkat lanjut untuk membuat penyeleksi berbutir halus untuk mencatat peristiwa data, yang dapat membantu Anda mengontrol biaya dengan hanya mencatat peristiwa data tertentu yang menarik.

Contoh:

- Anda dapat menyertakan atau mengecualikan panggilan API tertentu dengan menambahkan filter di `eventName` bidang.
- Anda dapat menyertakan atau mengecualikan pencatatan untuk sumber daya tertentu dengan menambahkan filter di `resources.ARN` bidang. Misalnya, jika Anda mencatat peristiwa data S3, Anda dapat mengecualikan pencatatan untuk bucket S3 untuk jejak Anda.
- Anda dapat memilih untuk mencatat hanya peristiwa hanya-tulis atau peristiwa hanya-baca dengan menambahkan filter pada bidang. `readOnly`

Tabel berikut menjelaskan bidang yang didukung untuk memfilter peristiwa data. Untuk daftar bidang yang didukung untuk setiap jenis CloudTrail peristiwa, lihat AdvancedEventSelectordi Referensi AWS CloudTrail API.

Bidang	Diperlukan	Operator yang valid	Deskripsi
eventCategory	Ya	`Equals`	Bidang ini diatur `Data` untuk mencatat peristiwa data.
resources.type	Ya	`Equals`	Bidang ini digunakan untuk memilih jenis sumber daya yang ingin Anda log peristiwa data. Tabel peristiwa Data menunjukkan nilai yang mungkin.
readOnly	Tidak	`Equals`	Ini adalah bidang opsional yang digunakan untuk menyertakan atau mengecualikan peristiwa data berdasark an `readOnly` nilainya. Nilai `true` log hanya membaca peristiwa. Nilai `false` log hanya menulis peristiwa. Jika Anda tidak menambahkan bidang ini, CloudTrail log acara baca dan tulis.

eventName	Tidak	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Ini adalah file opsional yang digunakan untuk menyaring atau menyaring peristiwa data apa pun yang dicatat CloudTrail, seperti atau. `PutBucket` `GetSnapshotBlock`
			Jika Anda menggunakan AWS CLI, Anda dapat menentukan beberapa nilai dengan memisahkan setiap nilai dengan koma.
			Jika Anda menggunakan konsol, Anda dapat menentukan beberapa nilai dengan membuat kondisi untuk setiap yang ingin `eventName` Anda filter.

resources.ARN	Tidak	`EndsWith`	Ini adalah bidang opsional yang digunakan untuk mengecualikan

Bidang	Diperlukan	Operator yang valid	Deskripsi

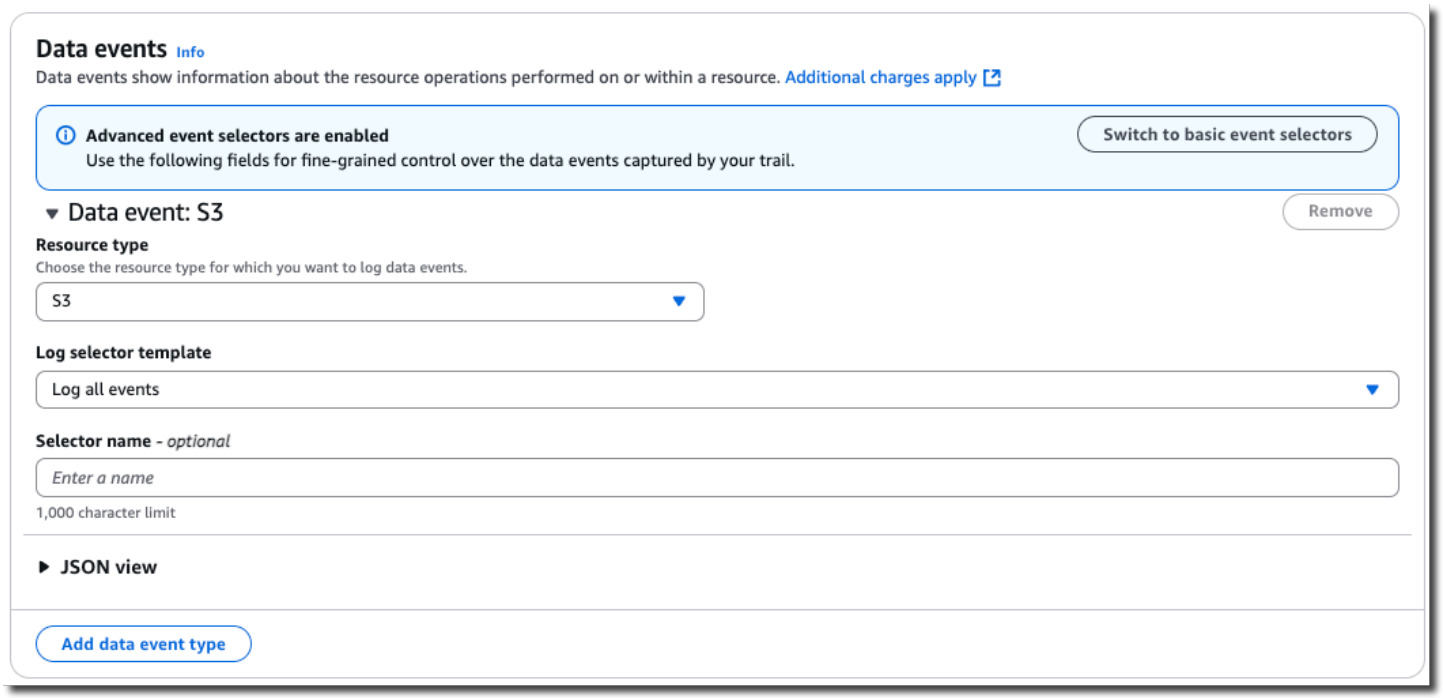
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			atau menyertakan peristiwa data untuk sumber daya tertentu dengan menyediakan`resources.ARN` . Anda dapat menggunakan operator mana pun dengan`resources.ARN` , tetapi jika Anda menggunakan `Equals` atau`NotEquals` , nilainya harus sama persis dengan ARN sumber daya yang valid untuk yang `resources.type` Anda tentukan. Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok.
			
			Jika Anda menggunakan AWS CLI, Anda dapat menentukan beberapa nilai dengan memisahkan setiap nilai dengan koma.
			
			Jika Anda menggunakan konsol, Anda dapat menentukan beberapa nilai dengan membuat kondisi untuk setiap yang ingin `resources.ARN` Anda filter.

Bidang	Diperlukan	Operator yang valid	Deskripsi
eventSource	Tidak	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	Anda dapat menggunakannya untuk menyertakan atau mengecualikan sumber acara tertentu. Biasanya eventSource merupakan bentuk pendek dari nama layanan tanpa spasi plus.amazonaws.com . Misalnya, Anda dapat mengatur eventSource Equals ec2.amazonaws.com untuk hanya mencatat peristiwa data Amazon EC2.
eventType	Tidak	EndsWith Equals NotEndsWith NotEquals NotStartsWith StartsWith	EventType untuk menyertakan atau mengecualikan. Misalnya, Anda dapat mengatur bidang ini NotEquals AwsServiceEvent untuk mengecualikan Layanan AWS peristiwa.
sessionCredentialFromConsole	Tidak	Equals NotEquals	Sertakan atau kecualikan acara yang berasal dari Konsol Manajemen AWS sesi. Bidang ini dapat diatur ke Equals atau NotEquals dengan nilaitrue.

Bidang	Diperlukan	Operator yang valid	Deskripsi

`userIdentity.arn`	Tidak	`EndsWith`
		`Equals`
		`NotEndsWith`
		`NotEquals`
		`NotStartsWith`
		`StartsWith`
			Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

Untuk mencatat peristiwa data menggunakan CloudTrail konsol, Anda memilih opsi Peristiwa data, lalu pilih jenis sumber daya yang diminati saat Anda membuat atau memperbarui penyimpanan data jejak atau peristiwa. Tabel peristiwa data menunjukkan kemungkinan jenis sumber daya yang dapat Anda pilih di CloudTrail konsol.



Untuk mencatat peristiwa data dengan AWS CLI, konfigurasikan `--advanced-event-selector` parameter untuk mengatur `eventCategory` sama dengan `Data` dan `resources.type` nilai sama dengan nilai tipe sumber daya yang ingin Anda log peristiwa data. Tabel peristiwa Data mencantumkan jenis sumber daya yang tersedia.

Misalnya, jika Anda ingin mencatat peristiwa data untuk semua kumpulan Identitas Cognito, Anda akan mengonfigurasi `--advanced-event-selectors` parameter agar terlihat seperti ini:

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

Contoh sebelumnya mencatat semua peristiwa data Cognito di kumpulan Identity. Anda dapat lebih lanjut menyempurnakan pemilih acara lanjutan untuk memfilter pada`eventName`,`readOnly`, dan `resources.`ARN bidang untuk mencatat peristiwa tertentu yang menarik atau mengecualikan peristiwa yang tidak menarik.

Anda dapat mengonfigurasi pemilih acara lanjutan untuk memfilter peristiwa data berdasarkan beberapa bidang. Misalnya, Anda dapat mengonfigurasi penyeleksi peristiwa lanjutan untuk mencatat semua panggilan Amazon `PutObject` S3 `DeleteObject` dan API tetapi mengecualikan pencatatan peristiwa untuk bucket S3 tertentu seperti yang ditunjukkan pada contoh berikut. Ganti *`amzn-s3-demo-bucket`* dengan nama bucket Anda.

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith": ["arn:aws:s3:::amzn-s3-demo-
bucket/"] }
    ]
  }
]'
```

Anda juga dapat menyertakan beberapa kondisi untuk bidang. Untuk informasi tentang bagaimana beberapa kondisi dievaluasi, lihatBagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang.

Anda dapat menggunakan pemilih acara lanjutan untuk mencatat peristiwa manajemen dan data. Untuk mencatat peristiwa data untuk beberapa jenis sumber daya, tambahkan pernyataan pemilih bidang untuk setiap jenis sumber daya yang ingin Anda log peristiwa data.

> **Note**
>
> Trails dapat menggunakan penyeleksi acara dasar atau pemilih acara lanjutan, tetapi tidak keduanya. Jika Anda menerapkan penyeleksi acara lanjutan ke jejak, pemilih acara dasar apa pun yang ada akan ditimpa.
> Selector tidak mendukung penggunaan wildcard seperti. * Untuk mencocokkan beberapa nilai dengan satu kondisi, Anda dapat menggunakan`StartsWith`,`EndsWith`,`NotStartsWith`, atau `NotEndsWith` untuk secara eksplisit mencocokkan awal atau akhir bidang acara.

Topik

- Bagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang
- AWS CLI contoh untuk memfilter peristiwa data

Bagaimana CloudTrail mengevaluasi beberapa kondisi untuk suatu bidang

Untuk penyeleksi acara tingkat lanjut, CloudTrail evaluasi beberapa kondisi untuk bidang sebagai berikut:

- Operator DESELECT adalah DAN akan bersama-sama. Jika salah satu kondisi operator DESELECT terpenuhi, acara tidak dikirimkan. Ini adalah operator DESELECT yang valid untuk pemilih acara tingkat lanjut:
  - `NotEndsWith`
  - `NotEquals`
  - `NotStartsWith`
- Operator SELECT adalah ATAU akan bersama-sama. Ini adalah operator SELECT yang valid untuk pemilih acara tingkat lanjut:
  - `EndsWith`
  - `Equals`
  - `StartsWith`
- Kombinasi operator SELECT dan DESELECT mengikuti aturan di atas dan kedua grup adalah AND 'd bersama-sama.

Contoh yang menunjukkan beberapa kondisi untuk bidang **`Resources.arn`**

Contoh pernyataan pemilih peristiwa berikut mengumpulkan peristiwa data untuk jenis `AWS::S3::Object` sumber daya dan menerapkan beberapa kondisi di `resources.ARN` lapangan.

```
{
    "Name": "S3Select",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
```

```
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "resources.ARN",
        "Equals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object1"
        ],
        "StartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "EndsWith": [
          "object3"
        ],
        "NotStartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/deselect"
        ],
        "NotEndsWith": [
          "object5"
        ],
        "NotEquals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object6"
        ]
      }
    ]
  }
```

Dalam contoh sebelumnya, peristiwa data Amazon S3 untuk sumber daya akan `AWS::S3::Object` dikirimkan jika:

1. Tak satu pun dari kondisi operator DESELECT ini terpenuhi:
   - `resources.ARN`bidang `NotStartsWith` nilainya `arn:aws:s3:::amzn-s3-demo-bucket/deselect`
   - `resources.ARN`bidang `NotEndsWith` nilainya `object5`
   - `resources.ARN`bidang `NotEquals` nilainya `arn:aws:s3:::amzn-s3-demo-bucket/object6`
2. Setidaknya satu dari kondisi operator SELECT ini terpenuhi:
   - `resources.ARN`bidang `Equals` nilainya `arn:aws:s3:::amzn-s3-demo-bucket/object1`

- `resources.ARN`bidang `StartsWith` nilainya `arn:aws:s3:::amzn-s3-demo-bucket/`
- `resources.ARN`bidang `EndsWith` nilainya `object3`

Berdasarkan logika evaluasi:

1. Peristiwa data untuk `amzn-s3-demo-bucket/object1` akan dikirimkan karena cocok dengan nilai untuk `Equals` operator dan tidak cocok dengan nilai apa pun untuk`NotStartsWith`,`NotEndsWith`, dan `NotEquals` operator.
2. Peristiwa data untuk `amzn-s3-demo-bucket/object2` akan dikirimkan karena cocok dengan nilai untuk `StartsWith` operator dan tidak cocok dengan nilai apa pun untuk`NotStartsWith`,`NotEndsWith`, dan `NotEquals` operator.
3. Peristiwa data untuk `amzn-s3-demo-bucket1/object3` akan dikirimkan karena cocok dengan `EndsWith` operator dan tidak cocok dengan nilai apa pun untuk`NotStartsWith`,`NotEndsWith`, dan `NotEquals` operator.
4. Peristiwa data untuk tidak `arn:aws:s3:::amzn-s3-demo-bucket/deselectObject4` akan dikirimkan karena cocok dengan kondisi untuk `NotStartsWith` meskipun sesuai dengan kondisi untuk `StartsWith` operator.
5. Peristiwa data untuk tidak `arn:aws:s3:::amzn-s3-demo-bucket/object5` akan dikirimkan karena cocok dengan kondisi untuk `NotEndsWith` meskipun sesuai dengan kondisi untuk `StartsWith` operator.
6. Peristiwa data untuk tidak `arn:aws:s3:::amzn-s3-demo-bucket/object6` akan terkirim karena sesuai dengan kondisi `NotEquals` operator meskipun sesuai dengan kondisi `StartsWith` operator.

AWS CLI contoh untuk memfilter peristiwa data

Bagian ini memberikan AWS CLI contoh yang menunjukkan cara memfilter peristiwa data pada bidang yang berbeda. Untuk AWS CLI contoh tambahan, lihat Log peristiwa data untuk jejak dengan menggunakan pemilih acara tingkat lanjut danPencatatan peristiwa data untuk menyimpan data acara dengan AWS CLI.

Untuk informasi tentang cara mencatat peristiwa data menggunakan konsol, lihatMencatat peristiwa data dengan Konsol Manajemen AWS.

Contoh:

- Contoh 1: Pemfilteran pada bidang EventName
- Contoh 2: Memfilter pada bidang Resources.arn dan pengguna Identity.arn
- Contoh 3: Memfilter pada bidang resources.type dan eventName untuk mengecualikan objek individual yang dihapus oleh peristiwa Amazon S3 DeleteObjects
- Contoh 4: Memfilter pada bidang EventSource untuk mengecualikan peristiwa data siklus hidup Amazon S3
- Contoh 5: Memfilter pada bidang EventSource untuk mengecualikan peristiwa data kegagalan autentikasi Amazon S3

Contoh 1: Pemfilteran pada bidang **`EventName`**

Pada contoh pertama, `--advanced-event-selectors` for a trail dikonfigurasi untuk mencatat hanya panggilan`GetObject`,`PutObject`, dan `DeleteObject` API untuk objek Amazon S3 dalam bucket tujuan umum.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

Contoh berikutnya membuat penyimpanan data peristiwa baru yang mencatat peristiwa data untuk EBS Direct API tetapi mengecualikan panggilan `ListChangedBlocks` API. Anda dapat menggunakan update-event-data-storeperintah untuk memperbarui penyimpanan data acara yang ada.

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
```

```
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
        ]
    }
]'
```

Contoh 2: Memfilter pada bidang Resources.arn dan pengguna Identity.arn

Contoh berikut menunjukkan cara menyertakan semua peristiwa data untuk semua objek Amazon S3 dalam bucket S3 tujuan umum tertentu tetapi mengecualikan peristiwa yang dihasilkan oleh. `bucket-scanner-role` `userIdentity` Nilai untuk acara S3 untuk `resources.type` bidang tersebut adalah`AWS::S3::Object`. Karena nilai ARN untuk objek S3 dan bucket S3 sedikit berbeda, Anda harus menambahkan operator untuk. `StartsWith` `resources.ARN`

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

Contoh 3: Memfilter pada bidang **`resources.type`** dan **`eventName`** untuk mengecualikan objek individual yang dihapus oleh peristiwa Amazon S3 DeleteObjects

Contoh berikut menunjukkan cara menyertakan semua peristiwa data untuk semua objek Amazon S3 dalam bucket Amazon S3 tujuan umum tertentu tetapi mengecualikan objek individual yang dihapus oleh operasi. `DeleteObject` Nilai untuk acara S3 untuk `resources.type` bidang tersebut adalah`AWS::S3::Object`. Nilai untuk nama acara adalah`DeleteObject`.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
```

```
--advanced-event-selectors \

{
    "Name": "Exclude Events for DeleteObject operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "NotEquals": [
          "DeleteObject"
        ]
      }
    ]
  },
  {
    "Name": "Exclude DeleteObject Events for individual objects deleted by
 DeleteObjects Operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "Equals": [
```

```
          "DeleteObject"
        ]
      },
      {
        "Field": "eventType",
        "NotEquals": [
          "AwsServiceEvent"
        ]
      }
    ]
  }
] (edited)
```

Contoh 4: Memfilter pada bidang **`EventSource`** untuk mengecualikan peristiwa data siklus hidup Amazon S3

Contoh berikut menunjukkan cara mencatat semua peristiwa data Amazon S3 tetapi mengecualikan operasi siklus hidup Amazon S3. Operasi ini mencakup kedaluwarsa objek, pembuatan penanda hapus, transisi kelas penyimpanan, dan pengguguran unggahan multibagian. Acara siklus hidup Amazon S3 menggunakan sumber peristiwa. `s3lifecycle.amazonaws.com` Dengan memfilter sumber `s3lifecycle.amazonaws.com` peristiwa menggunakan `NotEquals` operator, Anda dapat mengecualikan peristiwa yang dimulai layanan ini sambil terus mencatat semua peristiwa data Amazon S3 yang dimulai pengguna.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
  {
    "Name": "Log S3 data events but exclude lifecycle operations",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventSource", "NotEquals": ["s3lifecycle.amazonaws.com"] }
    ]
  }
]'
```

Contoh 5: Memfilter pada bidang **`EventSource`** untuk mengecualikan peristiwa data kegagalan autentikasi Amazon S3

Contoh berikut menunjukkan cara mencatat semua peristiwa data Amazon S3 tetapi mengecualikan peristiwa kegagalan autentikasi Amazon S3, sepertiAuthenticateSignatureDoesNotMatch,, dan. AuthenticateInvalidAccessKeyId AuthenticateExpiredToken Peristiwa kegagalan otentikasi Amazon S3 menggunakan sumber peristiwa. s3-authn-errors.amazonaws.com Dengan memfilter sumber s3-authn-errors.amazonaws.com acara menggunakan NotEquals operator, Anda dapat mengecualikan peristiwa ini sambil terus mencatat semua peristiwa data Amazon S3 yang berhasil.

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
  {
    "Name": "Log S3 data events but exclude authentication failure events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventSource", "NotEquals": ["s3-authn-errors.amazonaws.com"] }
    ]
  }
]'
```

Pemilih acara lanjutan ini menyaring semua peristiwa di mana eventSource beradas3-authn-errors.amazonaws.com. Kejadian kegagalan otentikasi mengikuti pola penamaan Authenticate diikuti oleh kode kesalahan (misalnya,,AuthenticateSignatureDoesNotMatch, AuthenticateInvalidAccessKeyIdAuthenticateExpiredToken,AuthenticateInvalidToken). Mengecualikan peristiwa ini dapat membantu mengurangi biaya jika Anda tidak perlu mengaudit upaya otentikasi yang gagal terhadap sumber daya Amazon S3 Anda.

Mengagregasikan peristiwa data

Peristiwa data memberikan informasi tentang operasi sumber daya yang dilakukan pada atau di sumber daya. Ini juga dikenal sebagai operasi bidang data. Peristiwa data sering kali merupakan aktivitas bervolume tinggi.

Dengan mengaktifkan agregasi pada peristiwa data Anda, Anda dapat secara efisien memantau pola akses data volume tinggi tanpa memproses sejumlah besar peristiwa individual. Fitur ini secara

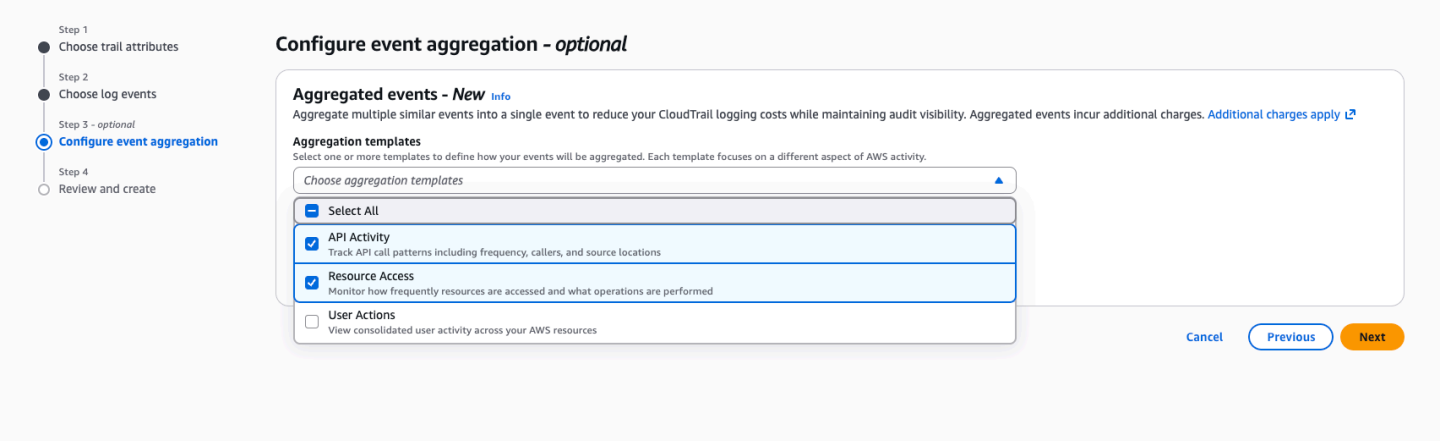
otomatis mengkonsolidasikan peristiwa data ke dalam ringkasan 5 menit, menunjukkan tren utama seperti frekuensi akses, tingkat kesalahan, dan tindakan yang paling sering digunakan. Misalnya, alih-alih memproses ribuan peristiwa akses bucket S3 individual untuk memahami pola penggunaan, Anda menerima ringkasan gabungan yang menunjukkan pengguna dan tindakan teratas.

Anda dapat mengaktifkan agregasi pada peristiwa data saat membuat jejak baru atau memperbarui jejak yang ada yang mengumpulkan peristiwa data. Anda dapat memilih salah satu atau semua dari tiga template out-of-the-box untuk menggabungkan peristiwa data Anda pada:

- Aktivitas API untuk mendapatkan ringkasan 5 menit dari peristiwa data Anda berdasarkan panggilan API yang dilakukan. Gunakan ini untuk memahami pola penggunaan API Anda, termasuk frekuensi, penelepon, dan sumber.
- Akses Sumber Daya untuk mendapatkan pola aktivitas pada AWS sumber daya Anda. Gunakan ini untuk memahami bagaimana AWS sumber daya Anda diakses, berapa kali mereka diakses di jendela 5 menit, siapa yang mengakses sumber daya, dan tindakan apa yang sedang dilakukan.
- Tindakan Pengguna untuk mendapatkan pola aktivitas berdasarkan prinsip IAM yang melakukan panggilan API di akun Anda.

Mengaktifkan agregasi untuk peristiwa data menggunakan konsol

Untuk mengaktifkan agregasi pada jejak, pertama-tama Anda memilih pencatatan peristiwa data saat membuat atau memperbarui jejak dan mengonfigurasi peristiwa data untuk mencatat peristiwa di jejak. Kemudian, pada langkah konfigurasikan agregasi acara, Anda dapat memilih template seperti Aktivitas API dan Akses Sumber Daya dari dropdown template agregasi seperti yang ditunjukkan pada gambar di bawah ini.



Mengaktifkan agregasi untuk peristiwa data menggunakan AWS CLI

Anda dapat mengonfigurasi jejak Anda untuk menggabungkan peristiwa menggunakan. AWS CLI

Untuk melihat apakah jejak Anda menggabungkan peristiwa data, jalankan perintah. `get-event-configurations`

```
aws cloudtrail get-event-configuration --region us-east-1 --trail-name TrailName
```

Perintah mengembalikan konfigurasi agregasi untuk jejak.

Sebelum mengaktifkan agregasi acara, Anda harus membuat jejak dan mengonfigurasi peristiwa data di dalamnya.

Untuk mengaktifkan agregasi acara di jalur, ikuti langkah di bawah ini. Jejak akan menggabungkan peristiwa berdasarkan templat `API_ACTIVITY` dan `RESOURCE_ACCESS` agregasi.

```
aws cloudtrail put-event-configuration --region us-east-1 --trail TrailName \
--aggregation-configurations \
'[
    {
        "EventCategory": "Data",
        "Templates":
        [
            "API_ACTIVITY",
            "RESOURCE_ACCESS"
        ]
    }
]'
```

Contoh: peristiwa agregat API_ACTIVITY

Berikut ini menunjukkan contoh peristiwa agregat untuk `API_ACTIVITY` template:

```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "62759c1a-6248-48e1-a6b3-d5fb7e6c4bc0",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-west-2",
    "eventSource": "s3.amazonaws.com",
    "timeWindow":
```

```
    {
        "windowStart": "2025-11-17T19:20:00Z",
        "windowEnd": "2025-11-17T19:25:00Z",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "eventName",
            "statistics":
            [
                {
                    "name": "PutObject",
                    "value": 1000
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
            {
                "dimension": "resourceARN",
                "statistics":
                [
                    {
                        "name": "arn:aws:s3:::bucket-1",
                        "value": 800
                    },
                    {
                        "name": "arn:aws:s3:::bucket-2",
                        "value": 150
                    },
                    {
                        "name": "arn:aws:s3:::bucket-3",
                        "value": 50
                    }
                ],
                "aggregationType": "Count"
            }
        ]
    }
}
```

Contoh: RESOURCE_ACCESS peristiwa agregat

Berikut ini menunjukkan contoh peristiwa agregat untuk `RESOURCE_ACCESS` template:


```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "2ed87efa-45c1-412d-bc38-7e0879faa6df",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-west-2",
    "eventSource": "s3.amazonaws.com",
    "timeWindow":
    {
        "windowStart": "2025-11-17T19:20:00Z",
        "windowEnd": "2025-11-17T19:25:00Z",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "resourceARN",
            "statistics":
            [
                {
                    "name": "arn:aws:s3:::bucket-1",
                    "value": 800
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
            {
                "dimension": "eventName",
                "statistics":
                [
                    {
                        "name": "PutObject",
                        "value": 800
                    }
                ],
                "aggregationType": "Count"
```

```
            }
        ]
    }
}
```

Peristiwa data pencatatan untuk AWS Config kepatuhan

Jika Anda menggunakan paket AWS Config kesesuaian untuk membantu perusahaan Anda mempertahankan kepatuhan terhadap standar formal seperti yang disyaratkan oleh Federal Risk and Authorization Management Program (FedRAMP) atau National Institute of Standards and Technology (NIST), paket kesesuaian untuk kerangka kerja kepatuhan umumnya mengharuskan Anda untuk mencatat peristiwa data untuk bucket Amazon S3, minimal. Paket kesesuaian untuk kerangka kerja kepatuhan mencakup aturan terkelola yang disebut `cloudtrail-s3-dataevents-enabled`yang memeriksa pencatatan peristiwa data S3 di akun Anda. Banyak paket kesesuaian yang tidak terkait dengan kerangka kerja kepatuhan juga memerlukan pencatatan peristiwa data S3. Berikut ini adalah contoh paket kesesuaian yang menyertakan aturan ini.

- Praktik Terbaik Operasional untuk Pilar Keamanan AWS Well-Architected Kerangka Kerja
- Praktik Terbaik Operasional untuk FDA Judul 21 CFR Bagian 11
- Praktik Terbaik Operasional untuk FFIEC
- Praktik Terbaik Operasional untuk FedRAMP (Sedang)
- Praktik Terbaik Operasional untuk Keamanan HIPAA
- Praktik Terbaik Operasional untuk K-ISMS
- Praktik Terbaik Operasional untuk Penebangan

Untuk daftar lengkap paket kesesuaian sampel yang tersedia di AWS Config, lihat Templat sampel paket kesesuaian di Panduan Pengembang.AWS Config

Mencatat peristiwa data dengan AWS SDK

Jalankan GetEventSelectorsoperasi untuk melihat apakah jejak Anda mencatat peristiwa data. Anda dapat mengonfigurasi jejak Anda untuk mencatat peristiwa data dengan menjalankan PutEventSelectorsoperasi. Untuk informasi lebih lanjut, lihat Referensi API AWS CloudTrail.

Jalankan GetEventDataStoreoperasi untuk melihat apakah penyimpanan data acara Anda mencatat peristiwa data. Anda dapat mengonfigurasi penyimpanan data acara Anda untuk menyertakan peristiwa data dengan menjalankan UpdateEventDataStoreoperasi CreateEventDataStoreatau dan

menentukan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI dan Referensi AWS CloudTrail API.

Menekan peristiwa rekursif dengan logging rekursif

Apa itu logging rekursif?

Saat CloudTrail mengirimkan file log ke tujuan jejak, operasi pengiriman tersebut dapat dicatat sendiri sebagai peristiwa. Tujuan termasuk bucket Amazon S3 atau grup CloudWatch log Log. Misalnya, saat CloudTrail mengirimkan file log ke bucket Amazon S3 Anda, ia akan melakukan panggilan `PutObject` API. Jika jejak Anda dikonfigurasi untuk mencatat peristiwa data Amazon S3, operasi pengiriman ini dicatat sebagai peristiwa, yang kemudian dikirim ke bucket Anda, menghasilkan peristiwa lain, dan seterusnya. Ini disebut peristiwa rekursif.

Anda dapat menggunakan `RecursiveLogging` pengaturan untuk menekan peristiwa ini.

Cara kerja penekanan logging rekursif

Saat Anda mengatur `RecursiveLogging` `false` pada jejak, CloudTrail menekan peristiwa pengiriman rekursif. CloudTrail menyaring peristiwa di mana `userIdentity.invokedBy` ada `cloudtrail.amazonaws.com` dan `eventSource` dan `eventName` cocok dengan salah satu dari berikut ini:

- `eventSource`adalah `s3.amazonaws.com` dan `eventName` sedang `PutObject`
- `eventSource`adalah `logs.amazonaws.com` dan `eventName` sedang `PutLogEvents`

Pengaturan ini hanya menekan peristiwa di mana layanan yang CloudTrail dipanggil. Semua acara lainnya disampaikan seperti yang diharapkan.

Mengkonfigurasi logging rekursif

Anda dapat mengonfigurasi `RecursiveLogging` pengaturan saat membuat atau memperbarui jejak.

Menonaktifkan logging rekursif (menekan peristiwa rekursif)

Untuk menekan peristiwa rekursif saat membuat jejak, gunakan `--no-recursive-logging` opsi:

```
aws cloudtrail create-trail \
    --name my-trail \
    --s3-bucket-name my-bucket \
```

```
    --no-recursive-logging
```

Untuk menekan peristiwa rekursif pada jejak yang ada:

```
aws cloudtrail update-trail \
    --name my-trail \
    --no-recursive-logging
```

Re-enabling pencatatan rekursif

Untuk mengaktifkan kembali logging rekursif (mengirimkan peristiwa rekursif):

```
aws cloudtrail update-trail \
    --name my-trail \
    --recursive-logging
```

Perilaku default

Secara default, `RecursiveLogging` diatur ke `true` pada semua jalur. Ini berarti peristiwa pengiriman rekursif dicatat. Jika Anda tidak menyetel `RecursiveLogging` secara eksplisit`false`, jejak Anda akan terus menerima semua peristiwa, termasuk yang dihasilkan oleh operasi CloudTrail pengiriman.

Mencatat peristiwa aktivitas jaringan

CloudTrail peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Peristiwa aktivitas jaringan memberikan visibilitas ke dalam operasi sumber daya yang dilakukan dalam VPC. Misalnya, mencatat peristiwa aktivitas jaringan dapat membantu pemilik titik akhir VPC mendeteksi saat kredensi dari luar organisasi mereka mencoba mengakses titik akhir VPC mereka.

Anda dapat mencatat peristiwa aktivitas jaringan untuk layanan berikut:

- Amazon Aurora DSQL
- Amazon Bedrock
- ID Suara Amazon Connect
- EventBridge Penjadwal Amazon
- Amazon Fraud Detector
- Amazon HealthLake

- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Langganan Amazon Q
- Amazon QuickSight
- Amazon Rekognition
- Amazon SageMaker
- Amazon Textract
- Layanan Streaming Amazon Transcribe
- Izin Terverifikasi Amazon
- Amazon WorkMail
- Platform Pengembang Anthropic Claude di AWS
- Athena
- AWS Registri Agen
- AWS AppConfig
- jaminan aws
- AWS Pertukaran Data B2B
- AWS Kalkulator Harga BCM
- AWS Penagihan
- AWS Cloud Map
- AWS Peringatan Dioda
- AWS Glue
- AWS IdentityStore Layanan
- AWS Faktur
- AWS IoT FleetWise
- AWS Terowongan Aman IoT
- AWS IoT SiteWise
- AWS License Manager
- AWS Pengukuran Pendapatan Pusat Mitra
- AWS Secrets Manager
- AWS SSO

- AWS Step Functions
- AWS Transfer Family
- AWS Transformasi
- AWSBillingAndCostManagementDataExports
- AWSLakeFormation
- Gerbang Cadangan
- Inti Agen Batuan Dasar
- API Kontrol Awan
- CloudFormation
- CloudHSM
- CloudTrail
- CodeDeploy
- Comprehend medis
- Otomatisasi Compute Optimizer
- DynamoDB
- Penskalaan Otomatis EC2
- Elastic Compute Cloud (EC2)
- Sistem File Elastis (EFS)
- pesan pengguna akhir
- IoT
- Layanan Manajemen Kunci (KMS)
- Lambda
- Relational Database Service (RDS) Core Control Plane
- Route 53 DNS Publik
- Vektor S3
- Layanan Token Keamanan (STS)
- Sign-In Portal
- Simple Email Service (SES)
- Simple Notification Service (SNS)
- LAYANAN ANTRIAN SEDERHANA (SQS)

- Simple Storage Service (S3)
- Layanan Alur Kerja Sederhana (SWF)
- Kontak SSM
- Storage Gateway

Anda dapat mengonfigurasi penyimpanan data jejak dan peristiwa untuk mencatat peristiwa aktivitas jaringan.

Secara default, jejak dan penyimpanan data peristiwa tidak mencatat peristiwa aktivitas jaringan. Biaya tambahan berlaku untuk acara aktivitas jaringan. Untuk informasi selengkapnya, silakan lihat AWS CloudTrail Harga.

Daftar Isi

- Bidang pemilih acara lanjutan untuk acara aktivitas jaringan
- Mencatat peristiwa aktivitas jaringan dengan Konsol Manajemen AWS
  - Memperbarui jejak yang ada untuk mencatat peristiwa aktivitas jaringan
  - Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan
- Mencatat peristiwa aktivitas jaringan dengan AWS Command Line Interface
  - Contoh: Mencatat peristiwa aktivitas jaringan untuk jejak
    - Contoh: Log peristiwa aktivitas jaringan untuk CloudTrail operasi
    - Contoh: Log VpceAccessDeniedperistiwa untuk AWS KMS
    - Contoh: Log VpceAccessDeniedperistiwa untuk Amazon S3
    - Contoh: Log VpceAccessDeniedperistiwa EC2 melalui titik akhir VPC tertentu
    - Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara
  - Contoh: Logging peristiwa aktivitas jaringan untuk penyimpanan data acara
    - Contoh: Log semua peristiwa aktivitas jaringan untuk CloudTrail operasi
    - Contoh: Log VpceAccessDeniedperistiwa untuk AWS KMS
    - Contoh: Log VpceAccessDeniedperistiwa EC2 melalui titik akhir VPC tertentu
    - Contoh: Log VpceAccessDeniedperistiwa untuk Amazon S3
    - Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara
- Mencatat peristiwa dengan AWS SDK

Bidang pemilih acara lanjutan untuk acara aktivitas jaringan

Anda mengonfigurasi pemilih peristiwa lanjutan untuk mencatat peristiwa aktivitas jaringan dengan menentukan sumber acara yang ingin Anda log aktivitas. Anda dapat mengonfigurasi penyeleksi peristiwa lanjutan menggunakan AWS SDK, AWS CLI, atau CloudTrail konsol.

Bidang pemilih peristiwa lanjutan berikut diperlukan untuk mencatat peristiwa aktivitas jaringan:

- `eventCategory`— Untuk mencatat peristiwa aktivitas jaringan, nilainya harus`NetworkActivity`. `eventCategory`hanya dapat menggunakan `Equals` operator.
- `eventSource`— Sumber acara yang ingin Anda catat peristiwa aktivitas jaringan. `eventSource`hanya dapat menggunakan `Equals` operator. Jika Anda ingin mencatat peristiwa aktivitas jaringan untuk beberapa sumber peristiwa, Anda harus membuat pemilih bidang terpisah untuk setiap sumber peristiwa.

  Nilai yang valid meliputi:

  - `aco-automation.amazonaws.com`
  - `agent-registry.amazonaws.com`
  - `appconfig.amazonaws.com`
  - `application-signals.amazonaws.com`
  - `appmesh.amazonaws.com`
  - `assurance.amazonaws.com`
  - `athena.amazonaws.com`
  - `autoscaling.amazonaws.com`
  - `aws-external-anthropic.amazonaws.com`
  - `b2bi.amazonaws.com`
  - `backup-gateway.amazonaws.com`
  - `bcm-data-exports.amazonaws.com`
  - `bcm-pricing-calculator.amazonaws.com`
  - `bedrock-agentcore.amazonaws.com`
  - `bedrock.amazonaws.com`
  - `billing.amazonaws.com`
  - `cassandra.amazonaws.com`
  - `ce.amazonaws.com`

- chime-sdk-media-pipelines.amazonaws.com
- chime-sdk-voice.amazonaws.com
- cloudcontrolapi.amazonaws.com
- cloudformation.amazonaws.com
- cloudhsm.amazonaws.com
- cloudtrail.amazonaws.com
- codedeploy.amazonaws.com
- comprehend.amazonaws.com
- comprehendmedical.amazonaws.com
- config.amazonaws.com
- diode-alerting.amazonaws.com
- ds.amazonaws.com
- dsql.amazonaws.com
- dynamodb.amazonaws.com
- ec2.amazonaws.com
- ecr.amazonaws.com
- ecs.amazonaws.com
- elasticfilesystem.amazonaws.com
- elasticloadbalancing.amazonaws.com
- end-user-messaging.amazonaws.com
- events.amazonaws.com
- eventsv2.amazonaws.com
- firehose.amazonaws.com
- frauddetector.amazonaws.com
- freetier.amazonaws.com
- fsx.amazonaws.com
- glue.amazonaws.com
- healthlake.amazonaws.com
- identitystore.amazonaws.com
- invoicing.amazonaws.com

- iot.amazonaws.com
- iotfleetwise.amazonaws.com
- iotsecuredtunneling.amazonaws.com
- iotsitewise.amazonaws.com
- kms.amazonaws.com
- lakeformation.amazonaws.com
- lambda.amazonaws.com
- license-manager.amazonaws.com
- lookoutequipment.amazonaws.com
- lookoutvision.amazonaws.com
- monitoring.amazonaws.com
- partnercentral-prm.amazonaws.com
- personalize.amazonaws.com
- qbusiness.amazonaws.com
- quicksight.amazonaws.com
- rds.amazonaws.com
- rdsdata.amazonaws.com
- rdsdataapi.amazonaws.com
- rekognition.amazonaws.com
- rolesanywhere.amazonaws.com
- route53.amazonaws.com
- s3.amazonaws.com
- s3vectors.amazonaws.com
- sagemaker.amazonaws.com
- scheduler.amazonaws.com
- secretsmanager.amazonaws.com
- servicediscovery.amazonaws.com
- ses.amazonaws.com
- signin.amazonaws.com
- sns.amazonaws.com

- sqs.amazonaws.com
- ssm-contacts.amazonaws.com
- ssm.amazonaws.com
- sso-directory.amazonaws.com
- sso-oauth.amazonaws.com
- sso.amazonaws.com
- states.amazonaws.com
- storagegateway.amazonaws.com
- sts.amazonaws.com
- swf.amazonaws.com
- textract.amazonaws.com
- transcribe.amazonaws.com
- transcribestreaming.amazonaws.com
- transfer.amazonaws.com
- transform.amazonaws.com
- translate.amazonaws.com
- user-subscriptions.amazonaws.com
- verifiedpermissions.amazonaws.com
- voiceid.amazonaws.com
- workmail.amazonaws.com
- workmailmessageflow.amazonaws.com

Bidang pemilih acara lanjutan berikut adalah opsional:

- `eventName`— Tindakan yang diminta yang ingin Anda filter. Misalnya, `CreateKey` atau`ListKeys`. `eventName`dapat menggunakan operator apa pun.
- `errorCode`— Kode kesalahan yang diminta yang ingin Anda filter. Saat ini, satu-satunya yang valid `errorCode` adalah`VpceAccessDenied`. Anda hanya dapat menggunakan `Equals` operator dengan`errorCode`.
- `vpcEndpointId`— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan `vpcEndpointId`.

- `userIdentity.arn`— Sertakan atau kecualikan peristiwa untuk tindakan yang diambil oleh identitas IAM tertentu. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity. Anda dapat menggunakan operator apa pun dengan`userIdentity.arn`. CloudTrail mendukung bidang ini hanya untuk jalur. Anda tidak dapat memfilter peristiwa aktivitas jaringan `userIdentity.arn` untuk menyimpan data peristiwa.

Peristiwa aktivitas jaringan tidak dicatat secara default saat Anda membuat penyimpanan data jejak atau peristiwa. Untuk merekam peristiwa aktivitas CloudTrail jaringan, Anda harus secara eksplisit mengonfigurasi setiap sumber peristiwa yang ingin Anda kumpulkan aktivitasnya.

Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

Mencatat peristiwa aktivitas jaringan dengan Konsol Manajemen AWS

Anda dapat memperbarui penyimpanan data jejak atau peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan menggunakan konsol.

Topik

- Memperbarui jejak yang ada untuk mencatat peristiwa aktivitas jaringan
- Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan

Memperbarui jejak yang ada untuk mencatat peristiwa aktivitas jaringan

Gunakan prosedur berikut untuk memperbarui jejak yang ada untuk mencatat peristiwa aktivitas jaringan.

> **Note**
>
> Biaya tambahan berlaku untuk peristiwa aktivitas jaringan logging. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri CloudTrail konsol, buka halaman Trails, dan pilih nama jejak.

3. Jika jejak Anda mencatat peristiwa data menggunakan pemilih acara dasar, Anda harus beralih ke pemilih peristiwa lanjutan untuk mencatat peristiwa aktivitas jaringan.

   Ambil langkah-langkah ini untuk beralih ke pemilih acara tingkat lanjut:

   a. Di area peristiwa Data, perhatikan pemilih peristiwa data saat ini. Beralih ke pemilih acara lanjutan akan menghapus pemilih peristiwa data yang ada.

   b. Pilih Edit dan kemudian pilih Beralih ke pemilih acara lanjutan.

   c. Terapkan kembali pilihan acara data Anda menggunakan pemilih acara tingkat lanjut. Untuk informasi selengkapnya, lihat Memperbarui jejak yang ada untuk mencatat peristiwa data dengan pemilih acara lanjutan menggunakan konsol.

4. Di acara aktivitas jaringan, pilih Edit.

   Untuk mencatat peristiwa aktivitas jaringan, lakukan langkah-langkah berikut:

   a. Dari sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

   b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua peristiwa yang ditolak akses aktivitas jaringan, atau memilih Kustom untuk membuat pemilih log kustom untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

   c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

   d. Di Penyeleksi acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

      i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

         - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
         - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
         - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan `vpcEndpointId`.

ii. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat.

iii. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

e. Untuk menambahkan sumber peristiwa lain yang ingin Anda log peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

5. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan

Gunakan prosedur berikut untuk memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa aktivitas jaringan.

> **Note**
>
> Anda hanya dapat mencatat peristiwa aktivitas jaringan pada penyimpanan data peristiwa dari jenis CloudTrail peristiwa.

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri CloudTrail konsol, di bawah Danau, pilih Penyimpanan data acara.
3. Pilih nama penyimpanan data acara.
4. Di acara aktivitas jaringan, pilih Edit.

   Untuk mencatat peristiwa aktivitas jaringan, lakukan langkah-langkah berikut:

   a. Dari sumber peristiwa aktivitas jaringan, pilih sumber untuk peristiwa aktivitas jaringan.

   b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa aktivitas jaringan, mencatat semua peristiwa yang ditolak akses aktivitas jaringan, atau memilih Kustom untuk membuat pemilih log kustom untuk memfilter pada beberapa bidang, seperti `eventName` dan`vpcEndpointId`.

c. (Opsional) Masukkan nama untuk mengidentifikasi pemilih. Nama pemilih terdaftar sebagai Nama di pemilih acara lanjutan dan dapat dilihat jika Anda memperluas tampilan JSON.

d. Di Penyeleksi acara lanjutan membangun ekspresi dengan memilih nilai untuk Bidang, Operator, dan Nilai. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

   i. Untuk mengecualikan atau menyertakan peristiwa aktivitas jaringan, Anda dapat memilih dari bidang berikut di konsol.

      - **`eventName`**— Anda dapat menggunakan operator apa pun dengan`eventName`. Anda dapat menggunakannya untuk memasukkan atau mengecualikan acara apa pun, seperti`CreateKey`.
      - **`errorCode`**— Anda dapat menggunakannya untuk memfilter kode kesalahan. Saat ini, satu-satunya yang didukung `errorCode` adalah`VpceAccessDenied`.
      - **`vpcEndpointId`**— Mengidentifikasi titik akhir VPC yang dilewati operasi. Anda dapat menggunakan operator apa pun dengan `vpcEndpointId`.

   ii. Untuk setiap bidang, pilih + Syarat untuk menambahkan syarat sebanyak yang Anda butuhkan, hingga maksimum 500 nilai yang ditentukan untuk semua syarat.

   iii. Pilih + Bidang untuk menambahkan bidang lain sesuai kebutuhan. Untuk menghindari kesalahan, jangan setel nilai yang bertentangan atau duplikat untuk bidang.

e. Untuk menambahkan sumber peristiwa lain yang ingin Anda log peristiwa aktivitas jaringan, pilih Tambahkan pemilih peristiwa aktivitas jaringan.

f. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

5. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Mencatat peristiwa aktivitas jaringan dengan AWS Command Line Interface

Anda dapat mengonfigurasi jejak atau penyimpanan data peristiwa untuk mencatat peristiwa aktivitas jaringan menggunakan file. AWS CLI

Topik

- Contoh: Mencatat peristiwa aktivitas jaringan untuk jejak
- Contoh: Logging peristiwa aktivitas jaringan untuk penyimpanan data acara

Contoh: Mencatat peristiwa aktivitas jaringan untuk jejak

Anda dapat mengonfigurasi jejak Anda untuk mencatat peristiwa aktivitas jaringan menggunakan file. AWS CLI Jalankan put-event-selectorsperintah untuk mengonfigurasi penyeleksi acara lanjutan untuk jejak Anda.

Untuk melihat apakah jejak Anda mencatat peristiwa aktivitas jaringan, jalankan `get-event-selectors`perintah.

Topik

- Contoh: Log peristiwa aktivitas jaringan untuk CloudTrail operasi
- Contoh: Log VpceAccessDeniedperistiwa untuk AWS KMS
- Contoh: Log VpceAccessDeniedperistiwa untuk Amazon S3
- Contoh: Log VpceAccessDeniedperistiwa EC2 melalui titik akhir VPC tertentu
- Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara

Contoh: Log peristiwa aktivitas jaringan untuk CloudTrail operasi

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan semua peristiwa aktivitas jaringan untuk operasi CloudTrail API, seperti `CreateTrail` dan `CreateEventDataStore` panggilan. Nilai untuk `eventSource` bidang tersebut adalah`cloudtrail.amazonaws.com`.

```
aws cloudtrail put-event-selectors /
--trail-name TrailName /
--region region /
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
```

```
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit all CloudTrail API calls through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa untuk AWS KMS

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan `VpceAccessDenied` acara AWS KMS. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa dan `eventSource` bidang sama dengan`kms.amazonaws.com`.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
```

```
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
```

```
            ]
        }
    ]
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa untuk Amazon S3

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan `VpceAccessDenied` peristiwa untuk Amazon S3. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa dan `eventSource` bidang sama dengan`s3.amazonaws.com`.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
```

```
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa EC2 melalui titik akhir VPC tertentu

Contoh berikut menunjukkan cara mengonfigurasi jejak Anda untuk menyertakan `VpceAccessDenied` peristiwa untuk Amazon EC2 untuk titik akhir VPC tertentu. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa, `eventSource` bidang sama dengan`ec2.amazonaws.com`, dan `vpcEndpointId` sama dengan titik akhir VPC yang diinginkan.

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
```

```
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
```

```
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ]
}
```

Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara

Contoh berikut mengonfigurasi jejak untuk mencatat peristiwa manajemen dan semua peristiwa aktivitas jaringan untuk sumber peristiwa Amazon EC2 AWS KMS,, AWS Secrets Manager, dan Amazon S3. CloudTrail

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
```

```
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
```

```
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
```

```
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

Contoh: Logging peristiwa aktivitas jaringan untuk penyimpanan data acara

Anda dapat mengonfigurasi penyimpanan data acara Anda untuk menyertakan peristiwa aktivitas jaringan menggunakan AWS CLI. Gunakan `create-event-data-store`perintah untuk membuat penyimpanan data acara baru untuk mencatat peristiwa aktivitas jaringan. Gunakan `update-event-data-store`perintah untuk memperbarui pemilih acara lanjutan untuk penyimpanan data peristiwa yang ada.

Untuk melihat apakah penyimpanan data acara Anda menyertakan peristiwa aktivitas jaringan, jalankan `get-event-data-store`perintah.

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

Topik

- Contoh: Log semua peristiwa aktivitas jaringan untuk CloudTrail operasi
- Contoh: Log VpceAccessDeniedperistiwa untuk AWS KMS
- Contoh: Log VpceAccessDeniedperistiwa EC2 melalui titik akhir VPC tertentu
- Contoh: Log VpceAccessDeniedperistiwa untuk Amazon S3
- Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara

Contoh: Log semua peristiwa aktivitas jaringan untuk CloudTrail operasi

Contoh berikut menunjukkan cara membuat penyimpanan data peristiwa yang mencakup semua peristiwa aktivitas jaringan yang terkait dengan CloudTrail operasi, seperti panggilan ke `CreateTrail` dan`CreateEventDataStore`. Nilai untuk `eventSource` bidang diatur `kecloudtrail.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name "EventDataStoreName" \
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls over VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
```

```
        {
            "Name": "Audit all CloudTrail API calls over VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa untuk AWS KMS

Contoh berikut menunjukkan cara membuat penyimpanan data acara untuk menyertakan `VpceAccessDenied` acara untuk AWS KMS. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa dan `eventSource` bidang sama dengan`kms.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
```

```
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa EC2 melalui titik akhir VPC tertentu

Contoh berikut menunjukkan cara membuat penyimpanan data peristiwa untuk menyertakan `VpceAccessDenied` peristiwa untuk Amazon EC2 untuk titik akhir VPC tertentu. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa, `eventSource` bidang sama dengan`ec2.amazonaws.com`, dan `vpcEndpointId` sama dengan titik akhir VPC yang diinginkan.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.


```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
```

```
}
```

Contoh: Log **`VpceAccessDenied`**peristiwa untuk Amazon S3

Contoh berikut menunjukkan cara membuat penyimpanan data acara untuk menyertakan `VpceAccessDenied` peristiwa untuk Amazon S3. Contoh ini menetapkan `errorCode` bidang sama dengan `VpceAccessDenied` peristiwa dan `eventSource` bidang sama dengan`s3.amazonaws.com`.

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
```

```
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
     ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

Contoh: Log semua peristiwa manajemen dan peristiwa aktivitas jaringan untuk beberapa sumber acara

Contoh berikut memperbarui penyimpanan data peristiwa yang saat ini hanya mencatat peristiwa manajemen untuk juga mencatat peristiwa aktivitas jaringan untuk beberapa sumber peristiwa. Untuk memperbarui penyimpanan data acara untuk menambahkan pemilih acara baru, jalankan `get-event-data-store` perintah untuk mengembalikan pemilih acara lanjutan saat ini. Kemudian, jalankan `update-event-data-store` perintah dan teruskan `--advanced-event-selectors` yang menyertakan pemilih saat ini ditambah pemilih baru. Untuk mencatat peristiwa aktivitas jaringan untuk beberapa sumber peristiwa, sertakan satu pemilih untuk setiap sumber peristiwa yang ingin Anda log.

```
aws cloudtrail update-event-data-store \
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]},
```

```
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

Perintah mengembalikan contoh output berikut.

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
           {
```

```
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
```

```
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
```

```
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-11-20T21:00:17.820000+00:00"
}
```

Mencatat peristiwa dengan AWS SDK

Jalankan GetEventSelectorsoperasi untuk melihat apakah jejak Anda mencatat peristiwa aktivitas jaringan. Anda dapat mengonfigurasi jejak Anda untuk mencatat peristiwa aktivitas jaringan dengan menjalankan PutEventSelectorsoperasi. Untuk informasi lebih lanjut, lihat Referensi API AWS CloudTrail.

Jalankan GetEventDataStoreoperasi untuk melihat apakah penyimpanan data acara Anda mencatat peristiwa aktivitas jaringan. Anda dapat mengonfigurasi penyimpanan data acara Anda untuk menyertakan peristiwa aktivitas jaringan dengan menjalankan CreateEventDataStoreatau UpdateEventDataStoreoperasi dan menentukan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Membuat, memperbarui, dan mengelola penyimpanan data acara dengan AWS CLI dan Referensi AWS CloudTrail API.

CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM

Anda dapat memperkaya peristiwa CloudTrail manajemen dan peristiwa data dengan menambahkan kunci tag sumber daya, kunci tag utama, dan kunci kondisi global IAM saat Anda membuat atau memperbarui penyimpanan data peristiwa. Ini memungkinkan Anda untuk mengkategorikan, mencari, dan menganalisis CloudTrail peristiwa berdasarkan konteks bisnis, seperti alokasi biaya dan manajemen keuangan, operasi, dan persyaratan keamanan data. Anda dapat menganalisis peristiwa dengan menjalankan kueri di CloudTrail Lake. Anda juga dapat memilih untuk menggabungkan

penyimpanan data acara Anda dan menjalankan kueri di Amazon Athena. Anda dapat menambahkan kunci tag sumber daya dan kunci kondisi global IAM ke penyimpanan data peristiwa menggunakan CloudTrail konsol AWS CLI, dan SDK.

> **Note**
>
> Tag sumber daya yang Anda tambahkan setelah pembuatan atau pembaruan sumber daya mungkin mengalami penundaan sebelum tag tersebut tercermin dalam CloudTrail peristiwa. CloudTrail peristiwa untuk penghapusan sumber daya mungkin tidak menyertakan informasi tag.
> Kunci kondisi global IAM akan selalu terlihat dalam output kueri, tetapi mungkin tidak terlihat oleh pemilik sumber daya.

Saat Anda menambahkan kunci tag sumber daya ke peristiwa yang diperkaya, CloudTrail sertakan kunci tag yang dipilih yang terkait dengan sumber daya yang terlibat dalam panggilan API.

Saat Anda menambahkan kunci kondisi global IAM ke penyimpanan data peristiwa, CloudTrail sertakan informasi tentang kunci kondisi yang dipilih yang dievaluasi selama proses otorisasi, termasuk detail tambahan tentang prinsipal, sesi, dan permintaan itu sendiri.

> **Note**
>
> Mengkonfigurasi CloudTrail untuk menyertakan kunci kondisi atau tag utama tidak berarti bahwa kunci kondisi atau tag utama ini akan ada di setiap peristiwa. Misalnya, jika Anda telah menyiapkan CloudTrail untuk menyertakan kunci kondisi global tertentu tetapi Anda tidak melihatnya dalam peristiwa tertentu, ini menunjukkan bahwa kunci tersebut tidak relevan dengan evaluasi kebijakan IAM untuk tindakan tersebut.

Setelah Anda menambahkan kunci tag sumber daya atau kunci kondisi IAM, CloudTrail sertakan `eventContext` bidang dalam CloudTrail peristiwa yang menyediakan informasi kontekstual yang dipilih untuk tindakan API.

Ada beberapa pengecualian ketika acara tidak akan menyertakan `eventContext` bidang, termasuk yang berikut:

- Peristiwa API yang terkait dengan sumber daya yang dihapus mungkin atau mungkin tidak memiliki tag sumber daya.

- `eventContext`Bidang tidak akan memiliki data untuk peristiwa yang tertunda, dan tidak akan hadir untuk peristiwa yang diperbarui setelah panggilan API. Misalnya, jika ada penundaan atau pemadaman untuk Amazon EventBridge, tag untuk acara mungkin tetap kedaluwarsa untuk beberapa waktu setelah pemadaman diselesaikan. Beberapa AWS layanan akan mengalami penundaan yang lebih lama. Untuk informasi selengkapnya, lihat Pembaruan tag sumber daya CloudTrail untuk acara yang diperkaya.
- Jika Anda mengubah atau menghapus peran AWSServiceRoleForCloudTrailEventContext terkait layanan yang digunakan untuk acara yang diperkaya, tidak CloudTrail akan mengisi tag sumber daya apa pun. `eventContext`
- Untuk acara yang melibatkan lebih dari 100 sumber daya, `eventContext` bidang ini hanya akan menyertakan informasi tag sumber daya untuk 100 sumber daya pertama, diurutkan menurut abjad menurut ARN.

> **Note**
>
> `eventContext`Bidang ini hanya ada dalam peristiwa untuk penyimpanan data peristiwa yang dikonfigurasi untuk menyertakan kunci tag sumber daya, kunci tag utama, dan kunci kondisi global IAM. Acara yang dikirim ke Riwayat acara EventBridge, Amazon, dapat dilihat dengan AWS CLI `lookup-events` perintah, dan dikirim ke jalur, tidak akan menyertakan bidang. `eventContext`

Topik

- Layanan AWS tag sumber daya pendukung
- Layanan AWS mendukung kunci kondisi global IAM
- Contoh acara

Layanan AWS tag sumber daya pendukung

Semua tag sumber daya Layanan AWS dukungan. Untuk informasi selengkapnya, lihat Layanan yang mendukung AWS Resource Groups Tagging API.

Pembaruan tag sumber daya CloudTrail untuk acara yang diperkaya

Ketika dikonfigurasi untuk melakukannya, CloudTrail menangkap informasi tentang tag sumber daya dan menggunakannya untuk memberikan informasi dalam peristiwa yang diperkaya. Saat

bekerja dengan tag sumber daya, ada kondisi tertentu di mana tag sumber daya mungkin tidak tercermin secara akurat pada saat permintaan sistem untuk acara. Selama operasi standar, tag yang diterapkan pada waktu pembuatan sumber daya selalu ada dan akan mengalami penundaan minimal atau tidak ada. Namun, layanan berikut diharapkan mengalami penundaan dalam perubahan tag sumber daya yang muncul di CloudTrail acara:

- Konektor Suara Amazon Chime
- AWS CloudTrail
- AWS CodeConnections
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Keyspaces (untuk Apache Cassandra)
- Amazon Kinesis
- Amazon Lex V2
- Amazon MemoryDB
- Amazon S3
- Amazon Security Lake
- AWS Direct Connect
- AWS IAM Identity Center
- AWS Key Management Service
- AWS Lambda
- AWS Marketplace Wawasan Vendor
- AWS Organizations
- AWS Payment Cryptography
- Amazon Simple Queue Service

Pemadaman layanan juga dapat menyebabkan keterlambatan pembaruan informasi tag sumber daya. Jika terjadi penundaan pemadaman layanan, CloudTrail peristiwa berikutnya akan mencakup `addendum` bidang yang mencakup informasi tentang perubahan tag sumber daya. Informasi tambahan ini akan digunakan sebagaimana ditentukan untuk memberikan diperkayaCloudTrailevents.

Layanan AWS mendukung kunci kondisi global IAM

Berikut ini Layanan AWS mendukung kunci kondisi global IAM untuk acara yang diperkaya:

- AWS Certificate Manager
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Log Amazon
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon Cognito Sync
- Amazon Comprehend
- Amazon Comprehend Medical
- ID Suara Pelanggan Amazon Connect
- AWS Control Tower
- Amazon Data Firehose
- Amazon Elastic Block Store
- Elastic Load Balancing
- Media Sosial Olah Pesan Pengguna Akhir AWS
- Amazon EventBridge
- EventBridge Penjadwal Amazon
- Amazon Data Firehose
- Amazon FSx
- AWS HealthImaging
- AWS IoT FleetWise
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS IoT Wireless
- Amazon Kendra

- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- AWS Network Firewall
- AWS Payment Cryptography
- Amazon Personalize
- AWS Proton
- Amazon Rekognition
- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon SQS
- AWS Step Functions
- AWS Storage Gateway
- Amazon SWF
- Rantai Pasokan AWS
- Amazon Timestream
- Amazon Timestream untuk InfluxDB
- Amazon Transcribe
- AWS Transfer Family
- AWS Trusted Advisor
- Amazon WorkSpaces
- AWS X-Ray

Kunci kondisi global IAM yang didukung untuk acara yang diperkaya

Tabel berikut mencantumkan kunci kondisi global IAM yang didukung untuk peristiwa yang CloudTrail diperkaya, dengan nilai contoh:

Kunci Kondisi Global dan Nilai Sampel

Key	Nilai contoh
aws:FederatedProvider	"*IdP*"
aws:TokenIssueTime	"*123456789* "
aws:MultiFactorAuthAge	“99"
aws:MultiFactorAuthPresent	"*true*"
aws:SourceIdentity	"*UserName*"
aws:PrincipalAccount	“111122223333"
aws:PrincipalArn	“arn:aws:iam::” *555555555555:role/myRole*
aws:PrincipalIsAWSService	"*false*"
aws:PrincipalOrgI D	"*o-rganization* "
aws:PrincipalOrgPaths	["*o-rganization/path-of-org* "]
aws:PrincipalServiceName	"*cloudtrail.amazonaws.com* "
aws:PrincipalServiceNamesList	["*cloudtrail.amazonaws.com*","*s3.amazonaws.com* "]
aws:PrincipalType	"*AssumedRole* "
aws:userid	"*userid*"
aws:username	"*username*"
aws:RequestedRegion	*us-east-2* "
aws:SecureTransport	"*true*"
aws:ViaAWSService	"*false*"

Key	Nilai contoh
aws:CurrentTime	"*2025-04-30 15:30:00* "
aws:EpochTime	"*1746049800* "
aws:SourceAccount	"*111111111111* "
aws:SourceOrgID	"*o-rganization* "

Contoh acara

Dalam contoh berikut, `eventContext` bidang menyertakan kunci kondisi global IAM `aws:ViaAWSService` dengan nilai`false`, yang menunjukkan panggilan API tidak dibuat oleh sebuah Layanan AWS.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/admin",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/admin",
                "accountId": "123456789012",
                "userName": "admin"
            },
            "attributes": {
                "creationDate": "2025-01-22T22:05:56Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-01-22T22:06:16Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "GetTrailStatus",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:133.0)
 Gecko/20100101 Firefox/133.0",
    "requestParameters": {
        "name": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail"
    },
    "responseElements": null,
    "requestID": "d09c4dd2-5698-412b-be7a-example1a23",
    "eventID": "9cb5f426-7806-46e5-9729-exampled135d",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true",
    "eventContext": {
        "requestContext": {
            "aws:ViaAWSService": "false"
        },
        "tagContext": {}
    }
}
```


CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan

Halaman ini menjelaskan isi rekaman peristiwa manajemen, data, atau aktivitas jaringan.

Isi catatan berisi bidang yang membantu Anda menentukan tindakan yang diminta serta kapan dan di mana permintaan dibuat. Jika nilai Opsional adalah True, bidang hanya ada jika berlaku untuk layanan, API, atau jenis acara. Nilai Opsional False berarti bahwa bidang selalu ada, atau keberadaannya tidak bergantung pada layanan, API, atau jenis acara. Contohnya adalah`responseElements`, yang hadir dalam acara untuk tindakan yang membuat perubahan (membuat, memperbarui, atau menghapus tindakan).

> **Note**
>
> Bidang untuk acara yang diperkaya seperti hanya `eventContext` tersedia untuk acara manajemen dan peristiwa data. Mereka tidak tersedia untuk acara jaringan.

`eventTime`

Tanggal dan waktu permintaan selesai, dalam waktu universal terkoordinasi (UTC). Cap waktu acara berasal dari host lokal yang menyediakan titik akhir API layanan tempat panggilan API dibuat. Misalnya, peristiwa CreateBucket API yang dijalankan di Wilayah AS Barat (Oregon) akan mendapatkan cap waktunya dari waktu pada AWS host yang menjalankan titik akhir Amazon S3,. `s3.us-west-2.amazonaws.com` Secara umum, AWS layanan menggunakan Network Time Protocol (NTP) untuk menyinkronkan jam sistem mereka.

Sejak: 1.0

Opsional: Salah

`eventVersion`

Versi format peristiwa log. Versi saat ini adalah 1.11.

`eventVersion`Nilainya adalah versi mayor dan minor dalam formulir*`major_version`*. *`minor_version`*. Misalnya, Anda dapat memiliki `eventVersion` nilai`1.10`, di mana `1` adalah versi utama, dan `10` merupakan versi minor.

CloudTrail menambah versi utama jika perubahan dilakukan pada struktur acara yang tidak kompatibel ke belakang. Ini termasuk menghapus bidang JSON yang sudah ada, atau mengubah bagaimana isi bidang direpresentasikan (misalnya, format tanggal). CloudTrail menambah versi minor jika perubahan menambahkan bidang baru ke struktur acara. Hal ini dapat terjadi jika informasi baru tersedia untuk beberapa atau semua peristiwa yang ada, atau jika informasi baru hanya tersedia untuk jenis acara baru. Aplikasi dapat mengabaikan bidang baru agar tetap kompatibel dengan versi minor baru dari struktur acara.

Jika CloudTrail memperkenalkan jenis acara baru, tetapi struktur acara sebaliknya tidak berubah, versi acara tidak berubah.

Untuk memastikan bahwa aplikasi Anda dapat mengurai struktur acara, kami sarankan Anda melakukan perbandingan yang setara dengan nomor versi utama. Untuk memastikan bahwa

bidang yang diharapkan oleh aplikasi Anda ada, kami juga menyarankan untuk melakukan perbandingan yang lebih baik dari pada versi minor. Tidak ada angka nol terkemuka dalam versi minor. Anda dapat menafsirkan keduanya *major_version* dan *minor_version* sebagai angka, dan melakukan operasi perbandingan.

Sejak: 1.0

Opsional: Salah

userIdentity

Informasi tentang identitas IAM yang membuat permintaan. Untuk informasi selengkapnya, lihat CloudTrail elemen userIdentity.

Sejak: 1.0

Opsional: Salah

eventSource

Layanan di mana permintaannya dibuat. Nama ini biasanya merupakan bentuk pendek dari nama layanan tanpa spasi plus `.amazonaws.com`. Contoh:

- CloudFormation adalah`cloudformation.amazonaws.com`.
- Amazon EC2 adalah. `ec2.amazonaws.com`
- Amazon Simple Workflow Service adalah`swf.amazonaws.com`.

Konvensi ini memiliki beberapa pengecualian. Misalnya, `eventSource` untuk Amazon CloudWatch adalah`monitoring.amazonaws.com`.

Sejak: 1.0

Opsional: Salah

eventName

Tindakan yang diminta, yang merupakan salah satu tindakan dalam API untuk layanan itu.

Sejak: 1.0

Opsional: Salah

`awsRegion`

Permintaan itu dibuat untuk, sepertius-east-2. Wilayah AWS Lihat CloudTrail Daerah yang didukung.

Sejak: 1.0

Opsional: Salah

`sourceIPAddress`

Alamat IP di mana permintaan itu dibuat. Untuk tindakan yang berasal dari konsol layanan, alamat yang dilaporkan adalah untuk sumber daya pelanggan yang mendasarinya, bukan server web konsol. Untuk layanan di AWS, hanya nama DNS yang ditampilkan.

> **Note**
>
> Untuk peristiwa yang berasal dari AWS, bidang ini biasanyaAWS Internal/#, di mana # adalah nomor yang digunakan untuk tujuan internal.

Sejak: 1.0

Opsional: Salah

`userAgent`

Agen yang melaluinya permintaan dibuat, seperti Konsol Manajemen AWS, AWS layanan, AWS SDK atau. AWS CLI

Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran peristiwa maksimum 1 MB, konten bidang hanya terpotong jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Berikut ini adalah contoh nilai:

- `lambda.amazonaws.com`Permintaan dibuat dengan AWS Lambda.
- `aws-sdk-java`Permintaan dibuat dengan AWS SDK untuk Java.
- `aws-sdk-ruby`Permintaan dibuat dengan AWS SDK untuk Ruby.

- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5`— Permintaan dibuat dengan AWS CLI diinstal di Linux.

> **Note**
>
> Untuk peristiwa yang berasal dari AWS, jika CloudTrail tahu yang Layanan AWS membuat panggilan, bidang ini adalah sumber acara dari layanan panggilan (misalnya,`ec2.amazonaws.com`). Jika tidak, bidang ini adalah`AWS Internal/#`, di mana `#` nomor yang digunakan untuk tujuan internal.

Sejak: 1.0

Opsional: Benar

`errorCode`

Kesalahan AWS layanan jika permintaan mengembalikan kesalahan. Untuk contoh yang menunjukkan bidang ini, lihatKode kesalahan dan contoh log pesan.

Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran peristiwa maksimum 1 MB, konten bidang hanya terpotong jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Untuk peristiwa aktivitas jaringan, ketika ada pelanggaran kebijakan titik akhir VPC, kode kesalahannya adalah. `VpceAccessDenied`

Sejak: 1.0

Opsional: Benar

`errorMessage`

Jika permintaan mengembalikan kesalahan, deskripsi kesalahan. Pesan ini mencakup pesan untuk kegagalan otorisasi. CloudTrail menangkap pesan yang dicatat oleh layanan dalam penanganan pengecualiannya. Sebagai contoh, lihat Kode kesalahan dan contoh log pesan.

Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran peristiwa maksimum 1

MB, konten bidang hanya terpotong jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Untuk peristiwa aktivitas jaringan, ketika ada pelanggaran kebijakan titik akhir VPC, `errorMessage` akan selalu menjadi pesan berikut:. `The request was denied due to a VPC endpoint policy` Untuk informasi selengkapnya tentang peristiwa yang ditolak akses untuk pelanggaran kebijakan titik akhir VPC, lihat Contoh pesan kesalahan akses ditolak di Panduan Pengguna IAM. Untuk contoh peristiwa aktivitas jaringan yang menunjukkan pelanggaran kebijakan titik akhir VPC, lihat Peristiwa aktivitas jaringan dalam panduan ini.

> **Note**
>
> Beberapa AWS layanan menyediakan `errorCode` dan `errorMessage` sebagai bidang tingkat atas dalam acara tersebut. AWS Layanan lain memberikan informasi kesalahan sebagai bagian dari`responseElements`.

Sejak: 1.0

Opsional: Benar

`requestParameters`

Parameter, jika ada, yang dikirim dengan permintaan. Parameter ini didokumentasikan dalam dokumentasi referensi API untuk AWS layanan yang sesuai. Bidang ini memiliki ukuran maksimum 100 KB. Ketika ukuran bidang melebihi 100 KB, `requestParameters` konten dihilangkan. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran acara maksimum 1 MB, konten bidang hanya dihilangkan jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Sejak: 1.0

Opsional: Salah

`responseElements`

Elemen respons, jika ada, untuk tindakan yang membuat perubahan (membuat, memperbarui, atau menghapus tindakan). Untuk `readOnly` API, bidang ini adalah`null`. Jika tindakan tidak

mengembalikan elemen respons, bidang ini adalah`null`. Elemen respons untuk tindakan didokumentasikan dalam referensi API dokumentasi yang sesuai Layanan AWS.

Bidang ini memiliki ukuran maksimum 100 KB. Ketika ukuran bidang melebihi 100 KB, `reponseElements` konten dihilangkan. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran acara maksimum 1 MB, konten bidang hanya dihilangkan jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

`responseElements`Nilai ini berguna untuk membantu Anda melacak permintaan dengan AWS Dukungan. Keduanya `x-amz-request-id` dan `x-amz-id-2` berisi informasi yang membantu Anda melacak permintaan Dukungan. Nilai-nilai ini adalah sama dengan yang dikembalikan layanan sebagai respons atas permintaan itu memulai acara, sehingga Anda dapat menggunakannya untuk mencocokkan acara dengan permintaan.

Sejak: 1.0

Opsional: Salah

`additionalEventData`

Data tambahan tentang peristiwa yang bukan bagian dari permintaan atau tanggapan. Bidang ini memiliki ukuran maksimum 28 KB. Ketika ukuran bidang melebihi 28 KB, `additionalEventData` konten dihilangkan. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran acara maksimum 1 MB, konten bidang hanya dihilangkan jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Konten `additionalEventData` adalah variabel. Misalnya, untuk peristiwa Konsol Manajemen AWS login, `additionalEventData` dapat menyertakan `MFAUsed` bidang dengan nilai `Yes` jika permintaan dibuat oleh pengguna root atau IAM menggunakan otentikasi multi-faktor (MFA).

Sejak: 1.0

Opsional: Benar

`requestID`

Nilai yang mengidentifikasi permintaan. Layanan yang dipanggil menghasilkan nilai ini. Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran peristiwa maksimum 1 MB, konten bidang hanya terpotong jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Sejak: 1.01

Opsional: Benar

`eventID`

GUID dihasilkan oleh CloudTrail untuk mengidentifikasi setiap peristiwa secara unik. Anda dapat menggunakan nilai ini untuk mengidentifikasi satu peristiwa. Misalnya, Anda dapat menggunakan ID sebagai kunci utama untuk mengambil data log dari database yang dapat dicari.

Sejak: 1.01

Opsional: Salah

`eventType`

Mengidentifikasi jenis peristiwa yang menghasilkan catatan peristiwa. Ini bisa menjadi salah satu dari nilai berikut:

- `AwsApiCall`Sebuah API dipanggil.
- `AwsServiceEvent`— Layanan ini menghasilkan acara yang terkait dengan jejak Anda. Misalnya, ini dapat terjadi ketika akun lain melakukan panggilan dengan sumber daya yang Anda miliki.
- `AwsConsoleAction`— Tindakan diambil di konsol yang bukan panggilan API.
- `AwsConsoleSignIn`— Seorang pengguna di akun Anda (root, IAM, federasi, SAMP, atau SwitchRole) masuk ke. Konsol Manajemen AWS
- `AwsVpceEvents`— peristiwa aktivitas CloudTrail jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke file. Layanan AWS Untuk merekam peristiwa aktivitas jaringan, pemilik titik akhir VPC harus mengaktifkan peristiwa aktivitas jaringan untuk sumber peristiwa.

Sejak: 1.02

Opsional: Salah

`apiVersion`

Mengidentifikasi versi API yang terkait dengan `AwsApiCall` `eventType` nilai.

Sejak: 1.01

Opsional: Benar

`managementEvent`

Nilai Boolean yang mengidentifikasi apakah acara tersebut adalah acara manajemen. `managementEvent`ditampilkan dalam catatan peristiwa jika `eventVersion` 1,06 atau lebih tinggi, dan jenis acara adalah salah satu dari berikut ini:

- `AwsApiCall`
- `AwsConsoleAction`
- `AwsConsoleSignIn`
- `AwsServiceEvent`

Sejak: 1.06

Opsional: Benar

`readOnly`

Mengidentifikasi apakah operasi ini adalah operasi read-only. Ini dapat berupa salah satu dari nilai berikut:

- `true`— Operasi hanya baca (misalnya,`DescribeTrails`).
- `false`— Operasi hanya menulis (misalnya,`DeleteTrail`).

Sejak: 1.01

Opsional: Benar

`resources`

Daftar sumber daya yang diakses dalam acara tersebut. Bidang dapat berisi informasi berikut:

- ARN Sumber Daya
- ID akun pemilik sumber daya
- Pengidentifikasi jenis sumber daya dalam format: `AWS::`*`aws-service-name`*`::`*`data-type-name`*

Misalnya, ketika suatu `AssumeRole` peristiwa dicatat, `resources` bidang dapat muncul seperti berikut:

- ARN: `arn:aws:iam::123456789012:role/myRole`
- ID Akun: `123456789012`
- Pengidentifikasi jenis sumber daya: `AWS::IAM::Role`

Misalnya log dengan `resources` bidang, lihat Peristiwa AWS STS API di File CloudTrail Log di Panduan Pengguna IAM atau Logging AWS KMS API Calls di Panduan AWS Key Management Service Pengembang.

Sejak: 1.01

Opsional: Benar

`recipientAccountId`

Merupakan ID akun yang menerima acara ini. `recipientAccountID`Mungkin berbeda dari CloudTrail elemen userIdentity`accountId`. Ini dapat terjadi dalam akses sumber daya lintas akun. Misalnya, jika kunci KMS, juga dikenal sebagai AWS KMS key, digunakan oleh akun terpisah untuk memanggil Encrypt API, `recipientAccountID` nilai `accountId` dan akan sama untuk acara yang dikirimkan ke akun yang melakukan panggilan, tetapi nilainya akan berbeda untuk acara yang dikirimkan ke akun yang memiliki kunci KMS.

Sejak: 1.02

Opsional: Benar

`serviceEventDetails`

Mengidentifikasi peristiwa layanan, termasuk apa yang memicu peristiwa dan hasilnya. Untuk informasi selengkapnya, lihat Layanan AWS acara. Bidang ini memiliki ukuran maksimum 100 KB. Ketika ukuran bidang melebihi 100 KB, `serviceEventDetails` konten dihilangkan. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran acara maksimum 1 MB, konten bidang hanya dihilangkan jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Sejak: 1.05

Opsional: Benar

`sharedEventID`

GUID dihasilkan oleh CloudTrail untuk mengidentifikasi CloudTrail peristiwa secara unik dari AWS tindakan yang sama yang dikirim ke akun yang berbeda. AWS

Misalnya, ketika akun menggunakan akun AWS KMS keymilik akun lain, akun yang menggunakan kunci KMS dan akun yang memiliki kunci KMS menerima CloudTrail peristiwa terpisah untuk tindakan yang sama. Setiap CloudTrail acara yang disampaikan untuk AWS aksi ini berbagi hal yang sama`sharedEventID`, tetapi juga memiliki keunikan `eventID` dan`recipientAccountID`.

Untuk informasi selengkapnya, lihat Contoh ShareDeventid.

> **Note**
>
> `sharedEventID`Bidang ini hadir hanya ketika CloudTrail acara dikirimkan ke beberapa akun. Jika penelepon dan pemilik adalah AWS akun yang sama, hanya CloudTrail mengirim satu acara, dan `sharedEventID` bidang tidak ada.

Sejak: 1.03

Opsional: Benar

`vpcEndpointId`

Mengidentifikasi titik akhir VPC tempat permintaan dibuat dari VPC ke layanan AWS lain, seperti Amazon EC2.

> **Note**
>
> Untuk acara yang berasal dari AWS dan melalui VPC, bidang ini `AWS Internal` biasanya atau nama layanan. Layanan AWS

Sejak: 1.04

Opsional: Benar

`vpcEndpointAccountId`

Mengidentifikasi Akun AWS ID pemilik titik akhir VPC untuk titik akhir yang sesuai yang telah dilalui permintaan.

> **Note**
>
> Untuk acara yang berasal dari AWS dan melalui VPC, bidang ini `AWS Internal` biasanya atau nama layanan. Layanan AWS

Sejak: 1.09

Opsional: Benar

`eventCategory`

Menampilkan kategori acara. Kategori acara digunakan dalam `LookupEvents`panggilan untuk memfilter peristiwa manajemen.

- Untuk acara manajemen, nilainya adalah`Management`.
- Untuk peristiwa data, nilainya adalah`Data`.
- Untuk peristiwa aktivitas jaringan, nilainya adalah`NetworkActivity`.

Sejak: 1.07

Opsional: Salah

`addendum`

Jika pengiriman acara tertunda, atau informasi tambahan tentang peristiwa yang ada tersedia setelah acara dicatat, bidang addendum menunjukkan informasi tentang mengapa acara ditunda. Jika informasi hilang dari peristiwa yang ada, bidang addendum mencakup informasi yang hilang dan alasan mengapa itu hilang. Isi termasuk yang berikut ini.

- **`reason`**- Alasan bahwa acara atau beberapa isinya hilang. Nilai dapat berupa salah satu dari berikut ini.
  - **`DELIVERY_DELAY`**— Ada penundaan pengiriman acara. Ini bisa disebabkan oleh lalu lintas jaringan yang tinggi, masalah konektivitas, atau masalah CloudTrail layanan.

- **`UPDATED_DATA`**— Bidang dalam catatan peristiwa hilang atau memiliki nilai yang salah.
- **`SERVICE_OUTAGE`**— Layanan yang mencatat peristiwa untuk CloudTrail mengalami pemadaman, dan tidak dapat mencatat peristiwa. CloudTrail Ini sangat jarang.

- **`updatedFields`**- Bidang catatan acara yang diperbarui oleh addendum. Ini hanya disediakan jika alasannya`UPDATED_DATA`.
- **`originalRequestID`**- ID unik asli dari permintaan. Ini hanya disediakan jika alasannya`UPDATED_DATA`.
- **`originalEventID`**- ID acara asli. Ini hanya disediakan jika alasannya`UPDATED_DATA`.

Sejak: 1.08

Opsional: Benar

`sessionCredentialFromConsole`

String dengan nilai `true` atau `false` yang menunjukkan apakah suatu peristiwa berasal dari Konsol Manajemen AWS sesi atau tidak. Bidang ini tidak ditampilkan kecuali nilainya`true`, artinya klien yang digunakan untuk melakukan panggilan API adalah proxy atau klien eksternal. Jika klien proxy digunakan, bidang `tlsDetails` acara tidak ditampilkan.

Sejak: 1.08

Opsional: Benar

`eventContext`

Bidang ini hadir dalam peristiwa yang diperkaya yang direkam untuk penyimpanan data peristiwa yang dikonfigurasi untuk menyertakan kunci tag sumber daya atau kunci kondisi global IAM. Untuk informasi selengkapnya, lihat CloudTrail Perkaya peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.

Isi meliputi:

- `requestContext`— Termasuk informasi tentang kunci kondisi global IAM yang dievaluasi selama proses otorisasi, termasuk rincian tambahan tentang prinsipal, sesi, jaringan, dan permintaan itu sendiri.
- `tagContext`— Termasuk tag yang terkait dengan sumber daya yang terlibat dalam panggilan API serta tag yang terkait dengan prinsip IAM seperti peran atau pengguna. Untuk informasi selengkapnya, lihat Mengontrol akses untuk prinsipal IAM.

Peristiwa API yang terkait dengan sumber daya yang dihapus tidak akan memiliki tag sumber daya.

> **Note**
>
> `eventContext`Bidang ini hanya ada dalam peristiwa untuk penyimpanan data peristiwa yang dikonfigurasi untuk menyertakan kunci tag sumber daya dan kunci kondisi global IAM. Acara yang dikirim ke Riwayat acara EventBridge, Amazon, dapat dilihat dengan AWS CLI `lookup-events` perintah, dan dikirim ke jalur, tidak akan menyertakan bidang. `eventContext`

Sejak: 1.11

Opsional: Benar

`edgeDeviceDetails`

Menampilkan informasi tentang perangkat edge yang menjadi target permintaan. Saat ini, acara `S3 Outposts`perangkat menyertakan bidang ini. Bidang ini memiliki ukuran maksimum 28 KB; konten yang melebihi batas itu terpotong. Untuk penyimpanan data peristiwa yang dikonfigurasi untuk memiliki ukuran peristiwa maksimum 1 MB, konten bidang hanya terpotong jika muatan peristiwa melebihi 1 MB dan ukuran bidang maksimum terlampaui.

Sejak: 1.08

Opsional: Benar

`tlsDetails`

Menampilkan informasi tentang versi Transport Layer Security (TLS), cipher suite, dan nama domain yang sepenuhnya memenuhi syarat (FQDN) dari nama host yang disediakan klien yang digunakan dalam panggilan API layanan, yang biasanya merupakan FQDN dari titik akhir layanan. CloudTrailmasih mencatat detail TLS sebagian jika informasi yang diharapkan hilang atau kosong. Misalnya, jika versi TLS dan cipher suite hadir, tetapi `HOST` header kosong, detail TLS yang tersedia masih dicatat dalam acara tersebut. CloudTrail

- **`tlsVersion`**- Versi TLS dari permintaan.
- **`cipherSuite`**- Suite cipher (kombinasi algoritma keamanan yang digunakan) dari permintaan.

- **`clientProvidedHostHeader`**- Nama host yang disediakan klien yang digunakan dalam panggilan API layanan, yang biasanya merupakan FQDN dari titik akhir layanan.
- **`keyExchange`**- Metode pertukaran kunci yang digunakan dalam jabat tangan TLS. Bidang ini menunjukkan apakah koneksi menggunakan kriptografi klasik atau kriptografi pasca-kuantum. Contoh nilai termasuk `X25519MLKEM768` untuk TLS 1.3 pasca-kuantum, `x25519` untuk TLS 1.3 klasik, dan `secp256r1` untuk TLS 1.2.

> **Note**
>
> Ada beberapa kasus ketika `tlsDetails` bidang tidak ada dalam catatan peristiwa.
>
> - `tlsDetails`Bidang tidak ada jika panggilan API dilakukan oleh atas nama Anda. Layanan AWS `invokedBy`Bidang dalam `userIdentity` elemen mengidentifikasi Layanan AWS yang membuat panggilan API.
> - Jika `sessionCredentialFromConsole` hadir dengan nilai true, `tlsDetails` hadir dalam catatan peristiwa hanya jika klien eksternal digunakan untuk membuat panggilan API.

Sejak: 1.08

Opsional: Benar

Urutan pemotongan bidang untuk ukuran acara maksimum 1 MB

Anda dapat memperluas ukuran acara maksimum dari 256 KB hingga 1 MB saat Anda membuat atau memperbarui penyimpanan data acara menggunakan CloudTrail konsol AWS CLI, dan SDK.

Memperluas ukuran acara sangat membantu untuk menganalisis dan memecahkan masalah peristiwa karena memungkinkan Anda untuk melihat konten lengkap bidang yang biasanya akan terpotong atau dihilangkan.

Bila payload acara melebihi 1 MB, CloudTrail potong bidang dengan urutan sebagai berikut:

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`

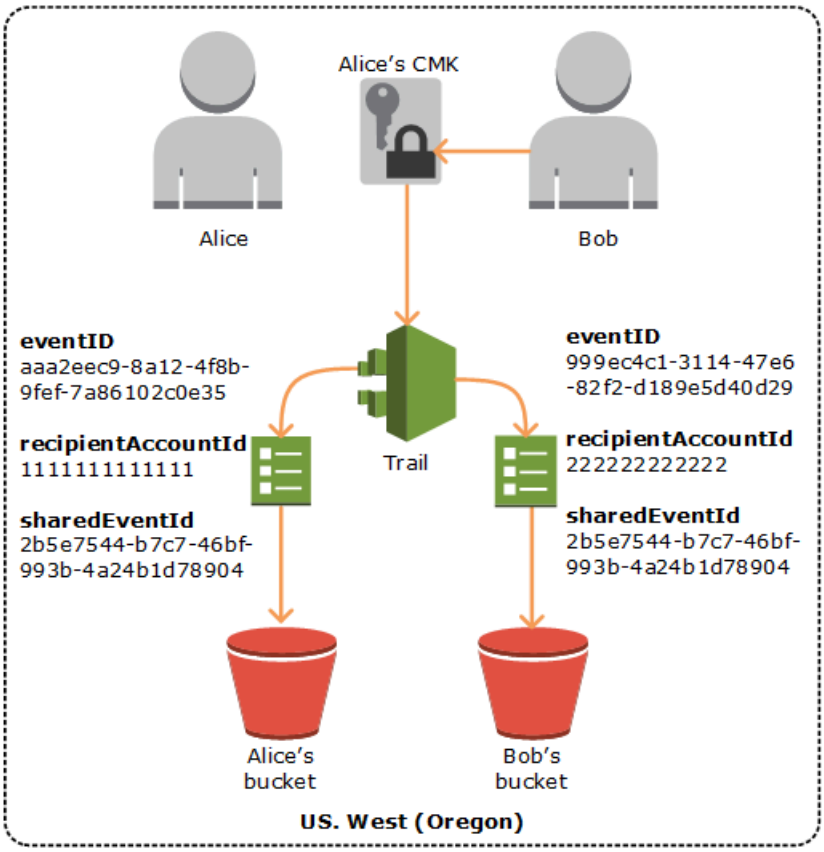
- `userAgent`
- `errorCode`
- `eventContext`
- `responseElements`
- `requestParameters`
- `errorMessage`

Jika muatan peristiwa tidak dapat dikurangi menjadi di bawah 1 MB bahkan setelah pemotongan, kesalahan akan terjadi.

Contoh ShareDeventid

Berikut ini adalah contoh yang menjelaskan bagaimana CloudTrail memberikan dua peristiwa untuk tindakan yang sama:

1. Alice memiliki AWS akun (111111111111) dan membuat akun. AWS KMS key Dia adalah pemilik kunci KMS ini.
2. Bob memiliki AWS akun (222222222222). Alice memberi Bob izin untuk menggunakan kunci KMS.
3. Setiap akun memiliki jejak dan ember terpisah.
4. Bob menggunakan kunci KMS untuk memanggil `Encrypt` API.
5. CloudTrail mengirimkan dua peristiwa terpisah.
    - Satu acara dikirim ke Bob. Acara tersebut menunjukkan bahwa ia menggunakan kunci KMS.
    - Satu acara dikirim ke Alice. Acara tersebut menunjukkan bahwa Bob menggunakan kunci KMS.
    - Peristiwa memiliki hal yang sama`sharedEventID`, tetapi `eventID` dan `recipientAccountID` unik.



CloudTrail merekam konten untuk acara agregat

AWS CloudTrail catatan peristiwa agregat mencakup bidang yang berbeda dari CloudTrail peristiwa lain dalam muatan JSON mereka. Peristiwa agregat berisi bidang-bidang berikut:

`eventVersion`

Versi acara agregat.

Sejak: 1.0

Opsional: Salah

`accountId`

ID akun yang menerima acara ini.

Sejak: 1.0

Opsional: Salah

`eventId`

GUID yang dihasilkan oleh CloudTrail untuk mengidentifikasi secara unik setiap peristiwa agregat. Anda dapat menggunakan nilai ini untuk mengidentifikasi satu peristiwa. Misalnya, Anda dapat menggunakan ID sebagai kunci utama untuk mengambil data log dari database yang dapat dicari.

Sejak: 1.0

Opsional: Salah

`eventCategory`

Mengidentifikasi kategori acara. Untuk peristiwa agregat, nilai ini selaluAggregated. Gunakan bidang ini untuk memfilter saat Anda menanyakan peristiwa berdasarkan kategori.

Sejak: 1.0

Opsional: Salah

`eventType`

Mengidentifikasi jenis peristiwa agregat. Untuk peristiwa agregat, nilai ini adalahAwsAggregatedEvent.

Sejak: 1.0

Opsional: Salah

`awsRegion`

CloudTrail Peristiwa atom yang dikumpulkan ke dalam catatan ini, sepertiap-northeast-1. Wilayah AWS Ini biasanya Wilayah tempat panggilan API layanan dilakukan.

Sejak: 1.0

Opsional: Salah

`eventSource`

AWS Layanan di mana peristiwa yang mendasarinya dicatat.

Sejak: 1.0

Opsional: Salah

`timeWindow`

Interval waktu di mana CloudTrail peristiwa atom dikumpulkan ke dalam catatan peristiwa agregat ini. `timeWindow`Bidang berisi rincian seperti waktu mulai jendela, waktu akhir jendela dan ukuran jendela.

Sejak: 1.0

Opsional: Salah

`windowStart`

Awal jendela agregasi, inklusif, dalam Waktu Universal (UTC), diwakili dalam format ISO-8601.

Sejak: 1.0

Opsional: Salah

`windowEnd`

Akhir jendela agregasi, eksklusif, dalam UTC, diwakili dalam format ISO-8601.

Sejak: 1.0

Opsional: Salah

`windowSize`

Durasi jendela agregasi. Perbedaannya `windowEnd - windowStart` harus sesuai dengan`windowSize`. `windowSize`Ini diwakili dalam format ISO-8601.

Sejak: 1.0

Opsional: Salah

`summary`

Ringkasan agregasi untuk peristiwa atom yang mendasarinya, dikelompokkan berdasarkan dimensi primer (misalnya,`eventName`, `resourceARN` atau`userIdentity`) dan secara opsional dipecah berdasarkan dimensi tambahan (misalnya,,`userAgent`,`sourceIpAddress`). `errorCodes`

Sejak: 1.0

Opsional: Salah

Ringkasan berisi bidang-bidang berikut:

primaryDimension

Dimensi agregasi utama untuk iniAwsAggregatedEvent. Ini adalah tampilan utama dari data agregat. Misalnya, dalam template API_ACTIVITY agregasi, dimensi utama adalaheventName; dalam RESOURCE_ACCESS template, ituresourceARN; dan dalam USER_ACTIONS template, ituuserIdentity.

Sejak: 1.0

Opsional: Salah

details

Dimensi tambahan yang memberikan detail lebih lanjut tentang peristiwa atom agregat. Setiap objek Detail dapat memberikan tampilan tambahan dari peristiwa mendasar yang sama, sepertieventName,,resourceARN,userIdentity, userAgent dan sourceIpAddress tergantung pada template agregasi.

Sejak: 1.0

Opsional: Salah

Setiap detail memberikan informasi berikut:

dimension

Nama dimensi yang digunakan untuk mengelompokkan peristiwa agregat. Nilai umum meliputi:

- eventName
- resourceARN
- userIdentity
- userAgent
- sourceIpAddress

Sejak: 1.0

Opsional: Salah

statistics

Daftar statistik untuk dimensi ini, di mana setiap entri mewakili satu ember (misalnya, satu nama acara atau satu sumber ARN) dan nilai agregatnya.

Sejak: 1.0

Opsional: Salah

Setiap entri dalam statistik berisi informasi berikut:

`name`

Pengenal bucket atau kunci untuk statistik ini dalam dimensi terkait.

`value`

Nilai numerik agregat untuk nama yang ditentukan dalam dimensi yang diberikan.

`aggregationType`

Jenis agregasi yang diterapkan `statistics.value` untuk menghitung dimensi ini. Nilai yang diizinkan:

- `Count`— Jumlah acara.

Sejak: 1.0

Opsional: Salah

`addendum`

Membawa metadata tentang pengiriman yang tertunda atau pembaruan ke yang sudah ada. AggregatedEvent

Sejak: 1.0

Opsional: Salah

`reason`

Alasan mengapa `AwsAggregatedEvent` ditunda, diperbarui, atau ditambah. Nilai umum dapat mencakup (tidak lengkap):

- `DELIVERY_DELAY`Pengiriman data agregat tertunda (misalnya, masalah jaringan atau volume tinggi).
- `UPDATED_DATA`— Data agregat dihitung ulang atau diperbaiki.
- `SERVICE_OUTAGE`— Pemadaman layanan yang mendasari memengaruhi ketersediaan acara.

Sejak: 1.0

Opsional: Benar

Contoh acara agregat

Berikut ini adalah contoh dari peristiwa CloudTrail agregat (`AwsAggregatedEvent`). Dalam contoh ini, CloudTrail agregat `PutAuditEvents` panggilan ke `cloudtrail-data.amazonaws.com` lebih dari jendela waktu lima menit di Wilayah. `us-east-1` Blok ringkasan menunjukkan dimensi agregasi utama (`eventName`) dan 30 `PutAuditEvents` panggilan terjadi selama jendela waktu. Entri detail lebih lanjut memecah panggilan tersebut oleh`resourceARN`,, `userIdentityuserAgent`, dan `sourceIpAddress` untuk menunjukkan bagaimana aktivitas didistribusikan di seluruh sumber daya, kepala sekolah, dan klien.

```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "4da798a8-1db6-4d17-8b51-4c33df06b56d",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-east-1",
    "eventSource": "cloudtrail-data.amazonaws.com",
    "timeWindow":
    {
        "windowStart": "2025-10-30 23:45:00",
        "windowEnd": "2025-10-30 23:50:00",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "eventName",
            "statistics":
            [
                {
                    "name": "PutAuditEvents",
                    "value": 30
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
            {
                "dimension": "resourceARN",
```

```
                "statistics":
                [
                    {
                        "name": "arn:aws:cloudtrail:us-
east-1:111122223333:channel/1234abcd-12ab-34cd-56ef-1234567890ab",
                        "value": 20
                    },
                    {
                        "name": "arn:aws:cloudtrail:us-
east-1:111122223333:channel/6789abcd-12ab-34cd-56ef-6789012345ab",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            },
            {
                "dimension": "userIdentity",
                "statistics":
                [
                    {
                        "name": "AWSAccount:111122223333",
                        "value": 20
                    },
                    {
                        "name": "AWSService:AWS Internal",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            },
            {
                "dimension": "userAgent",
                "statistics":
                [
                    {
                        "name": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0)
 Gecko/20100101 Firefox/102.0",
                        "value": 20
                    },
                    {
                        "name": "AWS Internal",
                        "value":10
                    }
                ],
```

```
                "aggregationType": "Count"
            },
            {
                "dimension": "sourceIpAddress",
                "statistics":
                [
                    {
                        "name": "1.2.3.4",
                        "value": 20
                    },
                    {
                        "name": "AWS Internal",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            }
        ]
    }
}
```

CloudTrail merekam konten untuk acara Insights untuk jalur

AWS CloudTrail Catatan peristiwa wawasan untuk jalur mencakup bidang yang berbeda dari CloudTrail peristiwa lain dalam struktur JSON mereka, kadang-kadang disebut payload. CloudTrail Peristiwa wawasan untuk jalur berisi bidang berikut:

- **`eventVersion`**— Versi acara.

  Sejak: 1.07

  Opsional: Salah
- **`eventType`**— Jenis acara. Nilainya selalu `AwsCloudTrailInsight` untuk acara Insights.

  Sejak: 1.07

  Opsional: Salah
- **`eventID`**— GUID yang dihasilkan oleh CloudTrail untuk mengidentifikasi setiap peristiwa secara unik. Anda dapat menggunakan nilai ini untuk mengidentifikasi satu peristiwa. Misalnya, Anda dapat menggunakan ID sebagai kunci utama untuk mengambil data log dari database yang dapat dicari.

Sejak: 1.07

Opsional: Salah

- **`eventTime`**— Waktu acara Insights dimulai atau dihentikan, dalam waktu universal terkoordinasi (UTC).

  Sejak: 1.07

  Opsional: Salah

- **`awsRegion`**— Wilayah AWS Tempat kejadian Wawasan terjadi, seperti`us-east-2`.

  Sejak: 1.07

  Opsional: Salah

- **`recipientAccountId`**— Merupakan ID akun yang menerima acara ini.

  Sejak: 1.07

  Opsional: Benar

- **`sharedEventID`**— GUID yang dihasilkan oleh CloudTrail Insights untuk mengidentifikasi peristiwa Insights secara unik. `sharedEventID`merupakan hal umum antara acara Insights awal dan akhir, dan membantu menghubungkan kedua peristiwa tersebut untuk mengidentifikasi aktivitas yang tidak biasa secara unik. Anda dapat menganggapnya `sharedEventID` sebagai ID peristiwa Insights keseluruhan.

  Sejak: 1.07

  Opsional: Salah

- **`insightDetails`**— Catatan peristiwa CloudTrail Insights untuk jejak mencakup `insightDetails` blok yang berisi informasi tentang pemicu yang mendasari peristiwa Insights, seperti sumber peristiwa, identitas pengguna, agen pengguna, ARN sumber daya, rata-rata historis atau garis dasar, statistik, nama API, dan apakah peristiwa tersebut merupakan awal atau akhir dari acara Insights.

  Sejak: 1.07

  Opsional: Salah

- **`state`**— Apakah acara tersebut merupakan acara Insights awal atau akhir. Nilai dapat berupa `Start` atau `End`.

  Sejak: 1.07

  Opsional: Salah

- **`eventSource`**— AWS Layanan yang menjadi sumber aktivitas yang tidak biasa, seperti`ec2.amazonaws.com`.

  Sejak: 1.07

  Opsional: Salah

- **`eventName`**— Nama acara Insights, biasanya nama API yang merupakan sumber aktivitas yang tidak biasa.

  Sejak: 1.07

  Opsional: Salah

- **`insightType`**— Jenis acara Wawasan. Nilai ini bisa jadi `ApiCallRateInsight` atau `ApiErrorRateInsight`.

  Sejak: 1.07

  Opsional: Salah

- **`errorCode`**— Kode kesalahan dari aktivitas yang tidak biasa. Lihat juga `errorCode` di CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

  Sejak: 1.07

  Opsional: Benar

- **`insightContext`**Informasi tentang AWS alat (disebut agen pengguna), pengguna dan peran IAM (disebut identitas pengguna), kode kesalahan, dan ARN sumber daya yang terkait dengan peristiwa yang CloudTrail dianalisis untuk menghasilkan peristiwa Wawasan. Elemen ini juga mencakup statistik yang menunjukkan bagaimana aktivitas yang tidak biasa dalam peristiwa Wawasan dibandingkan dengan aktivitas dasar, atau aktivitas normal.

  Sejak: 1.07

  Opsional: Salah

- **`statistics`**— Termasuk data tentang baseline, atau tingkat rata-rata umum panggilan ke atau kesalahan pada API subjek oleh akun sebagaimana diukur selama periode dasar, tingkat rata-rata panggilan atau kesalahan yang memicu peristiwa Wawasan, durasi, dalam menit, dari peristiwa Wawasan, dan durasi, dalam menit, dari periode pengukuran dasar.

  Sejak: 1.07

  Opsional: Salah

  - **`baseline`**— Panggilan API atau kesalahan per menit selama durasi dasar pada API subjek acara Insights untuk akun, dihitung selama tujuh hari sebelum dimulainya acara Insights.

    Sejak: 1.07

    Opsional: Salah

    - **`average`**— Rata-rata historis panggilan API atau kesalahan per menit selama tujuh hari sebelum waktu mulai aktivitas Insights.

      Sejak: 1.07

      Opsional: Salah

  - **`insight`**— Untuk acara Insights awal, nilai ini adalah jumlah rata-rata panggilan API atau kesalahan per menit selama awal aktivitas yang tidak biasa. Untuk acara Insights akhir, nilai ini adalah jumlah rata-rata panggilan API atau kesalahan per menit selama durasi aktivitas yang tidak biasa.

    Sejak: 1.07

    Opsional: Salah

    - **`average`**— Jumlah rata-rata panggilan API atau kesalahan yang dicatat per menit selama periode aktivitas yang tidak biasa.

      Sejak: 1.07

      Opsional: Salah

  - **`insightDuration`**— Durasi, dalam menit, dari acara Insights (periode waktu dari awal hingga akhir aktivitas yang tidak biasa pada API subjek). `insightDuration`terjadi di acara Insights awal dan akhir.

    Sejak: 1.07

Opsional: Salah

- **`baselineDuration`**— Durasi, dalam menit, dari periode dasar (periode waktu aktivitas normal diukur pada API subjek). `baselineDuration`minimal tujuh hari (10080 menit) sebelum acara Insights. Bidang ini muncul di acara Insights awal dan akhir. Waktu akhir `baselineDuration` pengukuran selalu merupakan awal dari acara Insights.

  Sejak: 1.07

  Opsional: Salah

- **`attributions`**— Termasuk informasi tentang identitas pengguna, agen pengguna, kode kesalahan, dan ARN sumber daya yang berkorelasi dengan aktivitas yang tidak biasa dan aktivitas dasar. Maksimal lima identitas pengguna, lima agen pengguna, lima kode kesalahan, dan lima ARN sumber daya ditangkap dalam `attributions` blok peristiwa Insights, diurutkan berdasarkan rata-rata jumlah aktivitas, dalam urutan menurun dari tertinggi ke terendah.

  Sejak: 1.07

  Opsional: Benar

  - **`attribute`**— Berisi jenis atribut. Nilai bisa`userIdentityArn`,`userAgent`,`errorCode`, atau`resourceArn`. Jika ada, nilai-nilai ini hanya akan muncul sekali dalam atribut individual. Nilai atribut yang berbeda dapat memiliki `resourceArn` nilai`userIdentityArn`,`userAgent`,`errorCode`, atau yang berbeda, tetapi setiap instance atribut hanya akan berisi satu nilai untuk`userIdentityArn`,`userAgent`,`errorCode`, atau`resourceArn`. A `resourceArn` tribut hanya tersedia untuk peristiwa Wawasan pada peristiwa data.

    Sejak: 1.07

    Opsional: Salah

  - **`insight`**Blok yang menampilkan lima nilai atribut teratas yang berkontribusi pada panggilan API atau kesalahan yang dibuat selama periode aktivitas yang tidak biasa, dalam urutan menurun dari jumlah panggilan atau kesalahan API terbesar hingga terkecil. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dibuat oleh nilai atribut selama periode aktivitas yang tidak biasa.

    Sejak: 1.07

Opsional: Salah

- **value**— Atribut yang berkontribusi pada panggilan API atau kesalahan yang dibuat selama periode aktivitas yang tidak biasa.

  Sejak: 1.07

  Opsional: Salah Salah

- **average**— Jumlah panggilan API atau kesalahan per menit selama periode aktivitas yang tidak biasa untuk atribut di `value` lapangan.

  Sejak: 1.07

  Opsional: Salah Salah

- **baseline**Blok yang menampilkan lima nilai atribut teratas yang berkontribusi paling besar terhadap panggilan atau kesalahan API selama periode aktivitas normal, dalam urutan menurun dari jumlah panggilan atau kesalahan API terbesar ke terkecil. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dibuat oleh nilai atribut selama periode aktivitas normal.

  Sejak: 1.07

  Opsional: Salah Salah

  - **value**— Atribut yang berkontribusi pada panggilan atau kesalahan API selama periode aktivitas normal.

    Sejak: 1.07

    Opsional: Salah Salah

  - **average**— Rata-rata historis panggilan API atau kesalahan per menit selama tujuh hari sebelum waktu mulai aktivitas Insights untuk atribut di `value` lapangan.

    Sejak: 1.07

    Optional:FalseSalah

- **eventCategory**— Kategori acara. Nilainya selalu `Insight` untuk acara Insights.

  Sejak: 1.07

  Opsional: Salah

Contoh blok **InsightDetails**

Berikut ini adalah contoh `insightDetails` blok peristiwa Insights untuk peristiwa Insights yang terjadi ketika API Penskalaan Otomatis Aplikasi di `CompleteLifecycleAction` panggil beberapa kali yang tidak biasa. Untuk contoh acara Wawasan lengkap, lihatInsights acara.

Contoh ini berasal dari acara Insights awal, ditunjukkan oleh`"state": "Start"`. Identitas pengguna teratas yang memanggil API yang terkait dengan peristiwa Insights `CodeDeployRole1CodeDeployRole2`,,`CodeDeployRole3`, dan, ditampilkan di `attributions` blok, bersama dengan rata-rata tingkat panggilan API untuk acara Insights ini, dan baseline untuk `CodeDeployRole1` peran tersebut. `attributions`Blok ini juga menunjukkan bahwa agen pengguna adalah`codedeploy.amazonaws.com`, yang berarti identitas pengguna teratas menggunakan AWS CodeDeploy konsol untuk menjalankan panggilan API.

Karena tidak ada kode kesalahan yang terkait dengan peristiwa yang dianalisis untuk menghasilkan peristiwa Wawasan (nilainya adalah`null`), `insight` rata-rata untuk kode kesalahan sama dengan `insight` rata-rata keseluruhan untuk seluruh peristiwa Wawasan, yang ditampilkan di `statistics` blok.

```
        "insightDetails": {
          "state": "Start",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
                "average": 0.0000882145
              },
              "insight": {
                "average": 0.6
              },
              "insightDuration": 5,
              "baselineDuration": 11336
            },
            "attributions": [
              {
                "attribute": "userIdentityArn",
                "insight": [
                  {
```

```
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                    "average": 0.2
                  },
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                    "average": 0.2
                  }
                ],
                "baseline": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
```

```
            }
          ],
          "baseline": [
            {
              "value": "null",
              "average": 0.0000882145
            }
          ]
        },
        {
          "attribute": "resourceArn",
          "insight": [
            {
              "value": "arn:aws:s3:::example-bucket",
              "average": 0.6
            }
          ],
          "baseline": [
            {
              "value": "arn:aws:s3:::example-bucket",
              "average": 0.0000882145
            }
          ]
        }
      ]
    }
  }
```

CloudTrail merekam konten untuk acara Wawasan untuk penyimpanan data acara

AWS CloudTrail Catatan peristiwa wawasan untuk penyimpanan data peristiwa mencakup bidang yang berbeda dari CloudTrail peristiwa lain dalam struktur JSON mereka, kadang-kadang disebut payload. Catatan peristiwa CloudTrail Insights untuk penyimpanan data acara mencakup bidang-bidang berikut:

> **Note**
>
> Bidang `insightValueinsightAverage`,`baselineValue`, dan `baselineAverage` bidang dalam `attributions` bidang `insightContext` akan mulai tidak digunakan lagi pada 23 Juni 2025.

- **`eventVersion`**— Versi format peristiwa log.

  Opsional: Salah
- **`eventCategory`**- Kategori acara. Nilai selalu `Insight` untuk acara Insights.

  Opsional: Salah
- **`eventType`**— Jenis acara. Nilai selalu `AwsCloudTrailInsight` untuk acara Insights.

  Opsional: Salah
- **`eventID`**— GUID dihasilkan oleh CloudTrail untuk mengidentifikasi setiap peristiwa secara unik. Anda dapat menggunakan nilai ini untuk mengidentifikasi satu peristiwa. Misalnya, Anda dapat menggunakan ID sebagai kunci utama untuk mengambil data log dari database yang dapat dicari.

  Opsional: Salah
- **`eventTime`**— Waktu acara Insights dimulai atau dihentikan, dalam waktu universal terkoordinasi (UTC).

  Opsional: Salah
- **`awsRegion`**— Di Wilayah AWS mana peristiwa Insights terjadi, sepertius`-east-2`.

  Opsional: Salah
- **`recipientAccountId`**— Merupakan ID akun yang menerima acara ini.

  Opsional: Benar
- **`sharedEventID`**— GUID yang dihasilkan oleh CloudTrail Insights untuk mengidentifikasi peristiwa Insights secara unik. `sharedEventID`adalah umum antara awal dan akhir peristiwa Wawasan, dan membantu menghubungkan kedua peristiwa untuk mengidentifikasi aktivitas yang tidak biasa secara unik. Anda dapat menganggapnya `sharedEventID` sebagai ID acara Insights keseluruhan.

  Opsional: Salah

- **`addendum`**Jika pengiriman acara tertunda, atau informasi tambahan tentang peristiwa yang ada tersedia setelah acara dicatat, bidang addendum menunjukkan informasi tentang mengapa acara ditunda. Jika informasi hilang dari peristiwa yang ada, bidang addendum mencakup informasi yang hilang dan alasan mengapa itu hilang. Lihat juga `addendum` di CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

  Opsional: Benar

- **`insightSource`**— Penyimpanan data acara sumber yang mengumpulkan peristiwa manajemen yang dianalisis.

  Opsional: Salah

- **`insightState`**— Apakah acara tersebut merupakan acara Insights awal atau akhir. Nilai dapat berupa `Start` atau `End`.

  Opsional: Salah

- **`insightEventSource`**— Layanan AWS Itu adalah sumber aktivitas yang tidak biasa, seperti`ec2.amazonaws.com`.

  Opsional: Salah

- **`insightEventName`**— Nama acara Insights, biasanya nama API yang merupakan sumber aktivitas yang tidak biasa.

  Opsional: Salah

- **`insightErrorCode`**— Kode kesalahan dari aktivitas yang tidak biasa. Lihat juga `errorCode` di CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

  Opsional: Benar

- **`insightType`**— Jenis acara Wawasan. Nilai ini bisa jadi `ApiCallRateInsight` atau `ApiErrorRateInsight`.

  Opsional: Salah

- **`insightContext`**— Berisi informasi tentang pemicu yang mendasari peristiwa Wawasan, seperti identitas pengguna, agen pengguna, rata-rata historis atau garis dasar, serta durasi dan rata-rata Wawasan.

  Opsional: Salah

- **`baselineAverage`**— Rata-rata jumlah panggilan API atau error per menit selama durasi baseline pada API subjek acara Insights untuk akun, dihitung selama tujuh hari sebelum dimulainya acara Insights.

  Opsional: Salah

- **`insightAverage`**— Untuk acara Insights awal, nilai ini adalah jumlah rata-rata panggilan API atau kesalahan per menit selama dimulainya aktivitas yang tidak biasa. Untuk acara Insights yang berakhir, nilai ini adalah jumlah rata-rata panggilan API atau error per menit selama durasi aktivitas yang tidak biasa.

  Opsional: Salah

- **`baselineDuration`**— Durasi, dalam menit, dari periode dasar (periode waktu aktivitas normal diukur pada API subjek). `baselineDuration`minimal tujuh hari (10080 menit) sebelum acara Insights. Bidang ini terjadi di acara Insights awal dan akhir. Waktu akhir `baselineDuration` pengukuran selalu merupakan awal dari peristiwa Wawasan.

  Opsional: Salah

- **`insightDuration`**— Durasi, dalam hitungan menit, acara Insights (periode waktu dari awal hingga akhir aktivitas yang tidak biasa pada API subjek). `insightDuratio`nterjadi di acara Insights awal dan akhir.

  Opsional: Salah

- **`attributions`**— Termasuk informasi tentang identitas pengguna, agen pengguna, atau kode kesalahan yang berkorelasi dengan aktivitas yang tidak biasa dan dasar.

  Opsional: Benar

  > **Note**
  >
  > Bidang `insightValueinsightAverage`,`baselineValue`, dan `baselineAverage` bidang dalam `attributions` bidang `insightContext` akan mulai tidak digunakan lagi pada 23 Juni 2025.

  - **`attribute`**— Berisi jenis atribut. Nilai bisa`userIdentityArn`,`userAgent`, atau`errorCode`. Jika ada, nilai-nilai ini akan muncul hanya sekali dalam atribut individu. Nilai atribut yang berbeda dapat memiliki `errorCode` nilai yang berbeda

`userIdentityArnuserAgent`,, atau, tetapi setiap instance atribut hanya akan berisi satu nilai untuk`userIdentityArn`,`userAgent`, atau`errorCode`.

Opsional: Salah

- **`insightValue`**— Nilai atribut teratas yang terjadi pada panggilan API atau kesalahan yang dibuat selama periode aktivitas yang tidak biasa.

  Opsional: Salah

- **`insightAverage`**— Jumlah panggilan API atau kesalahan per menit selama periode aktivitas yang tidak biasa untuk atribut di `insightValue` bidang.

  Opsional: Salah

- **`baselineValue`**— Nilai atribut teratas yang berkontribusi pada panggilan API atau kesalahan yang dicatat selama periode aktivitas normal.

  Opsional: Salah

- **`baselineAverage`**— Rata-rata historis panggilan API atau kesalahan per menit selama tujuh hari sebelum waktu mulai aktivitas Wawasan untuk atribut di bidang. `baselineValue`

  Opsional: Salah

- **`insight`**— Lima nilai atribut teratas yang berkontribusi pada panggilan API atau kesalahan yang dibuat selama periode aktivitas yang tidak biasa. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dibuat oleh atribut selama periode aktivitas yang tidak biasa.

  Opsional: Salah

  - **`value`**— Atribut yang berkontribusi pada panggilan API atau kesalahan yang dibuat selama periode aktivitas yang tidak biasa.

    Opsional: Salah

  - **`average`**— Rata-rata jumlah panggilan API atau kesalahan per menit selama periode aktivitas yang tidak biasa untuk atribut di `value` bidang.

    Opsional: Salah

- **`baseline`**— Lima nilai atribut teratas yang berkontribusi paling besar terhadap panggilan atau kesalahan API selama periode aktivitas normal. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dicatat oleh nilai atribut selama periode aktivitas normal.

Opsional: Salah

- **`value`**— Atribut yang berkontribusi pada panggilan API atau kesalahan selama periode aktivitas normal.

  Opsional: Salah

- **`average`**— Rata-rata historis panggilan API atau kesalahan per menit selama tujuh hari sebelum waktu mulai aktivitas Wawasan untuk atribut di bidang. `value`

  Opsional: Salah

CloudTrail elemen userIdentity

AWS Identity and Access Management (IAM) menyediakan berbagai jenis identitas. `userIdentity`Elemen berisi rincian tentang jenis identitas IAM yang membuat permintaan, dan kredensi mana yang digunakan. Jika kredensial sementara digunakan, elemen menunjukkan bagaimana kredensialnya diperoleh.

Daftar Isi

- Contoh
- Bidang
- Nilai untuk AWS STS API dengan SAFL dan federasi identitas web
- AWS STS identitas sumber

Contoh

`userIdentity`dengan kredensil pengguna IAM

Contoh berikut menunjukkan `userIdentity` elemen permintaan sederhana yang dibuat dengan kredensil dari pengguna IAM bernama. `Alice`

```
"userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJ45Q7YFFAREXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "",
```

```
    "userName": "Alice"
}
```

`userIdentity`dengan kredensil keamanan sementara

Contoh berikut menunjukkan `userIdentity` elemen untuk permintaan yang dibuat dengan kredensil keamanan sementara yang diperoleh dengan mengasumsikan peran IAM. Elemen berisi rincian tambahan tentang peran yang diasumsikan untuk mendapatkan kredensional.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAIDPPEZS35WEXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
            "accountId": "123456789012",
            "userName": "RoleToBeAssumed"
        },
        "signInSessionArn": "arn:aws:signin:us-east-1:123456789012:session/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    }
}
```

`userIdentity`untuk permintaan yang dibuat atas nama pengguna IAM Identity Center

Contoh berikut menunjukkan `userIdentity` elemen untuk permintaan yang dibuat atas nama pengguna IAM Identity Center.

```
"userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "123456789012",
    "onBehalfOf": {
        "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
```

```
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9067642ac7"
    },
    "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

Untuk mempelajari selengkapnya tentang cara Anda dapat menggunakan`userId`,`identityStoreArn`, dan`credentialId`, lihat Mengidentifikasi pengguna dan sesi dalam CloudTrail peristiwa yang dimulai pengguna Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM.

`userIdentity`untuk permintaan yang dibuat oleh pengguna AWS Builder ID

Contoh berikut menunjukkan `userIdentity` elemen untuk permintaan yang dibuat oleh pengguna AWS Builder ID. AWS Builder ID adalah profil pribadi yang menyediakan akses ke alat dan layanan tertentu termasuk AWS Builder Center, Amazon Q Developer, dan AWS Pelatihan dan Sertifikasi. `BuilderIdUser`Jenis ini muncul dalam CloudTrail peristiwa ketika permintaan API diotorisasi menggunakan token akses yang OAuth dikeluarkan Pusat Identitas IAM (otentikasi pembawa). Token ini dikaitkan dengan AWS Builder ID.

```
"userIdentity": {
    "type": "BuilderIdUser",
    "onBehalfOf": {
        "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
        "identityStoreArn": "arn:aws:identitystore::aws:identitystore/builderid"
    },
    "credentialId": "ABCDefGhiJKLMn11Lmn_1AbCDEFgHijk-AaBCdEFGHIjKLmnOPqrs11abEXAMPLE"
}
```

Tidak seperti `IdentityCenterUser` `BuilderIdUser` peristiwa, peristiwa tidak menyertakan `accountId` bidang karena AWS Builder ID adalah identitas AWS-managed yang tidak terkait dengan pelanggan Akun AWS tertentu.

Untuk informasi selengkapnya tentang AWS Builder ID, lihat Masuk dengan AWS Builder ID di Panduan AWS Sign-In Pengguna.

`userIdentity`dengan permintaan yang diprakarsai oleh penyedia produk

Semua tindakan yang dilakukan oleh penyedia produk menggunakan akses delegasi sementara secara otomatis masuk CloudTrail. Ini memberikan visibilitas lengkap dan auditabilitas aktivitas

penyedia produk di akun Anda AWS . Anda dapat mengidentifikasi tindakan mana yang diambil oleh penyedia produk, kapan itu terjadi, dan akun penyedia produk mana yang melakukannya.

Untuk membantu Anda membedakan antara tindakan yang diambil oleh prinsipal IAM Anda sendiri dan tindakan yang diambil oleh penyedia produk dengan akses yang didelegasikan, CloudTrail acara menyertakan bidang baru yang disebut di bawah elemen. `invokedByDelegate` `userIdentity` Bidang ini berisi ID AWS akun penyedia produk, sehingga mudah untuk memfilter dan mengaudit semua tindakan yang didelegasikan.

Contoh berikut menunjukkan `userIdentity` elemen untuk tindakan yang dilakukan oleh penyedia produk menggunakan akses didelegasikan sementara.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI...",
    "arn": "arn:aws:sts::123456789012:assumed-role/Alice/Session",
    "accountId": "123456789012",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAI...",
            "arn": "arn:aws:iam::123456789012:role/Alice",
            "accountId": "123456789012",
            "userName": "Alice"
        },
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    },
    "invokedByDelegate": {
        "accountId": "999999999999"
    }
}
```

`invokedByDelegate`Kolom berisi ID AWS akun penyedia produk yang melakukan tindakan menggunakan akses yang didelegasikan. Dalam contoh ini, akun 999999999999 (penyedia produk) melakukan tindakan di akun 123456789012 (akun pelanggan).

Bidang

Bidang berikut dapat muncul dalam `userIdentity` elemen.

`type`

Jenis identitas. Nilai-nilai berikut dimungkinkan:

- `Root`— Permintaan dibuat dengan Akun AWS kredensialmu. Jika `userIdentity` jenisnya`Root`, dan Anda menetapkan alias untuk akun Anda, `userName` bidang berisi alias akun Anda. Untuk informasi selengkapnya, lihat Akun AWS ID Anda dan aliasnya.
- `IAMUser`— Permintaan dibuat dengan kredensil pengguna IAM.
- `AssumedRole`— Permintaan dibuat dengan kredensil keamanan sementara yang diperoleh dengan peran dengan melakukan panggilan ke AWS Security Token Service (AWS STS) `AssumeRole`API. Ini dapat mencakup peran untuk Amazon EC2 dan akses API lintas akun.
- `Role`— Permintaan dibuat dengan identitas IAM persisten yang memiliki izin khusus. Penerbit sesi peran selalu menjadi peran. Untuk informasi selengkapnya tentang peran, lihat Istilah dan konsep peran dalam Panduan Pengguna IAM.
- `FederatedUser`— Permintaan dibuat dengan kredensil keamanan sementara yang diperoleh dari panggilan ke API. AWS STS `GetFederationToken` `sessionIssuer`Elemen menunjukkan apakah API dipanggil dengan kredenal pengguna root atau IAM.

  Untuk informasi selengkapnya tentang kredensial keamanan sementara, lihat Kredensial Keamanan Sementara dalam Panduan Pengguna IAM.
- `Directory`— Permintaan dibuat ke layanan direktori, dan jenisnya tidak diketahui. Layanan direktori meliputi: Amazon WorkDocs dan Amazon Quick.
- `AWSAccount`Permintaan itu dibuat oleh orang lain Akun AWS
- `AWSService`— Permintaan itu dibuat oleh seorang Akun AWS yang menjadi milik sebuah Layanan AWS. Misalnya, AWS Elastic Beanstalk mengasumsikan peran IAM di akun Anda untuk menelepon orang lain Layanan AWS atas nama Anda.
- `IdentityCenterUser`— Permintaan dibuat atas nama pengguna IAM Identity Center.
- `BuilderIdUser`— Permintaan dibuat oleh pengguna AWS Builder ID. Tidak seperti`IdentityCenterUser`, `BuilderIdUser` tipe tidak menyertakan `accountId` bidang karena AWS Builder ID adalah identitas AWS-managed yang tidak terikat ke akun pelanggan tertentu.
- `Unknown`— Permintaan dibuat dengan tipe identitas yang tidak CloudTrail dapat ditentukan.

Opsional: Salah

`AWSAccount`dan `AWSService` muncul `type` di log Anda ketika ada akses lintas akun menggunakan peran IAM yang Anda miliki.

Contoh: Cross-account akses yang diprakarsai oleh orang lain AWS akun

1. Anda memiliki peran IAM di akun Anda.
2. AWS Akun lain beralih ke peran itu untuk mengambil peran untuk akun Anda.
3. Karena Anda memiliki peran IAM, Anda menerima log yang menunjukkan akun lain yang mengambil peran tersebut. `type` adalah `AWSAccount`. Untuk contoh entri log, lihat peristiwa AWS STS API di file CloudTrail log.

Contoh: Cross-account akses yang diprakarsai oleh AWS layanan

1. Anda memiliki peran IAM di akun Anda.
2. AWS Akun yang dimiliki oleh AWS layanan mengasumsikan peran itu.
3. Karena Anda memiliki peran IAM, Anda menerima log yang menunjukkan AWS layanan mengambil peran tersebut. `type` adalah `AWSService`.

`userName`

Nama ramah dari identitas yang membuat panggilan. Nilai yang muncul di `userName` didasarkan pada nilai dalam`type`. Tabel berikut menunjukkan hubungan antara `type` dan`userName`:

`type`	**`userName`**	Deskripsi
`Root`(tidak ada set alias)	Tidak hadir	Jika Anda belum menyiapkan alias untuk Anda Akun AWS, `userName` bidang tidak muncul. Untuk informasi selengkapnya tentang alias akun, lihat Akun AWS ID Anda dan aliasnya. Perhatikan bahwa `userName` bidang tidak dapat berisi`Root`, karena `Root` merupakan tipe identitas dan bukan nama pengguna.
`Root`(alias set)	Alias akun	Untuk informasi selengkapnya tentang Akun AWS alias, lihat Akun AWS ID Anda dan aliasnya.
`IAMUser`	Nama pengguna pengguna IAM	

type	userName	Deskripsi
AssumedRole	Tidak hadir	Untuk AssumedRole jenisnya, Anda dapat menemukan userName bidang sessionContext sebagai bagian dari elemen SessionIssuer. Untuk entri contoh, lihatContoh.
Role	User-defined	sessionIssuer Bagian sessionContext dan berisi informasi tentang identitas yang mengeluarkan sesi untuk peran tersebut.
FederatedUser	Tidak hadir	sessionIssuer Bagian sessionContext dan berisi informasi tentang identitas yang mengeluarkan sesi untuk pengguna federasi.
Directory	Bisa hadir	Misalnya, nilainya bisa berupa alias akun atau alamat email dari Akun AWS ID terkait.
AWSService	Tidak hadir	
AWSAccount	Tidak hadir	
IdentityCenterUser	Tidak hadir*	onBehalfOf Bagian ini berisi informasi tentang ID pengguna Pusat Identitas IAM dan ARN toko identitas tempat panggilan dilakukan. Untuk mempelajari lebih lanjut tentang bagaimana Anda dapat menggunakan dua bidang ini, lihat Mengidentifikasi pengguna dan sesi dalam peristiwa yang dimulai oleh pengguna CloudTrail Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM. * Pusat Identitas IAM memancarkan userName bidang di bawah additionalEventData elemen dalam dua peristiwa masuk CloudTrail . Untuk informasi selengkapnya, lihat Nama pengguna dalam CloudTrail peristiwa login di Panduan Pengguna Pusat Identitas IAM.

type	userName	Deskripsi
BuilderIdUser	Tidak hadir	onBehalfOf Bagian ini berisi pengguna Builder ID userId dan AWS-managed identityStoreArn (arn:aws:identitystore::aws:identitystore/builderid). Gunakan bidang ini untuk mengidentifikasi pengguna Builder ID.
Unknown	Bisa hadir	Misalnya, nilainya bisa berupa alias akun atau alamat email dari Akun AWS ID terkait.

> **Note**
>
> userNameBidang berisi string HIDDEN_DUE_TO_SECURITY_REASONS ketika peristiwa yang direkam adalah kegagalan masuk konsol yang disebabkan oleh input nama pengguna yang salah. CloudTrail tidak merekam konten dalam kasus ini karena teks dapat berisi informasi sensitif, seperti dalam contoh berikut:
>
> - Pengguna secara tidak sengaja mengetikkan kata sandi di bidang nama pengguna.
> - Pengguna mengklik tautan untuk halaman masuk satu AWS akun, tetapi kemudian mengetikkan nomor akun untuk yang berbeda.
> - Pengguna secara tidak sengaja mengetikkan nama akun akun email pribadi, pengenal masuk bank, atau ID pribadi lainnya.

Opsional: Benar

principalId

Pengidentifikasi unik untuk entitas yang melakukan panggilan. Untuk permintaan yang dibuat dengan kredensil keamanan sementara, nilai ini mencakup nama sesi yang diteruskan keAssumeRole,AssumeRoleWithWebIdentity, atau panggilan GetFederationToken API.

Opsional: Benar

arn

Nama Sumber Daya Amazon (ARN) dari kepala sekolah yang melakukan panggilan. Bagian terakhir dari arn berisi pengguna atau peran yang melakukan panggilan.

Opsional: Benar

`accountId`

Akun yang memiliki entitas yang memberikan izin untuk permintaan tersebut. Jika permintaan dibuat dengan kredensil keamanan sementara, ini adalah akun yang memiliki pengguna IAM atau peran yang digunakan untuk mendapatkan kredensil.

Jika permintaan dibuat dengan token akses resmi IAM Identity Center, ini adalah akun yang memiliki instans Pusat Identitas IAM.

> **Note**
>
> Untuk `BuilderIdUser` jenis acara, `accountId` bidang tidak ada. AWS Builder ID adalah identitas AWS yang dikelola yang tidak terkait dengan pelanggan Akun AWS tertentu. `onBehalfOf`Elemen mengidentifikasi pengguna Builder ID sebagai gantinya.

Opsional: Benar

`accessKeyId`

ID kunci akses yang digunakan untuk menandatangani permintaan. Jika permintaan dibuat dengan kredenal keamanan sementara, ini adalah ID kunci akses dari kredenal sementara. Untuk alasan keamanan, `accessKeyId` mungkin tidak ada, atau mungkin ditampilkan sebagai string kosong.

Opsional: Benar

`sessionContext`

Jika permintaan dibuat dengan kredensil keamanan sementara, `sessionContext` berikan informasi tentang sesi yang dibuat untuk kredensil tersebut. Anda membuat sesi saat memanggil API apa pun yang mengembalikan kredensi sementara. Pengguna juga membuat sesi saat mereka bekerja di konsol dan membuat permintaan dengan API yang menyertakan otentikasi multi-faktor. Atribut berikut dapat muncul di`sessionContext`:

- `sessionIssuer`Jika pengguna membuat permintaan dengan kredensil keamanan sementara, `sessionIssuer` memberikan informasi tentang bagaimana pengguna memperoleh kredensil. Misalnya, jika mereka memperoleh kredensil keamanan sementara dengan mengambil peran, elemen ini memberikan informasi tentang peran yang diasumsikan. Jika mereka memperoleh kredensil dengan kredensi pengguna root atau IAM untuk dipanggil AWS STS

`GetFederationToken`, elemen tersebut memberikan informasi tentang akun root atau pengguna IAM. Elemen ini memiliki atribut berikut:

- `type`— Sumber kredensi keamanan sementara, seperti, `RootIAMUser`, atau. `Role`
- `userName`— Nama ramah pengguna atau peran yang mengeluarkan sesi. Nilai yang muncul tergantung pada `sessionIssuer` identitas`type`. Tabel berikut menunjukkan hubungan antara `sessionIssuer type` dan`userName`:

sessionIssuer jenis	**userName**	Deskripsi
`Root`(tidak ada set alias)	Tidak hadir	Jika Anda belum menyiapkan alias untuk akun Anda, `userName` bidang tidak muncul. Untuk informasi selengkapnya tentang Akun AWS alias, lihat Akun AWS ID Anda dan aliasnya. Perhatikan bahwa `userName` bidang tidak dapat berisi`Root`, karena `Root` merupakan tipe identitas, bukan nama pengguna.
`Root`(alias set)	Alias akun	Untuk informasi selengkapnya tentang Akun AWS alias, lihat ID AWS akun Anda dan aliasnya.
`IAMUser`	Nama pengguna pengguna IAM	Ini juga berlaku ketika pengguna federasi menggunakan sesi yang dikeluarkan oleh`IAMUser`.
`Role`	Nama peran	Peran yang diasumsikan oleh pengguna IAM, Layanan AWS, atau pengguna federasi identitas web dalam sesi peran.

- `principalId`— ID internal entitas yang digunakan untuk mendapatkan kredensil.
- `arn`ARN dari sumber (akun, pengguna IAM, atau peran) yang digunakan untuk mendapatkan kredensi keamanan sementara.
- `accountId`— Akun yang memiliki entitas yang digunakan untuk mendapatkan kredensi.

- `webIdFederationData`— Jika permintaan dibuat dengan kredensil keamanan sementara yang diperoleh oleh federasi identitas web, `webIdFederationData` daftar informasi tentang penyedia identitas.

  Elemen ini memiliki atribut berikut:

  - `federatedProvider`— Nama utama penyedia identitas (misalnya, `www.amazon.com` untuk Login with Amazon atau `accounts.google.com` untuk Google).
  - `attributes`— ID aplikasi dan ID pengguna seperti yang dilaporkan oleh penyedia (misalnya, `www.amazon.com:app_id` dan `www.amazon.com:user_id` untuk Login with Amazon).

  > **Note**
  >
  > Kelalaian bidang ini atau keberadaan bidang ini dengan nilai kosong menandakan bahwa tidak ada informasi tentang penyedia identitas.

- `assumedRoot`— Nilai adalah `true` untuk sesi sementara ketika akun manajemen atau panggilan AWS STS `AssumedRoot`administrator yang didelegasikan. Untuk informasi selengkapnya, lihat Melacak tugas istimewa CloudTrail di Panduan Pengguna IAM. Ini adalah bidang opsional.
- `signInSessionArn`— ARN dari sesi masuk yang mendukung permintaan, dalam formulir. `arn:aws:signin:<region>:<account-id>:session/<uuid>` ARN ini adalah nilai dari kunci kondisi `aws:SignInSessionArn` global. Kunci mengidentifikasi sesi lebih spesifik daripada ARN utama. Gunakan untuk mengaudit aktivitas API dengan sesi login, atau untuk menulis kebijakan yang mencabut sesi tertentu.

  Sesi yang berasal dari permintaan dapat berupa sesi masuk. Sesi ini juga dapat berasal dari token akses yang Anda peroleh melalui aliran mesin OAuth atau Signature Version 4 (SigV4). CloudTrail tidak mengubah ARN kepala sekolah. CloudTrail merekam bidang ini pada peristiwa API yang terjadi di bawah sesi tersebut. Ini adalah bidang opsional.
- `attributes`— Atribut untuk sesi.
  - `creationDate`— Tanggal dan waktu ketika kredensi keamanan sementara dikeluarkan. Diwakili dalam notasi dasar ISO 8601.
  - `mfaAuthenticated`— Nilainya adalah `true` jika pengguna root atau pengguna IAM yang menggunakan kredensialnya untuk permintaan tersebut juga diautentikasi dengan perangkat MFA; jika tidak,. `false`

- `sourceIdentity`— Lihat AWS STS identitas sumber di topik ini. `sourceIdentity`Bidang terjadi dalam peristiwa ketika pengguna mengambil peran IAM untuk melakukan tindakan. `sourceIdentity`mengidentifikasi identitas pengguna asli yang membuat permintaan, apakah identitas pengguna tersebut adalah pengguna IAM, peran IAM, pengguna yang diautentikasi melalui federasi, atau pengguna yang diautentikasi melalui SAML-based federasi identitas web yang sesuai dengan OpenID Connect (OIDC). Untuk informasi selengkapnya tentang mengonfigurasi AWS STS untuk mengumpulkan informasi identitas sumber, lihat Memantau dan mengontrol tindakan yang diambil dengan peran yang diasumsikan dalam Panduan Pengguna IAM.
- `ec2RoleDelivery`— Nilainya adalah `1.0` jika kredensialnya disediakan oleh Amazon EC2 Instans Metadata Service Version 1 (IMDSv1). Nilainya adalah `2.0` jika kredensialnya diberikan menggunakan skema IMDS baru.

  AWS kredensional yang disediakan oleh Amazon EC2 Instance Metadata Service (IMDS) menyertakan kunci konteks ec2: IAM. RoleDelivery Kunci konteks ini memudahkan penerapan skema baru berdasarkan layanan demi layanan atau sumber daya demi sumber daya dengan menggunakan kunci konteks sebagai syarat dalam kebijakan IAM, kebijakan sumber daya, atau kebijakan kontrol layanan. AWS Organizations Untuk informasi selengkapnya, lihat Metadata instans dan data pengguna di Panduan Pengguna Amazon EC2.

Opsional: Benar

`invokedBy`

Nama Layanan AWS yang membuat permintaan, ketika permintaan dibuat oleh Layanan AWS seperti Amazon EC2 Auto AWS Elastic Beanstalk Scaling atau. Bidang ini hanya ada ketika permintaan dibuat oleh Layanan AWS. Ini termasuk permintaan yang dibuat oleh layanan menggunakan sesi akses maju (FAS), Layanan AWS kepala sekolah, peran terkait layanan, atau peran layanan yang digunakan oleh file. Layanan AWS

Opsional: Benar

`invokedByDelegate`

Melacak permintaan yang dibuat oleh penyedia produk menggunakan akses delegasi sementara di AWS akun Anda. Bidang ini hanya muncul ketika penyedia produk memulai permintaan API menggunakan izin yang didelegasikan. Jika ada, `invokedByDelegate` berikan informasi tentang akun penyedia produk yang membuat permintaan. Elemen ini memiliki atribut berikut:

- `accountId`— ID AWS akun penyedia produk yang memulai permintaan.

Untuk informasi selengkapnya dan contoh JSON dari akses yang didelegasikan dalam CloudTrail acara, lihat CloudTrail entri untuk kredensil keamanan sementara di Panduan Pengguna IAM.

Opsional: Benar

`onBehalfOf`

Jika permintaan dibuat oleh pemanggil IAM Identity Center atau pengguna AWS Builder ID, `onBehalfOf` berikan informasi tentang pengguna atas nama siapa panggilan itu dibuat. Elemen ini memiliki atribut berikut:

- `userId`— ID pengguna IAM Identity Center atau pengguna AWS Builder ID atas nama siapa panggilan dilakukan.
- `identityStoreArn`— ARN dari toko identitas. Untuk pengguna IAM Identity Center, ini adalah ARN dari toko identitas organisasi. Untuk pengguna AWS Builder ID, nilainya adalah`arn:aws:identitystore::aws:identitystore/builderid`.

Opsional: Benar

`inScopeOf`

Jika permintaan dibuat dalam lingkup Layanan AWS, seperti Lambda atau Amazon ECS, permintaan tersebut memberikan informasi tentang sumber daya atau kredensil yang terkait dengan permintaan tersebut. Elemen ini dapat berisi atribut berikut:

- `sourceArn`— ARN dari sumber daya yang memanggil permintaan layanan-ke-layanan.
- `sourceAccount`— ID akun pemilik untuk`sourceArn`. Itu muncul bersama dengan`sourceArn`.
- `issuerType`— Jenis sumber daya`credentialsIssuedTo`. Misalnya, `AWS::Lambda::Function`.
- `credentialsIssuedTo`— Sumber daya yang terkait dengan lingkungan tempat kredensi dikeluarkan.

Opsional: Benar

`credentialId`

ID kredensi untuk permintaan tersebut. Ini hanya diatur ketika penelepon menggunakan token pembawa, seperti token akses resmi IAM Identity Center.

Opsional: Benar

Nilai untuk AWS STS API dengan SAFL dan federasi identitas web

AWS CloudTrail mendukung logging AWS Security Token Service (AWS STS) panggilan API yang dilakukan dengan Security Assertion Markup Language (SAMB) dan federasi identitas web. Saat pengguna melakukan panggilan ke `AssumeRoleWithWebIdentity`API `AssumeRoleWithSAML`dan, CloudTrail merekam panggilan dan mengirimkan acara ke bucket Amazon S3 Anda.

`userIdentity`Elemen untuk API ini berisi nilai-nilai berikut.

`type`

Tipe identitas.

- `SAMLUser`Permintaan itu dibuat dengan pernyataan SAFL.
- `WebIdentityUser`— Permintaan dibuat oleh penyedia federasi identitas web.

`principalId`

Pengidentifikasi unik untuk entitas yang melakukan panggilan.

- Sebab`SAMLUser`, ini adalah kombinasi dari tombol `saml:namequalifier` dan `saml:sub` tombol.
- Sebab`WebIdentityUser`, ini adalah kombinasi dari penerbit, ID aplikasi, dan ID pengguna.

`userName`

Nama identitas yang membuat panggilan.

- Sebab`SAMLUser`, inilah `saml:sub` kuncinya.
- Untuk`WebIdentityUser`, ini adalah ID pengguna.

`identityProvider`

Nama utama penyedia identitas eksternal. Bidang ini hanya muncul untuk `SAMLUser` atau `WebIdentityUser` jenis.

- Sebab`SAMLUser`, ini adalah `saml:namequalifier` kunci untuk pernyataan SAFL.
- Untuk`WebIdentityUser`, ini adalah nama penerbit penyedia federasi identitas web. Ini bisa menjadi penyedia yang Anda konfigurasikan, seperti berikut ini:
  - `cognito-identity.amazon.com`untuk Amazon Cognito

- `www.amazon.com`untuk Login with Amazon
- `accounts.google.com`untuk Google
- `graph.facebook.com`untuk Facebook

Berikut ini adalah `userIdentity` elemen contoh untuk `AssumeRoleWithWebIdentity` tindakan.

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

Misalnya log tentang bagaimana `userIdentity` elemen muncul `SAMLUser` dan `WebIdentityUser` tipe, lihat Logging IAM dan panggilan AWS STS API dengan AWS CloudTrail.

AWS STS identitas sumber

Administrator IAM dapat mengonfigurasi AWS Security Token Service untuk mengharuskan pengguna menentukan identitas mereka ketika mereka menggunakan kredensi sementara untuk mengambil peran. `sourceIdentity`Field terjadi dalam peristiwa ketika pengguna mengambil peran IAM atau melakukan tindakan apa pun dengan peran yang diasumsikan.

`sourceIdentity`Bidang mengidentifikasi identitas pengguna asli yang membuat permintaan, apakah identitas pengguna tersebut adalah pengguna IAM, peran IAM, pengguna yang diautentikasi dengan menggunakan federasi, atau pengguna yang diautentikasi dengan menggunakan SAML-based federasi identitas web yang sesuai dengan OpenID Connect (OIDC). Setelah administrator IAM mengonfigurasi AWS STS, CloudTrail mencatat `sourceIdentity` informasi dalam peristiwa dan lokasi berikut dalam catatan peristiwa:

- `AssumeRoleWithWebIdentity`Panggilan AWS STS `AssumeRoleAssumeRoleWithSAML`,, atau yang dibuat identitas pengguna ketika mengambil peran. `sourceIdentity`ditemukan di `requestParameters` blok AWS STS panggilan.
- `AssumeRoleWithWebIdentity`Panggilan AWS STS `AssumeRoleAssumeRoleWithSAML`,, atau yang dibuat identitas pengguna jika menggunakan peran untuk mengambil peran lain, yang dikenal sebagai rantai peran. `sourceIdentity`ditemukan di `requestParameters` blok AWS STS panggilan.

- API AWS layanan memanggil identitas pengguna yang dibuat saat mengambil peran dan menggunakan kredenal sementara yang ditetapkan oleh. AWS STS Dalam peristiwa API layanan`sourceIdentity`, ditemukan di `sessionContext` blok. Misalnya, jika identitas pengguna membuat bucket S3 baru, `sourceIdentity` terjadi di `sessionContext` blok `CreateBucket` acara.

Untuk informasi selengkapnya tentang cara mengonfigurasi AWS STS untuk mengumpulkan informasi identitas sumber, lihat Memantau dan mengontrol tindakan yang diambil dengan peran yang diasumsikan dalam Panduan Pengguna IAM. Untuk informasi selengkapnya tentang AWS STS peristiwa yang dicatat CloudTrail, lihat Pencatatan panggilan IAM dan AWS STS API AWS CloudTrail di Panduan Pengguna IAM.

Berikut ini adalah contoh cuplikan peristiwa yang menunjukkan bidang. `sourceIdentity`

`requestParameters`Bagian contoh

Dalam contoh cuplikan peristiwa berikut, pengguna membuat AWS STS `AssumeRole` permintaan, dan menetapkan identitas sumber, diwakili di sini oleh. *`source-identity-value-set`* Pengguna mengasumsikan peran yang diwakili oleh peran ARN`arn:aws:iam::123456789012:role/Assumed_Role`. `sourceIdentity`Bidang berada di `requestParameters` blok acara.

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

`responseElements`Bagian contoh

Dalam contoh cuplikan peristiwa berikut, pengguna membuat AWS STS `AssumeRole` permintaan untuk mengambil peran bernama`Developer_Role`, dan menetapkan identitas sumber,. `Admin` Pengguna mengasumsikan peran yang diwakili oleh peran ARN`arn:aws:iam::111122223333:role/Developer_Role`. `sourceIdentity`Bidang ditampilkan di `responseElements` blok `requestParameters` dan blok acara. Kredensi sementara yang digunakan untuk mengambil peran, string token sesi, dan ID peran yang diasumsikan, nama sesi, dan ARN sesi ditampilkan di `responseElements` blok, bersama dengan identitas sumber.

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

`sessionContext`Bagian contoh

Dalam contoh cuplikan peristiwa berikut, pengguna mengasumsikan peran bernama `DevRole` untuk memanggil API layanan. AWS Pengguna menetapkan identitas sumber, diwakili di sini oleh*source-identity-value-set*. `sourceIdentity`Bidang ada di `sessionContext` blok, di dalam `userIdentity` blok acara.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
```

```
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

Peristiwa non-API yang ditangkap oleh CloudTrail

Selain mencatat panggilan AWS API, CloudTrail menangkap peristiwa terkait lainnya yang mungkin memiliki dampak keamanan atau kepatuhan pada AWS akun Anda atau yang mungkin membantu Anda memecahkan masalah operasional.

- Layanan AWS peristiwa - CloudTrail mendukung pencatatan peristiwa layanan non-API. Peristiwa ini dibuat oleh AWS layanan tetapi tidak secara langsung dipicu oleh permintaan ke AWS API publik. Untuk acara-acara ini, `eventType` bidangnya adalah`AwsServiceEvent`.
- Konsol Manajemen AWS peristiwa login — CloudTrail log mencoba masuk ke Konsol Manajemen AWS, Forum AWS Diskusi, dan Pusat AWS Dukungan. Semua peristiwa masuk pengguna dan pengguna root IAM, serta semua peristiwa masuk pengguna gabungan, menghasilkan catatan masuk. CloudTrail Untuk acara masuk, `eventType` bidangnya adalah`AwsConsoleSignIn`.

Layanan AWS acara

CloudTrail mendukung pencatatan peristiwa layanan non-API. Peristiwa ini dibuat oleh AWS layanan tetapi tidak secara langsung dipicu oleh permintaan ke AWS API publik. Untuk acara-acara ini, `eventType` bidangnya adalah`AwsServiceEvent`.

Berikut ini adalah contoh skenario peristiwa AWS layanan ketika kunci yang dikelola pelanggan secara otomatis diputar di AWS Key Management Service (AWS KMS). Untuk informasi selengkapnya tentang memutar tombol KMS, lihat Memutar tombol KMS.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

Konsol Manajemen AWS acara masuk

CloudTrail log mencoba masuk ke Konsol Manajemen AWS, Forum AWS Diskusi, dan Pusat AWS Dukungan. Semua acara masuk pengguna IAM dan pengguna root, serta semua acara masuk pengguna federasi, menghasilkan catatan dalam file log. CloudTrail Untuk informasi tentang menemukan dan melihat log, lihat Menemukan file CloudTrail log Anda danMengunduh file CloudTrail log Anda.

Anda dapat menggunakannya Notifikasi Pengguna AWS untuk mengatur saluran pengiriman agar mendapatkan pemberitahuan tentang AWS CloudTrail acara. Anda akan menerima notifikasi saat ada sebuah peristiwa yang cocok dengan sebuah aturan yang Anda tentukan. Anda dapat menerima pemberitahuan untuk acara melalui beberapa saluran, termasuk email, Amazon Q Developer dalam pemberitahuan obrolan aplikasi obrolan, atau pemberitahuan AWS Console Mobile Application push. Anda juga dapat melihat notifikasi di Pusat Pem beritahuan Konsol. Notifikasi Pengguna mendukung agregasi, yang dapat mengurangi jumlah notifikasi yang Anda terima selama acara tertentu.

> **Note**
>
> Wilayah yang direkam dalam suatu `ConsoleLogin` acara bervariasi berdasarkan jenis pengguna dan apakah Anda menggunakan titik akhir global atau regional untuk masuk.
>
> - Jika Anda masuk sebagai pengguna root, CloudTrail rekam acara di salah satu Wilayah berikut: us-east-1, us-east-2, atau us-west-2.
> - Jika Anda masuk dengan pengguna IAM dan menggunakan titik akhir global, CloudTrail catat Wilayah `ConsoleLogin` acara sebagai berikut:
>   - Jika cookie alias akun ada di browser, CloudTrail catat `ConsoleLogin` acara di salah satu wilayah berikut: us-east-2, eu-north-1, atau ap-southeast-2. Ini karena proxy konsol mengalihkan pengguna berdasarkan latensi dari lokasi masuk pengguna.
>   - Jika cookie alias akun tidak ada di browser, catat `ConsoleLogin` acara CloudTrail di us-east-1. Ini karena proxy konsol mengalihkan kembali ke login global.
> - Jika Anda masuk dengan pengguna IAM dan menggunakan titik akhir Regional, catat CloudTrail `ConsoleLogin` peristiwa di Wilayah yang sesuai untuk titik akhir. Untuk informasi selengkapnya tentang AWS Sign-In titik akhir, lihat titik akhir AWS Sign-In dan kuota.

Topik

- Contoh catatan peristiwa untuk pengguna IAM
- Contoh catatan peristiwa untuk pengguna root
- Contoh catatan peristiwa untuk pengguna federasi

Contoh catatan peristiwa untuk pengguna IAM

Contoh berikut menunjukkan catatan peristiwa untuk beberapa skenario masuk pengguna IAM.

Topik

- Pengguna IAM, berhasil masuk tanpa MFA
- Pengguna IAM, berhasil masuk dengan MFA
- Pengguna IAM, tidak berhasil masuk
- Pengguna IAM, proses masuk memeriksa MFA (jenis perangkat MFA tunggal)
- Pengguna IAM, proses masuk memeriksa MFA (beberapa jenis perangkat MFA)

Pengguna IAM, berhasil masuk tanpa MFA

Catatan berikut menunjukkan bahwa pengguna bernama `Anaya` berhasil masuk Konsol Manajemen AWS tanpa menggunakan otentikasi multi-faktor (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
```

```
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Pengguna IAM, berhasil masuk dengan MFA

Catatan berikut menunjukkan bahwa pengguna IAM bernama Anaya berhasil masuk ke Konsol Manajemen AWS menggunakan otentikasi multi-faktor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
```

```
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Pengguna IAM, tidak berhasil masuk

Catatan berikut menunjukkan upaya masuk yang gagal dari pengguna IAM bernama. `Paulo`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
```

```
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Pengguna IAM, proses masuk memeriksa MFA (jenis perangkat MFA tunggal)

Berikut ini menunjukkan bahwa proses penandatanganan memeriksa apakah otentikasi multi-faktor (MFA) diperlukan untuk pengguna IAM saat masuk. Dalam contoh ini, nil `mfaType` ainya adalah`U2F MFA`, yang menunjukkan bahwa pengguna IAM mengaktifkan perangkat MFA tunggal atau beberapa perangkat MFA dari jenis yang sama (). `U2F MFA`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Pengguna IAM, proses masuk memeriksa MFA (beberapa jenis perangkat MFA)

Berikut ini menunjukkan bahwa proses penandatanganan memeriksa apakah otentikasi multi-faktor (MFA) diperlukan untuk pengguna IAM saat masuk. Dalam contoh ini, nil `mfaType` ainya adalah`Multiple MFA Devices`, yang menunjukkan bahwa pengguna IAM mengaktifkan beberapa jenis perangkat MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Mary"
    },
    "eventTime": "2023-07-19T23:10:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Multiple MFA Devices"
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


Contoh catatan peristiwa untuk pengguna root

Contoh berikut menunjukkan catatan peristiwa untuk beberapa skenario masuk `root` pengguna. Saat Anda masuk menggunakan pengguna root, CloudTrail catat `ConsoleLogin` acara di salah satu Wilayah berikut: us-east-1, us-east-2, atau us-west-2.

Topik

- Pengguna root, berhasil masuk tanpa MFA
- Pengguna root, berhasil masuk dengan MFA
- Pengguna root, tidak berhasil masuk
- Pengguna root, MFA berubah
- Pengguna root, kata sandi diubah

Pengguna root, berhasil masuk tanpa MFA

Berikut ini menunjukkan acara masuk yang berhasil untuk pengguna root yang tidak menggunakan otentikasi multi-faktor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Pengguna root, berhasil masuk dengan MFA

Berikut ini menunjukkan acara masuk yang berhasil untuk pengguna root menggunakan otentikasi multi-faktor (MFA).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
```

```
}
```

Pengguna root, tidak berhasil masuk

Berikut ini menunjukkan peristiwa masuk yang gagal untuk pengguna root yang tidak menggunakan MFA.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Pengguna root, MFA berubah

Berikut ini menunjukkan contoh peristiwa untuk pengguna root yang mengubah pengaturan otentikasi multi-faktor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

Pengguna root, kata sandi diubah

Berikut ini menunjukkan contoh peristiwa untuk pengguna root yang mengubah kata sandi mereka.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
```

```
}
```

Contoh catatan peristiwa untuk pengguna federasi

Contoh berikut menunjukkan catatan peristiwa untuk pengguna federasi. Pengguna federasi diberikan kredentif keamanan sementara untuk mengakses AWS sumber daya melalui `AssumeRole` permintaan.

Berikut ini menunjukkan contoh peristiwa untuk permintaan enkripsi federasi. ID kunci akses asli disediakan di `accessKeyId` bidang `userIdentity` elemen. Bid `accessKeyId` ang di dalam `responseElements` berisi ID kunci akses baru jika diminta `sessionDuration` diteruskan dalam permintaan enkripsi, jika tidak, itu berisi nilai ID kunci akses asli.

> **Note**
>
> Dalam contoh ini, `mfaAuthenticated` nilainya adalah `false` dan `MFAUsed` nil No ainya karena permintaan dibuat oleh pengguna federasi. Bidang-bidang ini hanya akan disetel ke true jika permintaan dibuat oleh pengguna IAM atau pengguna root menggunakan MFA.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Berikut ini menunjukkan acara masuk yang berhasil untuk pengguna federasi; tidak menggunakan otentikasi multi-faktor (MFA).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

Bekerja dengan file CloudTrail log

Anda dapat melakukan tugas yang lebih maju dengan CloudTrail file Anda.

- Pantau file CloudTrail log dengan mengirimkannya ke CloudWatch Log.
- Bagikan file log antar akun.
- Gunakan Perpustakaan AWS CloudTrail Pemrosesan untuk menulis aplikasi pemrosesan log di Java.
- Validasi file log Anda untuk memverifikasi bahwa mereka tidak berubah setelah pengiriman oleh CloudTrail.

Ketika suatu peristiwa terjadi di akun Anda, CloudTrail evaluasi apakah acara tersebut cocok dengan pengaturan untuk jejak Anda. Hanya peristiwa yang cocok dengan setelan jejak yang dikirimkan ke bucket Amazon S3 dan grup CloudWatch log Amazon Logs.

Anda dapat mengonfigurasi beberapa jejak secara berbeda sehingga jejak memproses dan hanya mencatat peristiwa yang Anda tentukan. Misalnya, satu jejak dapat mencatat data hanya-baca dan peristiwa manajemen, sehingga semua peristiwa hanya-baca dikirim ke satu bucket S3. Jejak lain hanya dapat mencatat data khusus tulis dan peristiwa manajemen, sehingga semua peristiwa khusus tulis dikirim ke bucket S3 terpisah.

Anda juga dapat mengonfigurasi jejak Anda untuk memiliki satu log jejak dan mengirimkan semua peristiwa manajemen ke satu bucket S3, dan mengonfigurasi jejak lain untuk mencatat dan mengirimkan semua peristiwa data ke bucket S3 lainnya.

Anda dapat mengonfigurasi jejak Anda untuk mencatat hal-hal berikut:

- Peristiwa data: Peristiwa ini memberikan visibilitas ke dalam operasi sumber daya yang dilakukan pada atau di dalam sumber daya. Ini juga dikenal sebagai operasi bidang data.
- Acara manajemen: Acara manajemen memberikan visibilitas ke dalam operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi bidang kontrol. Peristiwa manajemen juga dapat mencakup peristiwa non-API yang terjadi di akun Anda. Misalnya, ketika pengguna masuk ke akun Anda, CloudTrail mencatat `ConsoleLogin` peristiwa tersebut. Untuk informasi selengkapnya, lihat Peristiwa non-API yang ditangkap oleh CloudTrail.
- Peristiwa aktivitas CloudTrail jaringan: peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC

pribadi ke. Layanan AWS Peristiwa aktivitas jaringan memberikan visibilitas ke dalam operasi sumber daya yang dilakukan dalam VPC.

- Insights events: Insights event menangkap aktivitas tidak biasa yang terdeteksi di akun Anda. Jika peristiwa Insights diaktifkan, dan CloudTrail mendeteksi aktivitas yang tidak biasa, peristiwa Insights akan dicatat ke bucket S3 tujuan untuk jejak Anda, tetapi di folder yang berbeda. Anda juga dapat melihat jenis peristiwa Wawasan dan periode waktu kejadian saat Anda melihat peristiwa Wawasan di CloudTrail konsol. Tidak seperti jenis peristiwa lain yang ditangkap dalam CloudTrail jejak, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda yang berbeda secara signifikan dari pola penggunaan biasa akun.

  Insights event dihasilkan hanya untuk manajemen APIs. Untuk informasi selengkapnya, lihat Bekerja dengan CloudTrail Wawasan.

> **Note**
>
> CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian Tingkat AWS CloudTrail Layanan untuk informasi lebih lanjut.
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan attempted-to-deliver peristiwa ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Topik

- Menerima file CloudTrail log dari beberapa Wilayah
- Mengelola konsistensi data di CloudTrail
- Memantau File CloudTrail Log dengan CloudWatch Log Amazon
- Menerima file CloudTrail log dari beberapa akun
- Berbagi file CloudTrail log antar AWS akun
- Memvalidasi CloudTrail integritas file log
- CloudTrail contoh file log
- Menggunakan Pustaka CloudTrail Pemrosesan

Menerima file CloudTrail log dari beberapa Wilayah

Saat Anda membuat jejak Multi-wilayah, CloudTrail mencatat peristiwa dari semua Wilayah yang diaktifkan di akun Anda. CloudTrail mengirimkan file log ke bucket S3 dan grup CloudWatch log Log yang sama. Selama CloudTrail memiliki izin untuk menulis ke ember S3, ember untuk jejak Multi-wilayah tidak harus berada di Wilayah asal jejak.

Meskipun sebagian besar Wilayah AWS diaktifkan secara default untuk Anda Akun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual (juga disebut sebagai Wilayah keikutsertaan). Untuk informasi tentang Wilayah mana yang diaktifkan secara default, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi.AWS Account Management Untuk daftar CloudTrail dukungan Wilayah, lihatCloudTrail Daerah yang didukung.

Setelah Anda mengaktifkan Wilayah keikutsertaan, CloudTrail buat salinan identik dari setiap jejak Multi-wilayah di Wilayah keikutsertaan yang Anda aktifkan. Untuk informasi selengkapnya, lihat Apa yang terjadi jika Anda mengaktifkan Region keikutsertaan?.

Jika nanti Anda menonaktifkan Wilayah keikutsertaan, salinan jejak Multi-wilayah di Wilayah tersebut akan tetap ada. Karena akun Anda mungkin memiliki aktivitas di Wilayah yang Anda nonaktifkan, seperti tindakan Layanan AWS untuk menghapus sumber daya, CloudTrail akan terus menangkap aktivitas dan mencoba mengirimkan peristiwa ke bucket S3 untuk setiap jejak yang tidak dihapus sebelum Wilayah dinonaktifkan.

Untuk mengonversi jejak wilayah Tunggal yang ada menjadi jejak Multi-wilayah, Anda harus menggunakan. AWS CLI

Untuk mengubah jejak yang ada sehingga berlaku untuk semua Wilayah yang diaktifkan, tambahkan `--is-multi-region-trail` opsi ke update-trailperintah.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak sekarang merupakan jejak Multi-wilayah, verifikasi bahwa `IsMultiRegionTrail` elemen dalam output ditampilkan`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
```

```
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Untuk informasi selengkapnya, lihat sumber daya berikut:

- Memahami jalur Multi-wilayah dan Wilayah keikutsertaan
- Membuat jejak untuk Anda Akun AWS
- CloudTrail FAQs

Mengelola konsistensi data di CloudTrail

CloudTrail menggunakan model komputasi terdistribusi yang disebut konsistensi akhirnya. Setiap perubahan yang Anda buat pada CloudTrail konfigurasi Anda (atau AWS layanan lainnya), termasuk tag yang digunakan dalam kontrol akses berbasis atribut (ABAC), membutuhkan waktu untuk terlihat dari semua titik akhir yang mungkin. Beberapa keterlambatan hasil dari waktu yang diperlukan untuk mengirim data dari server ke server, dan dari Wilayah ke Wilayah di seluruh dunia. CloudTrail juga menggunakan caching untuk meningkatkan kinerja, tetapi dalam beberapa kasus ini dapat menambah waktu. Perubahan mungkin tidak terlihat sampai waktu data yang disimpan di-cache sebelumnya habis.

Anda harus merancang aplikasi Anda untuk memperhitungkan potensi penundaan ini. Pastikan aplikasi bekerja sesuai harapan, bahkan ketika perubahan yang dilakukan di satu lokasi tidak secara langsung terlihat di lokasi lain. Perubahan tersebut termasuk mengaktifkan Wilayah keikutsertaan, membuat atau memperbarui jejak atau penyimpanan data peristiwa, memperbarui pemilih acara, dan memulai atau menghentikan pencatatan. Saat Anda membuat atau memperbarui penyimpanan data jejak atau peristiwa, CloudTrail mengirimkan log ke bucket S3 atau penyimpanan data peristiwa berdasarkan konfigurasi terakhir yang diketahui hingga perubahan menyebar ke semua lokasi.

Untuk informasi selengkapnya tentang bagaimana hal ini memengaruhi orang lain Layanan AWS, lihat sumber daya berikut:

- Amazon DynamoDB: Apa model konsistensi DynamoDB? di FAQ DynamoDB, dan Baca konsistensi di Panduan Pengembang Amazon DynamoDB.
- Amazon EC2: Konsistensi akhirnya dalam Referensi API Amazon Elastic Compute Cloud.

- Amazon EMR: Memastikan Konsistensi Saat Menggunakan Amazon S3 dan MapReduce Amazon Elastic untuk Alur Kerja AWS ETL di Blog Big Data.
- AWS Identity and Access Management (IAM): Perubahan yang saya buat tidak selalu langsung terlihat di Panduan Pengguna IAM.
- Amazon Redshift: Mengelola konsistensi data dalam Panduan Pengembang Database Amazon Redshift.
- Amazon S3: Model konsistensi data Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Memantau File CloudTrail Log dengan CloudWatch Log Amazon

Anda dapat menggunakan Amazon CloudWatch Logs untuk memantau, menyimpan, dan mengakses file log Anda CloudTrail.

CloudWatch Log memungkinkan Anda untuk memusatkan log dari semua sistem, aplikasi, dan Layanan AWS yang Anda gunakan, dalam satu layanan yang sangat skalabel. Anda kemudian dapat dengan mudah melihatnya, mencari kode atau pola kesalahan tertentu, memfilternya berdasarkan bidang tertentu, atau mengarsipkannya dengan aman untuk analisis masa depan. CloudWatch Log memungkinkan Anda untuk melihat semua log Anda, terlepas dari sumbernya, sebagai aliran peristiwa tunggal dan konsisten yang diurutkan berdasarkan waktu.

Selesaikan langkah-langkah berikut untuk mengonfigurasi CloudTrail dengan CloudWatch Log untuk memantau log jejak Anda dan diberi tahu saat aktivitas tertentu terjadi.

1. Konfigurasikan jejak Anda untuk mengirim peristiwa log ke CloudWatch Log.
2. Tentukan filter metrik CloudWatch Log untuk mengevaluasi peristiwa log untuk kecocokan dalam istilah, frasa, atau nilai. Misalnya, Anda dapat memantau `ConsoleLogin` acara.
3. Tetapkan CloudWatch metrik ke filter metrik.
4. Buat CloudWatch alarm yang dipicu sesuai dengan ambang batas dan periode waktu yang Anda tentukan. Anda dapat mengonfigurasi alarm untuk mengirim notifikasi saat alarm dipicu, sehingga Anda dapat mengambil tindakan.
5. Anda juga dapat mengonfigurasi CloudWatch untuk secara otomatis melakukan tindakan sebagai respons terhadap alarm.

Harga standar untuk Amazon CloudWatch dan Amazon CloudWatch Log berlaku. Untuk informasi selengkapnya, lihat CloudWatch Harga Amazon.

Untuk informasi selengkapnya tentang Wilayah tempat Anda dapat mengonfigurasi jejak untuk mengirim CloudWatch log ke Log, lihat Wilayah dan Kuota CloudWatch Log Amazon di Referensi AWS Umum.

Topik

- Mengirim acara ke CloudWatch Log
- Membuat CloudWatch alarm untuk CloudTrail acara: contoh
- Berhenti CloudTrail dari mengirim acara ke CloudWatch Log
- CloudWatch grup log dan penamaan aliran log untuk CloudTrail
- Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan

Mengirim acara ke CloudWatch Log

Saat Anda mengonfigurasi jejak Anda untuk mengirim peristiwa ke CloudWatch Log, CloudTrail kirimkan hanya peristiwa yang sesuai dengan pengaturan jejak Anda. Misalnya, jika Anda mengonfigurasi jejak Anda untuk mencatat peristiwa data saja, jejak Anda akan mengirimkan peristiwa data hanya ke grup CloudWatch log Log Anda. CloudTrail mendukung pengiriman data, Wawasan, dan acara manajemen ke CloudWatch Log. Untuk informasi selengkapnya, lihat Bekerja dengan file CloudTrail log.

> **Note**
>
> Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi menggunakan konsol. Administrator yang didelegasikan dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API.

Untuk mengirim peristiwa ke grup CloudWatch log Log:

- Pastikan Anda memiliki izin yang cukup untuk membuat atau menentukan peran IAM. Untuk informasi selengkapnya, lihat Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol.
- Jika Anda mengonfigurasi grup CloudWatch log Log menggunakan AWS CLI, pastikan Anda memiliki izin yang cukup untuk membuat aliran CloudWatch log Log di grup log yang Anda

tentukan dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut. Untuk informasi selengkapnya, lihat Membuat dokumen kebijakan.

- Buat jejak baru atau tentukan yang sudah ada. Untuk informasi selengkapnya, lihat Membuat dan memperbarui jejak dengan konsol.
- Buat grup log atau tentukan yang sudah ada.
- Tentukan peran IAM. Jika Anda memodifikasi peran IAM yang ada untuk jejak organisasi, Anda harus memperbarui kebijakan secara manual untuk mengizinkan pencatatan jejak organisasi. Untuk informasi selengkapnya, lihat contoh kebijakan ini danMembuat jejak untuk sebuah organisasi.
- Lampirkan kebijakan peran atau gunakan default.

Daftar Isi

- Mengkonfigurasi pemantauan CloudWatch Log dengan konsol
  - Membuat grup log atau menentukan grup log yang ada
  - Menentukan peran IAM
  - Melihat acara di CloudWatch konsol
- Mengkonfigurasi pemantauan CloudWatch Log dengan AWS CLI
  - Membuat grup log
  - Membuat peran
  - Membuat dokumen kebijakan
  - Memperbarui jejak
- Batasan

Mengkonfigurasi pemantauan CloudWatch Log dengan konsol

Anda dapat menggunakan Konsol Manajemen AWS untuk mengonfigurasi jejak Anda untuk mengirim peristiwa ke CloudWatch Log untuk pemantauan.

Membuat grup log atau menentukan grup log yang ada

CloudTrail menggunakan grup CloudWatch log Log sebagai titik akhir pengiriman untuk peristiwa log. Anda dapat membuat grup log atau menentukan grup yang sudah ada.

Untuk membuat atau menentukan grup log untuk jejak yang ada

1. Pastikan Anda masuk dengan pengguna administratif atau peran dengan izin yang cukup untuk mengonfigurasi integrasi CloudWatch Log. Untuk informasi selengkapnya, lihat Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol.

   > **Note**
   >
   > Hanya akun manajemen yang dapat mengonfigurasi grup CloudWatch log Log untuk jejak organisasi menggunakan konsol. Administrator yang didelegasikan dapat mengonfigurasi grup CloudWatch log Log menggunakan operasi AWS CLI atau CloudTrail `CreateTrail` atau `UpdateTrail` API.

2. Buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
3. Pilih nama jejak. Jika Anda memilih jalur Multi-wilayah, Anda akan diarahkan ke Wilayah tempat jejak itu dibuat. Anda dapat membuat grup log atau memilih grup log yang ada di Wilayah yang sama dengan jejak.

   > **Note**
   >
   > Jejak Multi-wilayah mengirimkan file log dari semua Wilayah yang diaktifkan di grup CloudWatch log Log yang Anda tentukan. Akun AWS

4. Di CloudWatch Log, pilih Edit.
5. Untuk CloudWatch Log, pilih Diaktifkan.
6. Untuk nama grup Log, pilih Baru untuk membuat grup log baru, atau Ada untuk menggunakan yang sudah ada. Jika Anda memilih Baru, CloudTrail menentukan nama untuk grup log baru untuk Anda, atau Anda dapat mengetikkan nama. Untuk informasi lebih lanjut tentang penamaan, lihatCloudWatch grup log dan penamaan aliran log untuk CloudTrail.
7. Jika Anda memilih yang ada, pilih grup log dari daftar drop-down.
8. Untuk nama Peran, pilih Baru untuk membuat peran IAM baru untuk izin mengirim log ke CloudWatch Log. Pilih Existing untuk memilih peran IAM yang ada dari daftar drop-down. Pernyataan kebijakan untuk peran baru atau yang sudah ada ditampilkan saat Anda memperluas dokumen Kebijakan. Untuk informasi selengkapnya tentang peran ini, silakan lihat Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

> **Note**
>
> Saat mengonfigurasi jejak, Anda dapat memilih bucket S3 dan topik SNS milik akun lain. Namun, jika Anda CloudTrail ingin mengirimkan peristiwa ke grup CloudWatch log Log, Anda harus memilih grup log yang ada di akun Anda saat ini.

9. Pilih Simpan perubahan.

Menentukan peran IAM

Anda dapat menentukan peran CloudTrail untuk diasumsikan untuk mengirimkan peristiwa ke aliran log.

Untuk menentukan peran

1. Secara default, `CloudTrail_CloudWatchLogs_Role` ditentukan untuk Anda. Kebijakan peran default memiliki izin yang diperlukan untuk membuat aliran CloudWatch log Log di grup log yang Anda tentukan, dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut.

   > **Note**
   >
   > Jika Anda ingin menggunakan peran ini untuk grup log untuk jejak organisasi, Anda harus mengubah kebijakan secara manual setelah membuat peran. Untuk informasi selengkapnya, lihat contoh kebijakan ini danMembuat jejak untuk sebuah organisasi.

   a. Untuk memverifikasi peran, buka AWS Identity and Access Management konsol di https://console.aws.amazon.com/iam/.
   b. Pilih Peran dan kemudian pilih CloudTrail_ CloudWatchLogs _Role.
   c. Dari tab Izin, perluas kebijakan untuk melihat kontennya.
2. Anda dapat menentukan peran lain, tetapi Anda harus melampirkan kebijakan peran yang diperlukan ke peran yang ada jika Anda ingin menggunakannya untuk mengirim peristiwa ke CloudWatch Log. Untuk informasi selengkapnya, lihat Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan.

Melihat acara di CloudWatch konsol

Setelah mengonfigurasi jejak untuk mengirim peristiwa ke grup CloudWatch log Log, Anda dapat melihat peristiwa di CloudWatch konsol. CloudTrail biasanya mengirimkan peristiwa ke grup log Anda dalam waktu rata-rata sekitar 5 menit setelah panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian Tingkat AWS CloudTrail Layanan untuk informasi lebih lanjut.

Untuk melihat peristiwa di CloudWatch konsol

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi kiri, di bawah Log, pilih Grup log.
3. Pilih grup log yang Anda tentukan untuk jejak Anda.
4. Pilih aliran log yang ingin Anda lihat.
5. Untuk melihat detail peristiwa yang dicatat jejak Anda, pilih acara.

> **Note**
>
> Kolom Waktu (UTC) di CloudWatch konsol menunjukkan kapan acara dikirim ke grup log Anda. Untuk melihat waktu aktual peristiwa itu dicatat CloudTrail, lihat `eventTime` bidangnya.

Mengkonfigurasi pemantauan CloudWatch Log dengan AWS CLI

Anda dapat menggunakan AWS CLI untuk mengkonfigurasi CloudTrail untuk mengirim peristiwa ke CloudWatch Log untuk pemantauan.

Membuat grup log

1. Jika Anda tidak memiliki grup log yang ada, buat grup CloudWatch log Log sebagai titik akhir pengiriman untuk peristiwa log menggunakan `create-log-group` perintah CloudWatch Log.

   ```
   aws logs create-log-group --log-group-name name
   ```

   Contoh berikut membuat grup log bernama`CloudTrail/logs`:

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. Ambil grup log Amazon Resource Name (ARN).

```
aws logs describe-log-groups
```

Membuat peran

Buat peran CloudTrail yang memungkinkannya mengirim peristiwa ke grup CloudWatch log Log. `create-role`Perintah IAM mengambil dua parameter: nama peran dan jalur file ke dokumen kebijakan peran asumsi dalam format JSON. Dokumen kebijakan yang Anda gunakan memberikan `AssumeRole` izin untuk CloudTrail. `create-role`Perintah membuat peran dengan izin yang diperlukan.

Untuk membuat file JSON yang akan berisi dokumen kebijakan, buka editor teks dan simpan konten kebijakan berikut dalam file bernama`assume_role_policy_document.json`.

JSON

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

Jalankan perintah berikut untuk membuat peran dengan `AssumeRole` izin untuk CloudTrail.

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

Ketika perintah selesai, catat peran ARN dalam output.

Membuat dokumen kebijakan

Buat dokumen kebijakan peran berikut untuk CloudTrail. Dokumen ini memberikan izin CloudTrail yang diperlukan untuk membuat aliran CloudWatch log Log di grup log yang Anda tentukan dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        }
    ]
}
```

Simpan dokumen kebijakan dalam file bernama`role-policy-document.json`.

Jika Anda membuat kebijakan yang mungkin digunakan untuk jejak organisasi juga, Anda perlu mengonfigurasinya sedikit berbeda. Misalnya, kebijakan berikut memberikan CloudTrail izin yang diperlukan untuk membuat aliran log Log di grup CloudWatch log yang Anda tentukan dan

untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut untuk kedua jejak di AWS akun 11111111111111 dan untuk jejak organisasi yang dibuat di akun 11111111111111 yang diterapkan ke organisasi dengan ID: AWS Organizations *o-exampleorgid*

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-aa111bb222_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-aa111bb222_*"
            ]
        }
    ]
}
```

Untuk informasi selengkapnya tentang jalur organisasi, lihatMembuat jejak untuk sebuah organisasi.

Jalankan perintah berikut untuk menerapkan kebijakan ke peran.

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

Memperbarui jejak

Perbarui jejak dengan grup log dan informasi peran menggunakan CloudTrail `update-trail` perintah.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

Untuk informasi selengkapnya tentang AWS CLI perintah, lihat Referensi Baris AWS CloudTrail Perintah.

Batasan

CloudWatch Log dan EventBridge masing-masing memungkinkan ukuran acara maksimum 256 KB. Meskipun sebagian besar acara layanan memiliki ukuran maksimum 256 KB, beberapa layanan masih memiliki acara yang lebih besar. CloudTrail tidak mengirim acara ini ke CloudWatch Log atau EventBridge.

Dimulai dengan CloudTrail acara versi 1.05, acara memiliki ukuran maksimum 256 KB. Ini untuk membantu mencegah eksploitasi oleh pelaku jahat, dan memungkinkan acara dikonsumsi oleh AWS layanan lain, seperti CloudWatch Log dan EventBridge.

Membuat CloudWatch alarm untuk CloudTrail acara: contoh

Topik ini menjelaskan cara mengonfigurasi alarm untuk CloudTrail acara, dan menyertakan contoh.

Topik

- Prasyarat
- Buat filter metrik dan buat alarm
- Contoh perubahan konfigurasi grup keamanan
- Contoh Konsol Manajemen AWS kegagalan masuk
- Contoh: Perubahan kebijakan IAM
- Mengkonfigurasi notifikasi untuk alarm CloudWatch Log

Prasyarat

Sebelum Anda dapat menggunakan contoh dalam topik ini, Anda harus:

- Buat jejak dengan konsol atau CLI.
- Buat grup log, yang dapat Anda lakukan sebagai bagian dari membuat jejak. Untuk informasi selengkapnya tentang membuat jejak, lihatMembuat jejak dengan CloudTrail konsol.
- Tentukan atau buat peran IAM yang memberikan CloudTrail izin untuk membuat aliran CloudWatch log Log di grup log yang Anda tentukan dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut. Default `CloudTrail_CloudWatchLogs_Role` melakukan ini untuk Anda.

Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log. Contoh di bagian ini dilakukan di konsol Amazon CloudWatch Logs. Untuk informasi selengkapnya tentang cara membuat filter metrik dan alarm, lihat Membuat metrik dari peristiwa log menggunakan filter dan Menggunakan CloudWatch alarm Amazon di Panduan Pengguna Amazon CloudWatch .

Buat filter metrik dan buat alarm

Untuk membuat alarm, Anda harus terlebih dahulu membuat filter metrik, dan kemudian mengkonfigurasi alarm berdasarkan filter. Prosedur ditampilkan untuk semua contoh. Untuk informasi selengkapnya tentang sintaks untuk filter metrik dan pola untuk peristiwa CloudTrail log, lihat bagian terkait JSON dari Filter dan sintaks pola di Panduan Pengguna Amazon CloudWatch Logs.

Contoh perubahan konfigurasi grup keamanan

Ikuti prosedur ini untuk membuat CloudWatch alarm Amazon yang dipicu saat perubahan konfigurasi terjadi pada grup keamanan.

Buat filter metrik

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Log, pilih Grup log.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. Dari menu Filter metrik atau Tindakan, pilih Buat filter metrik.
5. Pada halaman Tentukan pola, di Buat pola filter, masukkan yang berikut untuk pola Filter.

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
```

```
($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
|| ($.eventName = DeleteSecurityGroup) }
```

6. Dalam pola Uji, biarkan default. Pilih Berikutnya.
7. Pada halaman Tetapkan metrik, untuk nama Filter, masukkan**SecurityGroupEvents**.
8. Di Detail metrik, aktifkan Buat baru, lalu masukkan **CloudTrailMetrics** untuk namespace Metrik.
9. Untuk nama Metrik, ketik**SecurityGroupEventCount**.
10. Untuk nilai Metrik, ketik**1**.
11. Biarkan nilai Default kosong.
12. Pilih Berikutnya.
13. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Buat filter metrik untuk membuat filter, atau pilih Edit untuk kembali dan mengubah nilai.

Membuat alarm

Setelah Anda membuat filter metrik, halaman detail grup CloudWatch log log log untuk grup log CloudTrail jejak Anda akan terbuka. Ikuti prosedur ini untuk membuat alarm.

1. Pada tab Filter metrik, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. Di bilah Filter metrik, pilih Buat alarm.
2. Untuk Tentukan metrik dan kondisi, masukkan yang berikut ini.
   a. Untuk Grafik, garis diatur **1** berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. Untuk nama Metrik, pertahankan nama metrik saat ini,**SecurityGroupEventCount**.
   c. Untuk Statistik, pertahankan defaultnya,**Sum**.
   d. Untuk Periode, pertahankan default,**5 minutes**.
   e. Dalam Kondisi, untuk tipe Threshold, pilih Static.
   f. Untuk Kapan pun ***metric_name*** ada, pilih Greater/Equal.
   g. Untuk nilai ambang batas, masukkan**1**.
   h. Dalam konfigurasi tambahan, biarkan default. Pilih Berikutnya.
3. Pada halaman Konfigurasi tindakan, pilih Pemberitahuan, lalu pilih Dalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang batas 1 peristiwa perubahan dalam 5 menit dilintasi, dan SecurityGroupEventCountdalam keadaan alarm.

a. Untuk Mengirim pemberitahuan ke topik SNS berikut, pilih Buat topik baru.
b. Masukkan **`SecurityGroupChanges_CloudWatch_Alarms_Topic`** sebagai nama untuk topik Amazon SNS baru.
c. Di titik akhir Email yang akan menerima notifikasi, masukkan alamat email pengguna yang ingin Anda terima notifikasi jika alarm ini dinyalakan. Pisahkan alamat email dengan koma.

   Setiap penerima email akan menerima email yang meminta mereka untuk mengonfirmasi bahwa mereka ingin berlangganan topik Amazon SNS.
d. Pilih Buat topik.

4. Untuk contoh ini, lewati jenis tindakan lainnya. Pilih Berikutnya.
5. Pada halaman Tambahkan nama dan deskripsi, masukkan nama ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan **`Security group configuration changes`** nama, dan **`Raises alarms if security group configuration changes occur`** untuk deskripsi. Pilih Berikutnya.
6. Pada halaman Pratinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan, atau pilih Buat alarm untuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch buka halaman Alarm. Kolom Tindakan alarm menunjukkan konfirmasi Tertunda hingga semua penerima email pada topik SNS telah mengonfirmasi bahwa mereka ingin berlangganan notifikasi SNS.

Contoh Konsol Manajemen AWS kegagalan masuk

Ikuti prosedur ini untuk membuat CloudWatch alarm Amazon yang dipicu ketika ada tiga atau lebih kegagalan Konsol Manajemen AWS masuk selama periode lima menit.

Buat filter metrik

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Log, pilih Grup log.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. Dari menu Filter metrik atau Tindakan, pilih Buat filter metrik.
5. Pada halaman Tentukan pola, di Buat pola filter, masukkan yang berikut untuk pola Filter.

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. Dalam pola Uji, biarkan default. Pilih Berikutnya.
7. Pada halaman Tetapkan metrik, untuk nama Filter, masukkan**`ConsoleSignInFailures`**.
8. Di Detail metrik, aktifkan Buat baru, lalu masukkan **`CloudTrailMetrics`** untuk namespace Metrik.
9. Untuk nama Metrik, ketik**`ConsoleSigninFailureCount`**.
10. Untuk nilai Metrik, ketik**`1`**.
11. Biarkan nilai Default kosong.
12. Pilih Berikutnya.
13. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Buat filter metrik untuk membuat filter, atau pilih Edit untuk kembali dan mengubah nilai.

Membuat alarm

Setelah Anda membuat filter metrik, halaman detail grup CloudWatch log log log untuk grup log CloudTrail jejak Anda akan terbuka. Ikuti prosedur ini untuk membuat alarm.

1. Pada tab Filter metrik, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. Di bilah Filter metrik, pilih Buat alarm.
2. Pada halaman Buat Alarm, di Tentukan metrik dan kondisi, masukkan yang berikut ini.
   a. Untuk Grafik, garis diatur **`3`** berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. Untuk nama Metrik, pertahankan nama metrik saat ini,**`ConsoleSigninFailureCount`**.
   c. Untuk Statistik, pertahankan defaultnya,**`Sum`**.
   d. Untuk Periode, pertahankan default,**`5 minutes`**.
   e. Dalam Kondisi, untuk tipe Threshold, pilih Static.
   f. Untuk Kapan pun ***`metric_name`*** ada, pilih Greater/Equal.
   g. Untuk nilai ambang batas, masukkan**`3`**.
   h. Dalam konfigurasi tambahan, biarkan default. Pilih Berikutnya.
3. Pada halaman Konfigurasi tindakan, untuk Pemberitahuan, pilih Dalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang batas 3 peristiwa perubahan dalam 5 menit dilintasi, dan ConsoleSigninFailureCountdalam keadaan alarm.
   a. Untuk Mengirim pemberitahuan ke topik SNS berikut, pilih Buat topik baru.

b. Masukkan **`ConsoleSignInFailures_CloudWatch_Alarms_Topic`** sebagai nama untuk topik Amazon SNS baru.

c. Di titik akhir Email yang akan menerima notifikasi, masukkan alamat email pengguna yang ingin Anda terima notifikasi jika alarm ini dinyalakan. Pisahkan alamat email dengan koma.

   Setiap penerima email akan menerima email yang meminta mereka untuk mengonfirmasi bahwa mereka ingin berlangganan topik Amazon SNS.

d. Pilih Buat topik.

4. Untuk contoh ini, lewati jenis tindakan lainnya. Pilih Berikutnya.
5. Pada halaman Tambahkan nama dan deskripsi, masukkan nama ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan **`Console sign-in failures`** nama, dan **`Raises alarms if more than 3 console sign-in failures occur in 5 minutes`** untuk deskripsi. Pilih Berikutnya.
6. Pada halaman Pratinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan, atau pilih Buat alarm untuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch buka halaman Alarm. Kolom Tindakan alarm menunjukkan konfirmasi Tertunda hingga semua penerima email pada topik SNS telah mengonfirmasi bahwa mereka ingin berlangganan notifikasi SNS.

Contoh: Perubahan kebijakan IAM

Ikuti prosedur ini untuk membuat CloudWatch alarm Amazon yang dipicu saat panggilan API dilakukan untuk mengubah kebijakan IAM.

Buat filter metrik

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pilih Log di panel navigasi.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. Pilih Tindakan, lalu pilih Buat filter metrik.
5. Pada halaman Tentukan pola, di Buat pola filter, masukkan yang berikut untuk pola Filter.

```
{($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
```

```
($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
```

6. Dalam pola Uji, biarkan default. Pilih Berikutnya.
7. Pada halaman Tetapkan metrik, untuk nama Filter, masukkan**IAMPolicyChanges**.
8. Di Detail metrik, aktifkan Buat baru, lalu masukkan **CloudTrailMetrics** untuk namespace Metrik.
9. Untuk nama Metrik, ketik**IAMPolicyEventCount**.
10. Untuk nilai Metrik, ketik**1**.
11. Biarkan nilai Default kosong.
12. Pilih Berikutnya.
13. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Buat filter metrik untuk membuat filter, atau pilih Edit untuk kembali dan mengubah nilai.

Membuat alarm

Setelah Anda membuat filter metrik, halaman detail grup CloudWatch log log log untuk grup log CloudTrail jejak Anda akan terbuka. Ikuti prosedur ini untuk membuat alarm.

1. Pada tab Filter metrik, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. Di bilah Filter metrik, pilih Buat alarm.
2. Pada halaman Buat Alarm, di Tentukan metrik dan kondisi, masukkan yang berikut ini.
   a. Untuk Grafik, garis diatur **1** berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. Untuk nama Metrik, pertahankan nama metrik saat ini,**IAMPolicyEventCount**.
   c. Untuk Statistik, pertahankan defaultnya,**Sum**.
   d. Untuk Periode, pertahankan default,**5 minutes**.
   e. Dalam Kondisi, untuk tipe Threshold, pilih Static.
   f. Untuk Kapan pun ***metric_name*** ada, pilih Greater/Equal.
   g. Untuk nilai ambang batas, masukkan**1**.
   h. Dalam konfigurasi tambahan, biarkan default. Pilih Berikutnya.
   i.

3. Pada halaman Konfigurasi tindakan, untuk Pemberitahuan, pilih Dalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang batas 1 peristiwa perubahan dalam 5 menit dilintasi, dan IAMPolicyEventCountdalam keadaan alarm.

   a. Untuk Mengirim pemberitahuan ke topik SNS berikut, pilih Buat topik baru.

   b. Masukkan **`IAM_Policy_Changes_CloudWatch_Alarms_Topic`** sebagai nama untuk topik Amazon SNS baru.

   c. Di titik akhir Email yang akan menerima notifikasi, masukkan alamat email pengguna yang ingin Anda terima notifikasi jika alarm ini dinyalakan. Pisahkan alamat email dengan koma.

      Setiap penerima email akan menerima email yang meminta mereka untuk mengonfirmasi bahwa mereka ingin berlangganan topik Amazon SNS.

   d. Pilih Buat topik.

4. Untuk contoh ini, lewati jenis tindakan lainnya. Pilih Berikutnya.

5. Pada halaman Tambahkan nama dan deskripsi, masukkan nama ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan **`IAM Policy Changes`** nama, dan **`Raises alarms if IAM policy changes occur`** untuk deskripsi. Pilih Berikutnya.

6. Pada halaman Pratinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan, atau pilih Buat alarm untuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch buka halaman Alarm. Kolom Tindakan alarm menunjukkan konfirmasi Tertunda hingga semua penerima email pada topik SNS telah mengonfirmasi bahwa mereka ingin berlangganan notifikasi SNS.

Mengkonfigurasi notifikasi untuk alarm CloudWatch Log

Anda dapat mengonfigurasi CloudWatch Log untuk mengirim pemberitahuan setiap kali alarm dipicu CloudTrail. Melakukannya memungkinkan Anda merespons dengan cepat peristiwa operasional penting yang ditangkap dalam CloudTrail peristiwa dan terdeteksi oleh CloudWatch Log. CloudWatch menggunakan Amazon Simple Notification Service (SNS) untuk mengirim email. Untuk informasi selengkapnya, lihat Menyiapkan notifikasi Amazon SNS di CloudWatch Panduan Pengguna.

Berhenti CloudTrail dari mengirim acara ke CloudWatch Log

Anda dapat menghentikan pengiriman AWS CloudTrail peristiwa ke Amazon CloudWatch Logs dengan memperbarui jejak untuk menonaktifkan pengaturan CloudWatch Log.

Berhenti mengirim acara ke CloudWatch Log (konsol)

Untuk berhenti mengirim CloudTrail acara ke CloudWatch Log

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Jejak.
3. Pilih nama jejak yang ingin Anda nonaktifkan integrasi CloudWatch Log.
4. Di CloudWatch Log, pilih Edit.
5. Hapus kotak centang Diaktifkan.
6. Pilih Simpan perubahan.

Berhenti mengirim acara ke CloudWatch Log (CLI)

Anda dapat menghapus grup CloudWatch log Log sebagai titik akhir pengiriman dengan menjalankan update-trailperintah. Perintah berikut menghapus grup log dan peran dari konfigurasi jejak dengan mengganti nilai untuk ARN grup log CloudWatch dan peran Log ARN dengan nilai kosong.

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch grup log dan penamaan aliran log untuk CloudTrail

Amazon CloudWatch akan menampilkan grup log yang Anda buat untuk CloudTrail acara bersama grup log lain yang Anda miliki di Wilayah. Kami menyarankan Anda menggunakan nama grup log yang membantu Anda dengan mudah membedakan grup log dari yang lain. Misalnya, **`CloudTrail/logs`**.

Ikuti panduan ini saat memberi nama grup log:

- Nama grup log harus unik di dalam Wilayah untuk Akun AWS.
- Nama grup log dapat berisi antara 1 dan 512 karakter.
- Nama grup log terdiri dari karakter berikut: a-z, A-Z, 0-9, '_' (garis bawah), '-' (tanda hubung), '/' (garis miring), '.' (periode), dan '#' (tanda angka).

Saat CloudTrail membuat aliran log untuk grup log, itu memberi nama aliran log sesuai dengan format berikut: *account_ID* _ CloudTrail _*trail_region*.

> **Note**
>
> Jika volume CloudTrail log besar, beberapa aliran log dapat dibuat untuk mengirimkan data log ke grup log Anda. Ketika ada beberapa aliran log, beri CloudTrail nama setiap aliran log sesuai dengan format berikut: *account_ID* _ _ CloudTrail *trail_region* _*number*.

Untuk informasi selengkapnya tentang grup CloudWatch log, lihat Bekerja dengan grup log dan aliran log di Panduan Pengguna Amazon CloudWatch Logs dan CreateLogGroupdi Referensi API Amazon CloudWatch Logs.

Dokumen kebijakan peran CloudTrail untuk menggunakan CloudWatch Log untuk pemantauan

Bagian ini menjelaskan kebijakan izin yang diperlukan untuk CloudTrail peran untuk mengirim peristiwa log ke CloudWatch Log. Anda dapat melampirkan dokumen kebijakan ke peran saat mengonfigurasi CloudTrail untuk mengirim peristiwa, seperti yang dijelaskan dalamMengirim acara ke CloudWatch Log. Anda juga dapat membuat peran menggunakan IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS atau Membuat peran IAM ().AWS CLI

Contoh dokumen kebijakan berikut berisi izin yang diperlukan untuk membuat aliran CloudWatch log di grup log yang Anda tentukan dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut di Wilayah AS Timur (Ohio). (Ini adalah kebijakan default untuk peran IAM default`CloudTrail_CloudWatchLogs_Role`.)

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
```

```
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333:log-
group:log_group_name:log-stream:CloudTrail_log_stream_name_prefix*"
            ]
        }
    ]
}
```

Jika Anda membuat kebijakan yang mungkin digunakan untuk jejak organisasi juga, Anda harus memodifikasinya dari kebijakan default yang dibuat untuk peran tersebut. Misalnya, kebijakan berikut memberikan CloudTrail izin yang diperlukan untuk membuat aliran log Log di grup CloudWatch log yang Anda tentukan sebagai nilainya*log_group_name*, dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut untuk kedua jejak di AWS akun 11111111111111 dan untuk jejak organisasi yang dibuat di akun 11111111111111 yang diterapkan ke organisasi dengan ID: AWS Organizations *o-exampleorgid*

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
```

```
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-
group:log_group_name:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

Untuk informasi selengkapnya tentang jalur organisasi, lihatMembuat jejak untuk sebuah organisasi.

Menerima file CloudTrail log dari beberapa akun

Anda dapat CloudTrail mengirimkan file log dari beberapa Akun AWS ke dalam satu ember Amazon S3. Misalnya, Anda memiliki empat Akun AWS dengan akun IDs 111111111111, 222222222222, 333333333333, dan 4444444444444444, dan Anda ingin mengonfigurasi untuk mengirimkan file log dari keempat akun ini ke ember milik akun 11111111111111. CloudTrail Untuk mencapai ini, selesaikan langkah-langkah berikut secara berurutan:

1. Buat jejak di akun tempat bucket tujuan berada (11111111111111 dalam contoh ini). Jangan membuat jejak untuk akun lain.

   Untuk petunjuk, lihat Membuat jejak dengan konsol.

2. Perbarui kebijakan bucket di bucket tujuan Anda untuk memberikan izin lintas akun. CloudTrail

   Untuk petunjuk, lihat Menyetel kebijakan bucket untuk beberapa akun.

3. Buat jejak di akun lain (222222222222, 333333333333, dan 44444444444444 dalam contoh ini) yang ingin Anda log aktivitas. Saat Anda membuat jejak di setiap akun, tentukan bucket Amazon S3 milik akun yang Anda tentukan di langkah 1 (111111111111 dalam contoh ini). Untuk petunjuk, lihat Buat jejak di akun tambahan.

> **Note**
>
> Jika Anda memilih untuk mengaktifkan enkripsi SSE-KMS, kebijakan kunci KMS harus mengizinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda dan mencerna file, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log atau mencerna file dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

Menyunting akun pemilik bucket IDs untuk peristiwa data yang dipanggil oleh akun lain

Secara historis, jika peristiwa CloudTrail data diaktifkan di Akun AWS pemanggil API peristiwa data Amazon S3 CloudTrail , tunjukkan ID akun pemilik bucket S3 dalam peristiwa data (seperti). `PutObject` Ini terjadi meskipun akun pemilik bucket tidak mengaktifkan peristiwa data S3.

Sekarang, CloudTrail hapus ID akun pemilik bucket S3 di `resources` blok jika kedua kondisi berikut terpenuhi:

- Panggilan API peristiwa data berbeda Akun AWS dari pemilik bucket Amazon S3.
- Pemanggil API menerima `AccessDenied` kesalahan yang hanya untuk akun penelepon.

Pemilik sumber daya tempat panggilan API dibuat masih menerima acara lengkap.

Cuplikan catatan peristiwa berikut adalah contoh perilaku yang diharapkan. Dalam `Historic` cuplikan, ID akun 123456789012 dari pemilik bucket S3 ditampilkan ke pemanggil API dari akun lain. Dalam contoh perilaku saat ini, ID akun pemilik bucket tidak ditampilkan.

```
# Historic

"resources": [
    {
```

```
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

Berikut ini adalah perilaku saat ini.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

Topik

- Menyetel kebijakan bucket untuk beberapa akun
- Buat jejak di akun tambahan

Menyetel kebijakan bucket untuk beberapa akun

Agar bucket dapat menerima file log dari beberapa akun, kebijakan bucket harus memberikan CloudTrail izin untuk menulis file log dari semua akun yang Anda tentukan. Ini berarti Anda harus mengubah kebijakan bucket di bucket tujuan untuk memberikan CloudTrail izin menulis file log dari setiap akun yang ditentukan.

> **Note**
>
> Untuk alasan keamanan, pengguna yang tidak sah tidak dapat membuat jejak yang disertakan `AWSLogs/` sebagai `S3KeyPrefix` parameter.

Untuk mengubah izin bucket sehingga file dapat diterima dari beberapa akun

1. Masuk ke Konsol Manajemen AWS menggunakan akun yang memiliki ember (11111111111111 dalam contoh ini) dan buka konsol Amazon S3.
2. Pilih bucket tempat CloudTrail mengirimkan file log Anda, lalu pilih Izin.
3. Untuk kebijakan Bucket, pilih Edit.
4. Ubah kebijakan yang ada untuk menambahkan baris untuk setiap akun tambahan yang file lognya ingin dikirim ke bucket ini. Lihat contoh kebijakan berikut dan perhatikan `Resource` baris yang digarisbawahi yang menentukan ID akun kedua. Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan bucket Amazon S3. Ini membantu mencegah akses tidak sah ke bucket S3 Anda. Jika Anda memiliki jalur yang ada, pastikan untuk menambahkan satu atau lebih kunci kondisi.

   > **Note**
   >
   > ID AWS akun adalah nomor dua belas digit, termasuk angka nol di depan.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",

 "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
                    ]
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/111111111111/*",
                "arn:aws:s3:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/222222222222/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": [

 "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",

 "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
                    ],
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Buat jejak di akun tambahan

Anda dapat menggunakan konsol atau AWS CLI untuk membuat jejak tambahan Akun AWS dan menggabungkan file log mereka ke satu bucket Amazon S3. Atau, Anda dapat membuat

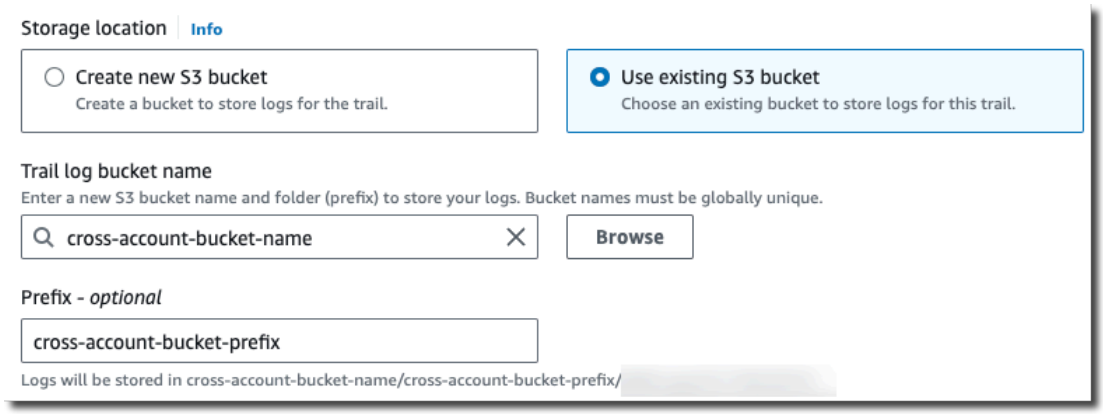
jejak organisasi untuk mencatat semua Akun AWS yang merupakan bagian dari organisasi AWS Organizations. Untuk informasi selengkapnya, lihat Membuat jejak untuk sebuah organisasi.

Menggunakan konsol untuk membuat jejak tambahan AWS rekening

Anda dapat menggunakan CloudTrail konsol untuk membuat jejak di akun tambahan.

1. Masuk Konsol Manajemen AWS dengan akun yang ingin Anda buat jejaknya. Ikuti langkah-langkah Membuat jejak dengan konsol untuk membuat jejak menggunakan konsol.
2. Untuk lokasi Penyimpanan, pilih Gunakan bucket S3 yang ada. Gunakan kotak teks untuk memasukkan nama bucket yang Anda gunakan untuk menyimpan file log di seluruh akun.

> **Note**
>
> Kebijakan bucket harus memberikan CloudTrail izin untuk menulis ke sana. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatMenyetel kebijakan bucket untuk beberapa akun.



3. Untuk Awalan, masukkan awalan yang Anda gunakan untuk menyimpan file log di seluruh akun. Jika Anda memilih untuk menggunakan awalan yang berbeda dari yang Anda tentukan dalam kebijakan bucket, Anda harus mengedit kebijakan bucket di bucket tujuan agar dapat menulis file log ke bucket menggunakan awalan baru ini. CloudTrail

Menggunakan CLI untuk membuat jejak tambahan AWS rekening

Anda dapat menggunakan alat baris AWS perintah untuk membuat jejak di akun tambahan dan menggabungkan file log mereka ke satu bucket Amazon S3. Untuk informasi selengkapnya tentang alat ini, lihat cloudtrail di Referensi AWS CLI Perintah.

Buat jejak dengan menggunakan create-trail perintah, dengan menentukan yang berikut:

- `--name`memenentukan nama jejak.
- `--s3-bucket-name`memenentukan bucket Amazon S3 yang Anda gunakan untuk menyimpan file log di seluruh akun.
- `--s3-prefix`menentukan awalan untuk jalur pengiriman file log (opsional).
- `--is-multi-region-trail`menentukan bahwa jejak ini akan mencatat peristiwa di semua AWS Wilayah di partisi tempat Anda bekerja.

Anda dapat membuat satu jejak untuk setiap Wilayah di mana akun menjalankan AWS sumber daya.

Contoh perintah berikut menunjukkan cara membuat jejak untuk akun tambahan Anda dengan menggunakan AWS CLI. Agar file log untuk akun ini dikirimkan ke bucket yang Anda buat di akun pertama Anda (111111111111 dalam contoh ini), tentukan nama bucket di opsi. `--s3-bucket-name` Nama bucket Amazon S3 unik secara global.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail
```

Ketika Anda menjalankan perintah, Anda akan melihat output yang mirip dengan yang berikut:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Untuk informasi selengkapnya tentang penggunaan CloudTrail dari alat baris AWS perintah, lihat referensi baris CloudTrail perintah.

Berbagi file CloudTrail log antar AWS akun

Bagian ini menjelaskan cara berbagi file CloudTrail log antara beberapa AWS akun. Pendekatan yang Anda gunakan untuk berbagi log Akun AWS bergantung pada konfigurasi bucket S3 Anda. Ini adalah opsi untuk berbagi file log:

- Pemilik bucket diberlakukan — Kepemilikan Objek S3 adalah setelan tingkat ember Amazon S3 yang dapat Anda gunakan untuk mengontrol kepemilikan objek yang diunggah ke bucket Anda dan untuk menonaktifkan atau mengaktifkan daftar kontrol akses (). ACLs Secara default, Kepemilikan Objek disetel ke setelan diberlakukan pemilik Bucket dan semuanya ACLs dinonaktifkan. Saat ACLs dinonaktifkan, pemilik bucket memiliki semua objek di bucket dan mengelola akses ke data secara eksklusif menggunakan kebijakan manajemen akses. Saat opsi diberlakukan pemilik Bucket disetel, akses dikelola melalui kebijakan bucket, sehingga pengguna tidak perlu mengambil peran.
- Asumsikan peran untuk berbagi file log — Jika Anda belum memilih setelan yang diterapkan pemilik Bucket, pengguna harus mengambil peran untuk mengakses file log di bucket S3 Anda.

Bagikan file log antar akun dengan mengambil peran

> **Note**
>
> Bagian ini hanya berlaku untuk bucket Amazon S3 yang tidak menggunakan setelan yang diberlakukan pemilik Bucket.

Bagian ini menjelaskan cara berbagi file CloudTrail log antara beberapa Akun AWS dengan mengasumsikan peran dan menjelaskan skenario untuk berbagi file log.

- Skenario 1: Berikan akses hanya-baca ke akun yang menghasilkan file log yang telah ditempatkan ke bucket Amazon S3 Anda.
- Skenario 2: Berikan akses ke semua file log di bucket Amazon S3 Anda ke akun pihak ketiga yang dapat menganalisis file log untuk Anda.

Untuk memberikan akses hanya-baca ke file log di bucket Amazon S3 Anda

1. Buat peran IAM untuk setiap akun yang ingin Anda bagikan file log. Anda harus menjadi administrator untuk memberikan izin.

Saat Anda membuat peran, lakukan hal berikut:

- Pilih Akun AWS opsi lain.
- Masukkan ID akun dua belas digit dari akun yang akan diberikan akses.
- Centang kotak Memerlukan MFA jika Anda ingin pengguna memberikan otentikasi multi-faktor sebelum mengambil peran.
- Pilih kebijakan AmazonS3 ReadOnlyAccess.

> **Note**
>
> Secara default, ReadOnlyAccess kebijakan AmazonS3 memberikan hak pengambilan dan daftar ke semua bucket Amazon S3 dalam akun Anda.

Untuk detail tentang manajemen izin untuk peran IAM, lihat peran IAM di Panduan Pengguna IAM.

2. Buat kebijakan akses yang memberikan akses hanya-baca ke akun yang ingin Anda bagikan file log.
3. Instruksikan setiap akun untuk mengambil peran untuk mengambil file log.

Untuk memberikan akses read-only ke file log dengan akun pihak ketiga

1. Buat peran IAM untuk akun pihak ketiga yang ingin Anda bagikan file log. Anda harus menjadi administrator untuk memberikan izin.

   Saat Anda membuat peran, lakukan hal berikut:

   - Pilih Akun AWS opsi lain.
   - Masukkan ID akun dua belas digit dari akun yang akan diberikan akses.
   - Masukkan ID eksternal yang memberikan kontrol tambahan atas siapa yang dapat mengambil peran. Untuk informasi selengkapnya, lihat Cara Menggunakan ID Eksternal Saat Memberikan Akses ke AWS Sumber Daya Anda kepada Pihak Ketiga dalam Panduan Pengguna IAM.
   - Pilih kebijakan AmazonS3 ReadOnlyAccess.

> **Note**
>
> Secara default, ReadOnlyAccess kebijakan AmazonS3 memberikan hak pengambilan dan daftar ke semua bucket Amazon S3 dalam akun Anda.

2. Buat kebijakan akses yang memberikan akses hanya-baca ke akun pihak ketiga yang ingin Anda bagikan file log.
3. Instruksikan akun pihak ketiga untuk mengambil peran untuk mengambil file log.

Bagian berikut memberikan detail lebih lanjut tentang langkah-langkah ini.

Topik

- Membuat kebijakan akses untuk memberikan akses ke akun yang Anda miliki
- Membuat kebijakan akses untuk memberikan akses ke pihak ketiga
- Dengan asumsi peran
- Berhenti berbagi file CloudTrail log antar AWS akun

Membuat kebijakan akses untuk memberikan akses ke akun yang Anda miliki

Sebagai pemilik bucket Amazon S3, Anda memiliki kendali penuh atas bucket Amazon S3 CloudTrail yang menulis file log untuk akun lain. Anda ingin berbagi file log setiap unit bisnis kembali ke unit bisnis yang membuatnya. Tapi, Anda tidak ingin unit dapat membaca file log unit lain.

Misalnya, untuk berbagi file log akun B dengan akun B tetapi tidak dengan akun C, Anda harus membuat peran IAM baru di akun Anda yang menentukan bahwa akun B adalah akun tepercaya. Kebijakan kepercayaan peran ini menetapkan bahwa akun B dipercaya untuk mengambil peran yang dibuat oleh akun Anda, dan akan terlihat seperti contoh berikut. Kebijakan kepercayaan dibuat secara otomatis jika Anda membuat peran menggunakan konsol. Jika Anda menggunakan SDK untuk membuat peran, Anda harus menyediakan kebijakan kepercayaan sebagai parameter ke `CreateRole` API. Jika Anda menggunakan CLI untuk membuat peran, Anda harus menentukan kebijakan kepercayaan dalam perintah CLI`create-role`.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Anda juga harus membuat kebijakan akses untuk menentukan bahwa akun B hanya dapat membaca dari lokasi tempat B menulis file lognya. Kebijakan akses akan terlihat seperti berikut ini. Perhatikan bahwa ARN Sumber Daya menyertakan ID akun dua belas digit untuk akun B, dan awalan yang Anda tentukan, jika ada, saat Anda mengaktifkan akun B CloudTrail selama proses agregasi. Untuk informasi selengkapnya tentang menentukan awalan, lihat. Buat jejak di akun tambahan

> **Important**
>
> Anda harus memastikan bahwa awalan dalam kebijakan akses persis sama dengan awalan yang Anda tentukan saat Anda mengaktifkan akun B. Jika tidak, maka Anda harus mengedit kebijakan akses peran IAM di akun Anda untuk memasukkan awalan aktual untuk akun B. Jika awalan dalam kebijakan akses peran tidak persis sama dengan awalan yang Anda tentukan saat Anda mengaktifkan akun B, maka akun B tidak akan dapat mengaksesnya file log. CloudTrail CloudTrail

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
```

```
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/account-B-id/
*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

Gunakan proses sebelumnya untuk akun tambahan apa pun.

Setelah Anda membuat peran untuk setiap akun dan menentukan kebijakan kepercayaan dan akses yang sesuai, dan setelah pengguna IAM di setiap akun diberikan akses oleh administrator akun tersebut, pengguna IAM di akun B atau C dapat mengambil peran secara terprogram.

Untuk informasi selengkapnya, lihat Dengan asumsi peran.

Membuat kebijakan akses untuk memberikan akses ke pihak ketiga

Anda harus membuat peran IAM terpisah untuk akun pihak ketiga. Saat Anda membuat peran, AWS secara otomatis menciptakan hubungan kepercayaan, yang menentukan bahwa akun pihak ketiga akan dipercaya untuk mengambil peran tersebut. Kebijakan akses untuk peran menentukan tindakan apa yang dapat dilakukan akun tersebut. Untuk informasi selengkapnya tentang membuat peran, lihat Membuat peran IAM.

Misalnya, hubungan kepercayaan yang dibuat oleh AWS menentukan bahwa akun pihak ketiga (akun Z dalam contoh ini) dipercaya untuk mengambil peran yang telah Anda buat. Berikut ini adalah contoh kebijakan kepercayaan:

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Jika Anda menetapkan ID eksternal saat membuat peran untuk akun pihak ketiga, kebijakan akses berisi `Condition` elemen tambahan yang menguji ID unik yang ditetapkan oleh akun tersebut. Tes dilakukan ketika peran diasumsikan. Contoh kebijakan akses berikut memiliki `Condition` elemen.

Untuk informasi selengkapnya, lihat Cara menggunakan ID eksternal saat memberikan akses ke AWS sumber daya Anda kepada pihak ketiga dalam Panduan Pengguna IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111111111111:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-account-Z"}}
    }]
}
```

Anda juga harus membuat kebijakan akses untuk akun Anda untuk menentukan bahwa akun pihak ketiga dapat membaca semua log dari bucket Amazon S3. Kebijakan akses akan terlihat seperti contoh berikut. Kartu liar (*) di akhir `Resource` nilai menunjukkan bahwa akun pihak ketiga dapat mengakses file log apa pun di bucket S3 yang telah diberikan aksesnya.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

Setelah Anda membuat peran untuk akun pihak ketiga dan menentukan hubungan kepercayaan dan kebijakan akses yang sesuai, pengguna IAM di akun pihak ketiga harus secara terprogram mengambil peran tersebut agar dapat membaca file log dari bucket. Untuk informasi selengkapnya, lihat Dengan asumsi peran.

Dengan asumsi peran

Anda harus menunjuk pengguna IAM terpisah untuk mengambil setiap peran yang Anda buat di setiap akun. Anda kemudian harus memastikan bahwa setiap pengguna IAM memiliki izin yang sesuai.

Pengguna dan peran IAM

Setelah Anda membuat peran dan kebijakan yang diperlukan, Anda harus menunjuk pengguna IAM di setiap akun yang ingin Anda bagikan file. Setiap pengguna IAM secara terprogram mengasumsikan peran yang sesuai untuk mengakses file log. Ketika pengguna mengambil peran,

AWS mengembalikan kredensi keamanan sementara ke pengguna tersebut. Mereka kemudian dapat membuat permintaan untuk membuat daftar, mengambil, menyalin, atau menghapus file log tergantung pada izin yang diberikan oleh kebijakan akses yang terkait dengan peran tersebut.

Untuk informasi selengkapnya tentang bekerja dengan identitas IAM, lihat Identitas IAM (pengguna, grup pengguna, dan peran).

Perbedaan utama dalam kebijakan akses yang Anda buat untuk setiap peran IAM di setiap skenario.

- Dalam skenario 1, kebijakan akses membatasi setiap akun untuk hanya membaca file lognya sendiri. Untuk informasi selengkapnya, lihat Membuat kebijakan akses untuk memberikan akses ke akun yang Anda miliki.
- Dalam skenario 2, kebijakan akses memungkinkan pihak ketiga untuk membaca semua file log yang digabungkan dalam bucket Amazon S3. Untuk informasi selengkapnya, lihat Membuat kebijakan akses untuk memberikan akses ke pihak ketiga.

Membuat kebijakan izin untuk pengguna IAM

Untuk melakukan tindakan yang diizinkan oleh peran, pengguna IAM harus memiliki izin untuk memanggil AWS STS `AssumeRole`API. Anda harus mengedit kebijakan untuk setiap pengguna untuk memberi mereka izin yang sesuai. Untuk melakukannya, Anda menetapkan elemen Resource dalam kebijakan yang Anda lampirkan ke pengguna IAM. Contoh berikut menunjukkan kebijakan untuk pengguna IAM di akun lain yang memungkinkan pengguna tersebut untuk mengambil peran bernama yang `Test` dibuat sebelumnya oleh Akun A.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/Test"
        }
    ]
}
```

Untuk menyunting kebijakan yang dikelola pelanggan (konsol)

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Dari daftar kebijakan, pilih nama kebijakan untuk disunting. Anda dapat menggunakan kotak pencarian untuk memfilter daftar kebijakan.
4. Pilih tab Izin, lalu pilih Edit.
5. Lakukan salah satu tindakan berikut:

   - Pilih opsi Visual untuk mengubah kebijakan Anda tanpa memahami sintaks JSON. Anda dapat membuat perubahan pada layanan, tindakan, sumber daya, atau kondisi opsional untuk setiap blokir izin dalam kebijakan Anda. Anda juga dapat mengimpor kebijakan untuk menambahkan izin tambahan ke bawah kebijakan Anda. Setelah selesai melakukan perubahan, pilih Berikutnya untuk melanjutkan.
   - Pilih opsi JSON untuk mengubah kebijakan Anda dengan mengetik atau menempelkan teks di kotak teks JSON. Anda juga dapat mengimpor kebijakan untuk menambahkan izin tambahan ke bawah kebijakan Anda. Selesaikan peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan, lalu pilih Berikutnya.

     > **Note**
     >
     > Anda dapat beralih antara opsi editor Visual dan JSON kapan saja. Namun, jika Anda melakukan perubahan atau memilih Berikutnya di editor Visual, IAM dapat merestrukturisasi kebijakan Anda untuk mengoptimalkannya bagi editor visual. Untuk informasi selengkapnya, lihat Restrukturisasi kebijakan dalam Panduan Pengguna IAM.

6. Pada halaman Tinjau dan simpan, tinjau Izin yang ditentukan dalam kebijakan ini, lalu pilih Simpan perubahan untuk menyimpan pekerjaan Anda.
7. Jika kebijakan terkelola sudah memiliki maksimal lima versi, memilih Simpan perubahan akan menampilkan kotak dialog. Untuk menyimpan versi baru Anda, versi kebijakan non-default tertua akan dihapus dan diganti dengan versi baru ini. Secara opsional, Anda dapat mengatur versi baru sebagai versi kebijakan default.

   Pilih Simpan perubahan untuk menyimpan versi kebijakan baru Anda.

Memanggil AssumeRole

Pengguna dapat mengambil peran dengan membuat aplikasi yang memanggil AWS STS `AssumeRole`API dan meneruskan nama sesi peran, Amazon Resource Number (ARN) peran yang akan diambil, dan ID eksternal opsional. Nama sesi peran ditentukan oleh akun yang membuat peran untuk diasumsikan. ID eksternal, jika ada, ditentukan oleh akun pihak ketiga dan diteruskan ke akun pemilik untuk dimasukkan selama pembuatan peran. Untuk informasi selengkapnya, lihat Cara Menggunakan ID Eksternal Saat Memberikan Akses ke AWS Sumber Daya Anda kepada Pihak Ketiga dalam Panduan Pengguna IAM. Anda dapat mengambil ARN dari Akun A dengan membuka konsol IAM.

Untuk menemukan Nilai ARN di Akun A dengan konsol IAM

1. Pilih Peran
2. Pilih peran yang ingin Anda periksa.
3. Cari Peran ARN di bagian Ringkasan.

AssumeRole API mengembalikan kredensi sementara yang akan digunakan untuk mengakses sumber daya dalam memiliki akun. Dalam contoh ini, sumber daya yang ingin Anda akses adalah bucket Amazon S3 dan file log yang berisi bucket. Kredensi sementara memiliki izin yang Anda tetapkan dalam kebijakan akses peran.

Contoh Python berikut (menggunakan AWS SDK for Python (Boto)) menunjukkan cara memanggil `AssumeRole` dan cara menggunakan kredenal keamanan sementara yang dikembalikan untuk mencantumkan semua bucket Amazon S3 yang dikendalikan oleh Akun A.

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
```

```
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

Berhenti berbagi file CloudTrail log antar AWS akun

Untuk berhenti berbagi file log ke yang lain Akun AWS, hapus peran yang Anda buat untuk akun itu. Untuk selengkapnya tentang cara menghapus peran, lihat Menghapus peran atau profil instance.

Memvalidasi CloudTrail integritas file log

Untuk menentukan apakah file log diubah, dihapus, atau tidak diubah setelah CloudTrail dikirimkan, Anda dapat menggunakan validasi integritas file CloudTrail log. Fitur ini dibangun

menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus atau memalsukan CloudTrail file log tanpa deteksi. Anda dapat menggunakan AWS CLI untuk memvalidasi file di lokasi di mana CloudTrail mengirimkannya.

Mengapa menggunakannya?

File log yang divalidasi sangat berharga dalam penyelidikan keamanan dan forensik. Misalnya, file log yang divalidasi memungkinkan Anda untuk menegaskan secara positif bahwa file log itu sendiri tidak berubah, atau kredenal pengguna tertentu melakukan aktivitas API tertentu. Proses validasi integritas file CloudTrail log juga memungkinkan Anda mengetahui apakah file log telah dihapus atau diubah, atau menegaskan secara positif bahwa tidak ada file log yang dikirim ke akun Anda selama periode waktu tertentu.

Cara kerjanya

Saat Anda mengaktifkan validasi integritas file log, CloudTrail buat hash untuk setiap file log yang dikirimkannya. Setiap jam, CloudTrail juga membuat dan mengirimkan file yang mereferensikan file log selama satu jam terakhir dan berisi hash masing-masing. File ini disebut file digest. CloudTrail menandatangani setiap file digest menggunakan kunci pribadi dari public dan private key pair. Setelah pengiriman, Anda dapat menggunakan kunci publik untuk memvalidasi file intisari. CloudTrail menggunakan pasangan kunci yang berbeda untuk masing-masing Wilayah AWS.

File digest dikirim ke bucket Amazon S3 yang sama yang terkait dengan jejak Anda sebagai file log CloudTrail Anda. Jika file log Anda dikirim dari semua Wilayah atau dari beberapa akun ke dalam satu bucket Amazon S3, CloudTrail akan mengirimkan file intisari dari Wilayah dan akun tersebut ke dalam bucket yang sama.

File digest dimasukkan ke dalam folder yang terpisah dari file log. Pemisahan file intisari dan file log ini memungkinkan Anda untuk menegakkan kebijakan keamanan terperinci dan memungkinkan solusi pemrosesan log yang ada untuk terus beroperasi tanpa modifikasi. Setiap file digest juga berisi tanda tangan digital dari file digest sebelumnya jika ada. Tanda tangan untuk file intisari saat ini ada di properti metadata objek file intisari Amazon S3. Untuk informasi selengkapnya tentang isi file digest, lihatCloudTrail struktur file digest.

Menyimpan log dan mencerna file

Anda dapat menyimpan file CloudTrail log dan mencerna file di Amazon S3 atau Amazon Glacier dengan aman, tahan lama, dan murah untuk jangka waktu yang tidak terbatas. Untuk meningkatkan

keamanan file digest yang disimpan di Amazon S3, Anda dapat menggunakan Amazon S3 MFA Delete.

Mengaktifkan validasi dan memvalidasi file

Untuk mengaktifkan validasi integritas file log, Anda dapat menggunakan Konsol Manajemen AWS, the AWS CLI, atau CloudTrail API. Mengaktifkan validasi integritas file log memungkinkan CloudTrail untuk mengirimkan file log intisari ke bucket Amazon S3 Anda, tetapi tidak memvalidasi integritas file. Untuk informasi selengkapnya, lihat Mengaktifkan validasi integritas file log untuk CloudTrail.

Untuk memvalidasi integritas file CloudTrail log, Anda dapat menggunakan AWS CLI atau membuat solusi Anda sendiri. AWS CLI Akan memvalidasi file di lokasi di mana CloudTrail mengirimkannya. Jika Anda ingin memvalidasi log yang telah dipindahkan ke lokasi lain, baik di Amazon S3 atau di tempat lain, Anda dapat membuat alat validasi Anda sendiri.

Untuk informasi tentang memvalidasi log dengan menggunakan AWS CLI, lihatMemvalidasi integritas file CloudTrail log dengan AWS CLI. Untuk informasi tentang pengembangan implementasi kustom validasi file CloudTrail log, lihat. Implementasi kustom validasi integritas file CloudTrail log

Mengaktifkan validasi integritas file log untuk CloudTrail

Anda dapat mengaktifkan validasi integritas file log dengan menggunakan Konsol Manajemen AWS, AWS Command Line Interface (AWS CLI), atau CloudTrail API. CloudTrail mulai mengirimkan file digest dalam waktu sekitar satu jam.

Konsol Manajemen AWS

Untuk mengaktifkan validasi integritas file log dengan CloudTrail konsol, pilih Ya untuk opsi Aktifkan validasi file log saat Anda membuat atau memperbarui jejak. Secara default, fitur ini diaktifkan untuk jalur baru. Untuk informasi selengkapnya, lihat Membuat dan memperbarui jejak dengan konsol.

AWS CLI

Untuk mengaktifkan validasi integritas file log dengan AWS CLI, gunakan `--enable-log-file-validation` opsi dengan perintah create-trail atau update-trail. Untuk menonaktifkan validasi integritas file log, gunakan `--no-enable-log-file-validation` opsi.

Contoh

`update-trail`Perintah berikut memungkinkan validasi file log dan mulai mengirimkan file intisari ke bucket Amazon S3 untuk jejak yang ditentukan.

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

Untuk mengaktifkan validasi integritas file log dengan CloudTrail API, setel parameter `EnableLogFileValidation` permintaan `true` saat memanggil `CreateTrail` atau`UpdateTrail`.

Untuk informasi selengkapnya, lihat CreateTraildan UpdateTraildi Referensi AWS CloudTrail API.

Memvalidasi integritas file CloudTrail log dengan AWS CLI

Untuk memvalidasi log dengan AWS Command Line Interface, gunakan CloudTrail `validate-logs` perintah. Perintah menggunakan file intisari yang dikirimkan ke bucket Amazon S3 Anda untuk melakukan validasi. Untuk informasi tentang file digest, lihatCloudTrail struktur file digest.

AWS CLI Ini memungkinkan Anda mendeteksi jenis perubahan berikut:

- Modifikasi atau penghapusan file log CloudTrail
- Modifikasi atau penghapusan file digest CloudTrail
- Modifikasi atau penghapusan kedua hal di atas

> **Note**
>
> AWS CLI Memvalidasi hanya file log yang direferensikan oleh file digest. Untuk informasi selengkapnya, lihat Memeriksa apakah file tertentu telah dikirimkan oleh CloudTrail.

Prasyarat

Untuk memvalidasi integritas file log dengan AWS CLI, kondisi berikut harus dipenuhi:

- Anda harus memiliki konektivitas online untuk AWS.
- Anda harus memiliki akses baca ke bucket Amazon S3 yang berisi file intisari dan log.
- File intisari dan log tidak boleh dipindahkan dari lokasi Amazon S3 asli CloudTrail tempat mengirimkannya.
- Peran yang menjalankan perintah harus memiliki izin untuk memanggil `ListObjects``GetObject`, dan `GetBucketLocation` untuk setiap bucket S3 direferensikan oleh jejak.

> **Note**
>
> File log yang telah diunduh ke disk lokal tidak dapat divalidasi dengan file. AWS CLI Untuk panduan tentang membuat alat Anda sendiri untuk validasi, lihatImplementasi kustom validasi integritas file CloudTrail log.

validasi-log

Sintaksis

Berikut ini adalah sintaks untuk`validate-logs`. Parameter opsional ditampilkan dalam tanda kurung.

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <amzn-s3-demo-bucket>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> `validate-logs`Perintahnya spesifik Wilayah. Anda harus menentukan opsi `--region` global untuk memvalidasi log untuk spesifik Wilayah AWS.

Opsi

Berikut ini adalah opsi baris perintah untuk. `validate-logs` `--start-time`Pilihan `--trail-arn` dan diperlukan. `--account-id`Opsi ini juga diperlukan untuk jalur organisasi.

`--start-time`

Menentukan bahwa file log dikirim pada atau setelah nilai timestamp UTC tertentu akan divalidasi. Contoh:`2015-01-08T05:21:42Z`.

`--end-time`

Secara opsional menentukan bahwa file log yang dikirimkan pada atau sebelum nilai stempel waktu UTC yang ditentukan akan divalidasi. Nilai default adalah waktu UTC saat ini (`Date.now()`). Contoh:`2015-01-08T12:31:41Z`.

> **Note**
>
> Untuk rentang waktu yang ditentukan, `validate-logs` perintah hanya memeriksa file log yang direferensikan dalam file intisari yang sesuai. Tidak ada file log lain di bucket Amazon S3 yang dicentang. Untuk informasi selengkapnya, lihat Memeriksa apakah file tertentu telah dikirimkan oleh CloudTrail.

`--s3-bucket`

Secara opsional menentukan bucket Amazon S3 tempat file digest disimpan. Jika nama bucket tidak ditentukan, AWS CLI maka akan mengambilnya dengan meneleponDescribeTrails().

`--s3-prefix`

Secara opsional menentukan awalan Amazon S3 tempat file intisari disimpan. Jika tidak ditentukan, AWS CLI akan mengambilnya dengan meneleponDescribeTrails().

> **Note**
>
> Anda harus menggunakan opsi ini hanya jika awalan Anda saat ini berbeda dari awalan yang digunakan selama rentang waktu yang Anda tentukan.

`--account-id`

Secara opsional menentukan akun untuk memvalidasi log. Parameter ini diperlukan untuk jejak organisasi untuk memvalidasi log untuk akun tertentu di dalam organisasi.

`--trail-arn`

Menentukan Nama Sumber Daya Amazon (ARN) dari jejak yang akan divalidasi. Format jejak ARN berikut.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Untuk mendapatkan jejak ARN untuk jejak, Anda dapat menggunakan `describe-trails` perintah sebelum menjalankan. `validate-logs`
> Anda mungkin ingin menentukan nama bucket dan awalan selain jejak ARN jika file log telah dikirim ke lebih dari satu bucket dalam rentang waktu yang Anda tentukan, dan Anda ingin membatasi validasi ke file log hanya di salah satu bucket.

`--verbose`

Secara opsional mengeluarkan informasi validasi untuk setiap file log atau digest dalam rentang waktu yang ditentukan. Output menunjukkan apakah file tetap tidak berubah atau telah dimodifikasi atau dihapus. Dalam mode non-verbose (default), informasi dikembalikan hanya untuk kasus-kasus di mana ada kegagalan validasi.

Contoh

Contoh berikut memvalidasi file log dari waktu mulai yang ditentukan hingga saat ini, menggunakan bucket Amazon S3 yang dikonfigurasi untuk jejak saat ini dan menentukan keluaran verbose.

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

Cara kerja **`validate-logs`**

`validate-logs`Perintah dimulai dengan memvalidasi file intisari terbaru dalam rentang waktu yang ditentukan. Pertama, ini memverifikasi bahwa file intisari telah diunduh dari lokasi yang diklaimnya. Dengan kata lain, jika CLI mengunduh file digest `df1` dari lokasi S3`p1`, validate-logs akan memverifikasi itu. `p1 == df1.digestS3Bucket + '/' + df1.digestS30bject`

Jika tanda tangan file intisari valid, ia memeriksa nilai hash dari masing-masing log yang direferensikan dalam file intisari. Perintah kemudian kembali ke masa lalu, memvalidasi file intisari sebelumnya dan file log yang direferensikan secara berurutan. Ini berlanjut sampai nilai yang ditentukan untuk `start-time` tercapai, atau sampai rantai digest berakhir. Jika file intisari hilang atau tidak valid, rentang waktu yang tidak dapat divalidasi ditunjukkan dalam output. `validate-logs`Perintah pertama kali beroperasi pada rantai intisari standar. Setelah menyelesaikan validasi

intisari standar, ini memvalidasi file intisari isi ulang, jika ada. Intisari isi ulang membentuk rantai validasi terpisah dan diproses secara independen dari intisari standar.

Hasil validasi

Hasil validasi dimulai dengan header ringkasan dalam format berikut:

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

Setiap baris output utama berisi hasil validasi untuk satu intisari atau file log dalam format berikut. Baris diawali dengan `(backfill)` menunjukkan file intisari isi ulang, yang membentuk rantai validasi terpisah dari file intisari standar.

```
<optional (backfill)> <Digest file | Log file> <S3 path> <Validation Message>
```

Tabel berikut menjelaskan kemungkinan pesan validasi untuk file log dan digest.

Jenis berkas	Pesan Validasi	Deskripsi
`Digest file`	`valid`	Tanda tangan file digest valid. File log yang direferensikannya dapat diperiksa. Pesan ini hanya disertakan dalam mode verbose.
`Digest file`	`INVALID: has been moved from its original location`	Bucket S3 atau objek S3 tempat file digest diambil tidak cocok dengan bucket S3 atau lokasi objek S3 yang direkam dalam file digest itu sendiri.
`Digest file`	`INVALID: invalid format`	Format file digest tidak valid. File log yang sesuai dengan rentang waktu yang diwakili oleh file intisari tidak dapat divalidasi.
`Digest file`	`INVALID: not found`	File digest tidak ditemukan. File log yang sesuai dengan rentang waktu yang diwakili oleh file intisari tidak dapat divalidasi.
`Digest file`	`INVALID: public key not found for fingerprint` *`fingerprint`*	Kunci publik yang sesuai dengan sidik jari yang direkam dalam file intisari tidak ditemukan. File digest tidak dapat divalidasi.

Jenis berkas	Pesan Validasi	Deskripsi
`Digest file`	`INVALID: signature verification failed`	Tanda tangan file digest tidak valid. Karena file digest tidak valid, file log yang direferen sikannya tidak dapat divalidasi, dan tidak ada pernyataan yang dapat dibuat tentang aktivitas API di dalamnya.
`Digest file`	`INVALID: Unable to load PKCS #1 key with fingerprint` *`fingerprint`*	Karena kunci publik yang dikodekan DER dalam format PKCS #1 yang memiliki sidik jari yang ditentukan tidak dapat dimuat, file intisari tidak dapat divalidasi.
`Log file`	`valid`	File log telah divalidasi dan belum dimodifik asi sejak saat pengiriman. Pesan ini hanya disertakan dalam mode verbose.
`Log file`	`INVALID: hash value doesn't match`	Hash untuk file log tidak cocok. File log telah dimodifikasi setelah pengiriman oleh CloudTrail.
`Log file`	`INVALID: invalid format`	Format file log tidak valid. File log tidak dapat divalidasi.
`Log file`	`INVALID: not found`	File log tidak ditemukan dan tidak dapat divalidasi.

Output mencakup informasi ringkasan tentang hasil yang dikembalikan.

Contoh output

Bertele-tele

Contoh `validate-logs` perintah berikut menggunakan `--verbose` bendera dan menghasilkan output sampel yang mengikuti. `[...]`menunjukkan output sampel telah disingkat.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid
```

```
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

`validate-logs`Perintah contoh berikut menggunakan `--verbose` bendera pada periode ketika file intisari isi ulang hadir dan menghasilkan output sampel yang mengikuti. Intisari isi ulang muncul dengan `(backfill)` awalan dan divalidasi secara terpisah dari rantai intisari standar. `[...]`menunjukkan output sampel telah disingkat.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2024-07-31T22:00:00Z --end-
time 2024-08-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2024-07-31T22:00:00Z and 2024-08-01T19:17:29Z

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T201728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1925Z_Xm3pK9vN2wQ5rT8h.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1915Z_Bj7cL4nM6pR9sU2v.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1930Z_Fy1dG8kN3qT6wX0z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1920Z_Hn5jM2pQ7sV9yB4e.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1950Z_Kp8rN1tW4xZ7aC3f.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1920Z_Mq6sP9uX2yB5dE8g.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1915Z_Rt4vQ7wZ0aC3fG6h.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T191728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1910Z_Uw9xR2yB5dH8jK1m.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T1055Z_Vz3aS6cE9fL2nP5q.json.gz valid
```

```
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T1040Z_Xy7bT0dG3hM6pR9s.json.gz valid

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T091728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T081728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T071728Z.json.gz valid
[...]
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/07/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240731T221728Z.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T201728Z_backfill.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T191728Z_backfill.json.gz valid
[...]

(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T101728Z_backfill.json.gz INVALID: signature verification failed

(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T091728Z_backfill.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T0830Z_Rn6uk0wY5aD9fJ3n.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T081728Z_backfill.json.gz valid
```

```
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T071728Z_backfill.json.gz valid
[...]
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/07/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240731T221728Z_backfill.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2145Z_Sp3vm7xZ2bE6gK0p.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2125Z_Tq0wn4ya9cF3hL7q.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2130Z_Ur7xp1zb6dG0jM4r.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2155Z_Vs4yq8ac3eH7kN1s.json.gz valid

Results requested for 2024-07-31T22:00:00Z to 2024-08-01T19:17:29Z
Results found for 2024-07-31T22:17:28Z to 2024-08-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
22/23 backfill digest files valid, 1/23 backfill digest files INVALID
63/63 log files valid
```

Tidak bertele-tele

Contoh `validate-logs` perintah berikut tidak menggunakan `--verbose` bendera. Dalam output sampel berikut, satu kesalahan ditemukan. Hanya informasi header, kesalahan, dan ringkasan yang dikembalikan.

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed
```

```
(backfill) Digest file s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/
us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T101728Z_backfill.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
22/23 backfill digest files valid, 1/23 backfill digest files INVALID
63/63 log files valid
```

Memeriksa apakah file tertentu telah dikirimkan oleh CloudTrail

Untuk memeriksa apakah file tertentu dalam bucket Anda dikirimkan oleh CloudTrail, jalankan `validate-logs` dalam mode verbose untuk periode waktu yang menyertakan file tersebut. Jika file muncul di output`validate-logs`, maka file tersebut dikirim oleh CloudTrail.

CloudTrail struktur file digest

Setiap file digest berisi nama file log yang dikirimkan ke bucket Amazon S3 Anda selama satu jam terakhir, nilai hash untuk file log tersebut, dan tanda tangan digital dari file intisari sebelumnya. Tanda tangan untuk file intisari saat ini disimpan dalam properti metadata dari objek file digest. Tanda tangan digital dan hash digunakan untuk memvalidasi integritas file log dan file digest itu sendiri.

Intisari lokasi file

File Digest dikirim ke lokasi bucket Amazon S3 yang mengikuti sintaks ini.

```
s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> Untuk jalur organisasi, lokasi bucket juga menyertakan ID unit organisasi, sebagai berikut:
>
> ```
> s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
> ```

```
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> File intisari isi ulang dikirimkan saat CloudTrail perlu menyertakan file log yang tidak direferensikan dalam intisari asli karena penundaan pemrosesan. File intisari isi ulang menggunakan `_backfill` akhiran dalam nama file mereka, sebagai berikut:
>
> ```
> s3://amzn-s3-demo-bucket/optional-prefix/AWSLogs/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp_backfill.json.gz
> ```

Contoh isi file intisari

Contoh file digest berikut berisi informasi untuk CloudTrail log.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "amzn-s3-demo-bucket",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
```

```
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "amzn-s3-demo-bucket",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```


Deskripsi bidang file Digest

Berikut ini adalah deskripsi untuk setiap bidang dalam file intisari:

`awsAccountId`

ID AWS akun tempat file intisari telah dikirimkan.

`digestStartTime`

Rentang waktu UTC awal yang dicakup oleh file intisari, mengambil sebagai referensi waktu di mana file log telah dikirimkan oleh. CloudTrail Ini berarti bahwa jika rentang waktunya [Ta, Tb], intisari akan berisi semua file log yang dikirimkan ke pelanggan antara Ta dan Tb.

`digestEndTime`

Rentang waktu UTC akhir yang dicakup oleh file intisari, mengambil sebagai referensi waktu di mana file log telah dikirimkan oleh. CloudTrail Ini berarti bahwa jika rentang waktunya [Ta, Tb], intisari akan berisi semua file log yang dikirimkan ke pelanggan antara Ta dan Tb.

`digestS3Bucket`

Nama bucket Amazon S3 tempat file intisari saat ini telah dikirimkan.

`digestS3Object`

Kunci objek Amazon S3 (yaitu, lokasi bucket Amazon S3) dari file intisari saat ini. Dua Wilayah pertama dalam string menunjukkan Wilayah dari mana file intisari dikirim. Wilayah terakhir (setelah`your-trail-name`) adalah Wilayah asal jalan setapak. Wilayah asal adalah Wilayah di mana jalan setapak itu dibuat. Dalam kasus jejak Multi-wilayah, ini bisa berbeda dari Wilayah tempat file intisari dikirim.

`newestEventTime`

Waktu UTC dari acara terbaru di antara semua peristiwa dalam file log di intisari.

`oldestEventTime`

Waktu UTC dari acara tertua di antara semua peristiwa dalam file log di intisari.

> **Note**
>
> Jika file digest dikirim terlambat, nilai `oldestEventTime` akan lebih awal dari nilai. `digestStartTime`

`previousDigestS3Bucket`

Bucket Amazon S3 tempat file intisari sebelumnya dikirimkan.

`previousDigestS3Object`

Kunci objek Amazon S3 (yaitu, lokasi bucket Amazon S3) dari file intisari sebelumnya.

`previousDigestHashValue`

Nilai hash yang dikodekan heksadesimal dari konten yang tidak terkompresi dari file intisari sebelumnya.

`previousDigestHashAlgorithm`

Nama algoritma hash yang digunakan untuk hash file digest sebelumnya.

`publicKeyFingerprint`

Sidik jari heksadesimal yang dikodekan dari kunci publik yang cocok dengan kunci pribadi yang digunakan untuk menandatangani file intisari ini. Anda dapat mengambil kunci publik untuk rentang waktu yang sesuai dengan file digest dengan menggunakan AWS CLI atau API. CloudTrail Dari kunci publik yang dikembalikan, kunci yang sidik jarinya cocok dengan nilai ini dapat digunakan untuk memvalidasi file intisari. Untuk informasi tentang mengambil kunci publik untuk file digest, lihat AWS CLI `list-public-keys`perintah atau API. CloudTrail `ListPublicKeys`

> **Note**
>
> CloudTrail menggunakan pasangan private/public kunci yang berbeda per Wilayah. Setiap file intisari ditandatangani dengan kunci pribadi yang unik untuk Wilayahnya. Oleh karena itu, ketika Anda memvalidasi file intisari dari Wilayah tertentu, Anda harus mencari di Wilayah yang sama untuk kunci publik yang sesuai.

`digestSignatureAlgorithm`

Algoritma yang digunakan untuk menandatangani file digest.

`logFiles.s3Bucket`

Nama bucket Amazon S3 untuk file log.

`logFiles.s3Object`

Kunci objek Amazon S3 dari file log saat ini.

`logFiles.newestEventTime`

Waktu UTC dari peristiwa terbaru dalam file log. Kali ini juga sesuai dengan cap waktu dari file log itu sendiri.

`logFiles.oldestEventTime`

Waktu UTC dari peristiwa tertua dalam file log.

`logFiles.hashValue`

Nilai hash yang dikodekan heksadesimal dari konten file log yang tidak terkompresi.

`logFiles.hashAlgorithm`

Algoritma hash digunakan untuk hash file log.

Memulai file intisari

Ketika validasi integritas file log dimulai, file intisari awal akan dihasilkan. File intisari awal juga akan dihasilkan ketika validasi integritas file log dimulai ulang (dengan menonaktifkan dan kemudian mengaktifkan kembali validasi integritas file log, atau dengan menghentikan logging dan kemudian memulai kembali logging dengan validasi diaktifkan). Dalam file intisari awal, bidang berikut yang berkaitan dengan file intisari sebelumnya akan menjadi nol:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

File cerna 'Kosong'

CloudTrail akan mengirimkan file intisari bahkan ketika tidak ada aktivitas API di akun Anda selama periode satu jam yang diwakili oleh file intisari. Ini dapat berguna ketika Anda perlu menegaskan bahwa tidak ada file log yang dikirim selama jam yang dilaporkan oleh file digest.

Contoh berikut menunjukkan konten file intisari yang direkam satu jam ketika tidak ada aktivitas API yang terjadi. Perhatikan bahwa `logFiles:[ ]` bidang di akhir isi file digest kosong.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
```

```
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "amzn-s3-demo-bucket",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```

Tanda tangan dari file intisari

Informasi tanda tangan untuk file intisari terletak di dua properti metadata objek objek file intisari Amazon S3. Setiap file intisari memiliki entri metadata berikut:

- `x-amz-meta-signature`

  Nilai enkode heksadesimal dari tanda tangan file digest. Berikut ini adalah contoh tanda tangan:

  ```
  3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
  28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
  05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
  ```

- `x-amz-meta-signature-algorithm`

  Berikut ini menunjukkan nilai contoh algoritma yang digunakan untuk menghasilkan tanda tangan intisari:

  `SHA256withRSA`

- `x-amz-meta-backfill-generation-timestamp`

Stempel waktu UTC saat intisari isi ulang dihasilkan. Properti metadata ini hanya ada dalam file intisari isi ulang dan digunakan untuk mengidentifikasi kunci publik yang benar untuk validasi tanda tangan. Berikut ini adalah contoh stempel waktu:

```
2025-05-20T00:00:00.000Z
```

Mencerna rantai file

Fakta bahwa setiap file intisari berisi referensi ke file intisari sebelumnya memungkinkan “rantai” yang memungkinkan alat validasi seperti AWS CLI untuk mendeteksi apakah file intisari telah dihapus. Ini juga memungkinkan file intisari dalam rentang waktu tertentu untuk diperiksa secara berturut-turut, dimulai dengan yang terbaru terlebih dahulu.

> **Note**
>
> Saat Anda menonaktifkan validasi integritas file log, rantai file intisari rusak setelah satu jam. CloudTrail tidak akan membuat file digest untuk file log yang dikirim selama periode di mana validasi integritas file log dinonaktifkan. Misalnya, jika Anda mengaktifkan validasi integritas berkas log pada siang hari tanggal 1 Januari, menonaktifkannya pada siang hari tanggal 2 Januari, dan mengaktifkan kembali pada siang hari tanggal 10 Januari, file digest tidak akan dibuat untuk berkas log yang dikirim pada siang hari tanggal 2 Januari hingga siang hari tanggal 10 Januari. Hal yang sama berlaku setiap kali Anda berhenti CloudTrail mencatat atau menghapus jejak.

Jika kebijakan bucket S3 trail Anda salah dikonfigurasi atau CloudTrail mengalami gangguan layanan yang tidak terduga, Anda mungkin tidak menerima semua atau beberapa file intisari. Untuk mengonfirmasi apakah jejak Anda memiliki kesalahan pengiriman intisari, jalankan `get-trail-status`perintah dan periksa `LatestDigestDeliveryError` parameter untuk kesalahan. Setelah masalah pengiriman diselesaikan (misalnya, dengan memperbaiki kebijakan bucket), CloudTrail akan mencoba mengirimkan ulang file intisari yang hilang. Selama periode pengiriman ulang, file intisari mungkin dikirim rusak, sehingga rantai mungkin sementara tampak rusak.

Jika logging dihentikan atau jejak dihapus, CloudTrail akan mengirimkan file intisari akhir. File digest ini dapat berisi informasi untuk file log yang tersisa yang mencakup peristiwa hingga dan termasuk `StopLogging` acara tersebut.

Implementasi kustom validasi integritas file CloudTrail log

Karena CloudTrail menggunakan standar industri, algoritma kriptografi yang tersedia secara terbuka dan fungsi hash, Anda dapat membuat alat Anda sendiri untuk memvalidasi integritas file log. CloudTrail Saat validasi integritas file log diaktifkan, kirimkan file CloudTrail intisari ke bucket Amazon S3 Anda. Anda dapat menggunakan file-file ini untuk mengimplementasikan solusi validasi Anda sendiri. Untuk informasi selengkapnya tentang file digest, lihatCloudTrail struktur file digest.

Topik ini menjelaskan bagaimana file digest ditandatangani, dan kemudian merinci langkah-langkah yang perlu Anda ambil untuk menerapkan solusi yang memvalidasi file digest dan file log yang mereka referensikan.

Memahami bagaimana file CloudTrail digest ditandatangani

CloudTrail file digest ditandatangani dengan tanda tangan digital RSA. Untuk setiap file digest, CloudTrail lakukan hal berikut:

1. Membuat string untuk penandatanganan data berdasarkan bidang file digest yang ditunjuk (dijelaskan di bagian berikutnya).
2. Mendapat kunci pribadi yang unik untuk Wilayah.
3. Melewati hash SHA-256 dari string dan kunci pribadi ke algoritma penandatanganan RSA, yang menghasilkan tanda tangan digital.
4. Mengkodekan kode byte tanda tangan ke dalam format heksadesimal.
5. Menempatkan tanda tangan digital ke properti `x-amz-meta-signature` metadata objek file intisari Amazon S3.

Isi string penandatanganan data

CloudTrail Objek berikut disertakan dalam string untuk penandatanganan data:

- Stempel waktu akhir file intisari dalam format diperpanjang UTC (misalnya,) `2015-05-08T07:19:37Z`
- Jalur S3 file intisari saat ini
- Hash SHA-256 yang dikodekan heksadesimal dari file intisari saat ini
- Tanda tangan heksadesimal yang dikodekan dari file intisari sebelumnya

Format untuk menghitung string ini dan string contoh disediakan nanti dalam dokumen ini.

Langkah-langkah implementasi validasi kustom

Saat menerapkan solusi validasi kustom, Anda harus memvalidasi file digest terlebih dahulu, dan kemudian file log yang direferensikannya.

Validasi file intisari

Untuk memvalidasi file intisari, Anda memerlukan tanda tangannya, kunci publik yang kunci pribadinya digunakan untuk menandatanganinya, dan string penandatanganan data yang Anda hitung.

1. Dapatkan file intisari.
2. Verifikasi bahwa file intisari telah diambil dari lokasi aslinya.
3. Dapatkan tanda tangan heksadesimal yang dikodekan dari file digest.
4. Dapatkan sidik jari yang dikodekan heksadesimal dari kunci publik yang kunci pribadinya digunakan untuk menandatangani file intisari.
5. Ambil kunci publik untuk rentang waktu yang sesuai dengan file digest.
6. Dari antara kunci publik yang diambil, pilih kunci publik yang sidik jarinya cocok dengan sidik jari dalam file intisari.
7. Menggunakan hash file digest dan bidang file digest lainnya, buat ulang string penandatanganan data yang digunakan untuk memverifikasi tanda tangan file digest.
8. Validasi tanda tangan dengan meneruskan hash SHA-256 dari string, kunci publik, dan tanda tangan sebagai parameter ke algoritma verifikasi tanda tangan RSA. Jika hasilnya benar, file digest valid.

Validasi file log

Jika file digest valid, validasi setiap file log yang direferensikan file digest.

1. Untuk memvalidasi integritas file log, hitung nilai hash SHA-256 pada konten yang tidak terkompresi dan bandingkan hasilnya dengan hash untuk file log yang direkam dalam heksadesimal dalam intisari. Jika hash cocok, file log valid.
2. Dengan menggunakan informasi tentang file intisari sebelumnya yang disertakan dalam file intisari saat ini, validasi file intisari sebelumnya dan file log yang sesuai secara berurutan.

Bagian berikut menjelaskan langkah-langkah ini secara rinci.

A. Dapatkan file digest

Langkah pertama adalah mendapatkan file intisari terbaru, memverifikasi bahwa Anda telah mengambilnya dari lokasi aslinya, memverifikasi tanda tangan digitalnya, dan mendapatkan sidik jari kunci publik.

1. Menggunakan S3 `GetObject`atau kelas Amazons3Client (misalnya), dapatkan file intisari terbaru dari bucket Amazon S3 Anda untuk rentang waktu yang ingin Anda validasi.
2. Periksa apakah bucket S3 dan objek S3 yang digunakan untuk mengambil file cocok dengan lokasi objek S3 bucket S3 yang direkam dalam file digest itu sendiri.
3. Selanjutnya, dapatkan tanda tangan digital dari file digest dari properti `x-amz-meta-signature` metadata objek file digest di Amazon S3.
4. Dalam file digest, dapatkan sidik jari kunci publik yang kunci pribadinya digunakan untuk menandatangani file intisari dari bidang. `digestPublicKeyFingerprint`

B. Ambil kunci publik untuk memvalidasi file digest

Untuk mendapatkan kunci publik untuk memvalidasi file digest, Anda dapat menggunakan salah satu AWS CLI atau API. CloudTrail Dalam kedua kasus, Anda menentukan rentang waktu (yaitu, waktu mulai dan waktu akhir) untuk file intisari yang ingin Anda validasi. Satu atau beberapa kunci publik dapat dikembalikan untuk rentang waktu yang Anda tentukan. Kunci yang dikembalikan mungkin memiliki rentang waktu validitas yang tumpang tindih.

> **Note**
>
> Karena CloudTrail menggunakan pasangan private/public kunci yang berbeda per Wilayah, setiap file intisari ditandatangani dengan kunci pribadi yang unik untuk Wilayahnya. Oleh karena itu, ketika Anda memvalidasi file intisari dari Wilayah tertentu, Anda harus mengambil kunci publiknya dari Wilayah yang sama.

Gunakan tombol AWS CLI untuk mengambil kunci publik

Untuk mengambil kunci publik untuk mencerna file dengan menggunakan AWS CLI, gunakan perintah. `cloudtrail list-public-keys` Perintah memiliki format berikut:

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time
<end-time>]
```

Parameter waktu mulai dan akhir waktu adalah stempel waktu UTC dan bersifat opsional. Jika tidak ditentukan, waktu saat ini digunakan, dan kunci publik atau kunci yang saat ini aktif dikembalikan.

Sampel Respon

Responsnya akan berupa daftar objek JSON yang mewakili kunci (atau kunci) yang dikembalikan:


```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

Gunakan CloudTrail API untuk mengambil kunci publik

Untuk mengambil kunci publik untuk mencerna file dengan menggunakan CloudTrail API, teruskan nilai waktu mulai dan waktu akhir ke API. `ListPublicKeys` `ListPublicKeys`API mengembalikan kunci publik yang kunci pribadinya digunakan untuk menandatangani file intisari dalam rentang waktu yang ditentukan. Untuk setiap kunci publik, API juga mengembalikan sidik jari yang sesuai.

`ListPublicKeys`

Bagian ini menjelaskan parameter permintaan dan elemen respons untuk `ListPublicKeys` API.

> **Note**
>
> Pengkodean untuk bidang biner `ListPublicKeys` untuk dapat berubah.

Parameter Permintaan

Nama	Deskripsi
`StartTime`	Secara opsional menentukan, di UTC, awal rentang waktu untuk mencari kunci publik untuk file intisari. CloudTrail Jika tidak StartTime ditentukan, waktu saat ini digunakan, dan kunci publik saat ini dikembalikan. Jenis: DateTime
`EndTime`	Secara opsional menentukan, di UTC, akhir rentang waktu untuk mencari kunci publik untuk file intisari. CloudTrail Jika tidak EndTime ditentukan, waktu saat ini digunakan. Jenis: DateTime

Elemen Respon

`PublicKeyList`, array `PublicKey` objek yang berisi:

Nama	Deskripsi

`Value`	DER menyandikan nilai kunci publik dalam format PKCS #1. Jenis: Gumpalan
`ValidityStartTime`	Waktu mulai validitas kunci publik. Jenis: DateTime
`ValidityEndTime`	Waktu berakhirnya validitas kunci publik. Jenis: DateTime
`Fingerprint`	Sidik jari kunci publik. Sidik jari dapat digunakan untuk mengidentifikasi kunci publik yang harus Anda gunakan untuk memvalidasi file intisari. Tipe: String

C. Pilih kunci publik yang akan digunakan untuk validasi

Dari antara kunci publik yang diambil oleh `list-public-keys` atau`ListPublicKeys`, pilih kunci publik yang dikembalikan yang sidik jarinya cocok dengan sidik jari yang direkam di `digestPublicKeyFingerprint` bidang file intisari. Ini adalah kunci publik yang akan Anda gunakan untuk memvalidasi file digest.

D. Buat ulang string penandatanganan data

Sekarang setelah Anda memiliki tanda tangan file digest dan kunci publik terkait, Anda perlu menghitung string penandatanganan data. Setelah menghitung string penandatanganan data, Anda akan memiliki input yang diperlukan untuk memverifikasi tanda tangan.

String penandatanganan data memiliki format berikut:

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

Contoh `Data_To_Sign_String` berikut.

```
2015-08-12T04:01:31Z
amzn-s3-demo-bucket/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

Setelah Anda membuat ulang string ini, Anda dapat memvalidasi file digest.

E. Validasi file intisari

Lewati hash SHA-256 dari string penandatanganan data yang dibuat ulang, tanda tangan digital, dan kunci publik ke algoritma verifikasi tanda tangan RSA. Jika output benar, tanda tangan dari file digest diverifikasi dan file digest valid.

F. Validasi file log

Setelah Anda memvalidasi file intisari, Anda dapat memvalidasi file log yang direferensikannya. File DIGEST berisi hash SHA-256 dari file log. Jika salah satu file log diubah setelah CloudTrail dikirimkan, hash SHA-256 akan berubah, dan tanda tangan file digest tidak akan cocok.

Berikut ini menunjukkan bagaimana memvalidasi file log:

1. Lakukan file `S3 Get` log menggunakan informasi lokasi S3 di file digest `logFiles.s3Bucket` dan `logFiles.s30bject` bidang.
2. Jika `S3 Get` operasi berhasil, ulangi melalui file log yang tercantum dalam array LogFiles file digest menggunakan langkah-langkah berikut:
   a. Ambil hash asli file dari `logFiles.hashValue` bidang log yang sesuai dalam file digest.
   b. Hash konten yang tidak terkompresi dari file log dengan algoritma hashing yang ditentukan dalam. `logFiles.hashAlgorithm`
   c. Bandingkan nilai hash yang Anda hasilkan dengan nilai untuk log di file intisari. Jika hash cocok, file log valid.

G. Validasi intisari tambahan dan file log

Di setiap file intisari, bidang berikut menyediakan lokasi dan tanda tangan dari file intisari sebelumnya:

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

Gunakan informasi ini untuk mengunjungi file intisari sebelumnya secara berurutan, memvalidasi tanda tangan masing-masing dan file log yang mereka referensikan dengan menggunakan langkah-langkah di bagian sebelumnya. Satu-satunya perbedaan adalah bahwa untuk file intisari sebelumnya, Anda tidak perlu mengambil tanda tangan digital dari properti metadata Amazon S3 objek file intisari. Tanda tangan untuk file intisari sebelumnya disediakan untuk Anda di `previousDigestSignature` lapangan.

Anda dapat kembali sampai file intisari awal tercapai, atau sampai rantai file digest rusak, mana yang lebih dulu.

Memvalidasi file intisari dan log secara offline

Saat memvalidasi file intisari dan log secara offline, Anda biasanya dapat mengikuti prosedur yang dijelaskan di bagian sebelumnya. Namun, Anda harus mempertimbangkan bidang-bidang berikut:

Menangani file intisari terbaru

Tanda tangan digital dari file intisari terbaru (yaitu, “saat ini”) ada di properti metadata Amazon S3 dari objek file digest. Dalam skenario offline, tanda tangan digital untuk file intisari saat ini tidak akan tersedia.

Dua cara yang mungkin untuk menangani ini adalah:

- Karena tanda tangan digital untuk file intisari sebelumnya ada di file intisari saat ini, mulailah memvalidasi dari file intisari. next-to-last Dengan metode ini, file intisari terbaru tidak dapat divalidasi.
- Sebagai langkah awal, dapatkan tanda tangan untuk file intisari saat ini dari properti metadata objek file digest dan kemudian simpan secara offline dengan aman. Ini akan memungkinkan file intisari saat ini divalidasi selain file sebelumnya dalam rantai.

Resolusi jalur

Bidang dalam file intisari yang diunduh seperti `s3Object` dan masih `previousDigestS3Object` akan menunjuk ke lokasi online Amazon S3 untuk file log dan file cerna. Solusi offline harus menemukan cara untuk mengubah rute ini ke jalur log dan mencerna file yang diunduh saat ini.

Kunci publik

Untuk memvalidasi offline, semua kunci publik yang Anda butuhkan untuk memvalidasi file log dalam rentang waktu tertentu harus diperoleh terlebih dahulu secara online (dengan meneleponListPublicKeys, misalnya) dan kemudian disimpan secara offline dengan aman. Langkah ini harus diulang setiap kali Anda ingin memvalidasi file tambahan di luar rentang waktu awal yang Anda tentukan.

Contoh cuplikan validasi

Contoh cuplikan berikut menyediakan kode kerangka untuk memvalidasi file CloudTrail digest dan log. Kode kerangka online/offline agnostik; artinya, terserah Anda untuk memutuskan apakah akan menerapkannya dengan atau tanpa konektivitas online ke. AWS Implementasi yang disarankan menggunakan Java Cryptography Extension (JCE) dan Bouncy Castle sebagai penyedia keamanan.

Cuplikan sampel menunjukkan:

- Cara membuat string penandatanganan data yang digunakan untuk memvalidasi tanda tangan file digest.
- Cara memverifikasi tanda tangan file digest.
- Cara memverifikasi hash file log.
- Struktur kode untuk memvalidasi rantai file intisari.

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;

public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {
```

```
        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
 as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
 ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
 file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:

                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }
```

```
                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
```

```
                    byte[] expectedHash =
 Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail contoh file log

CloudTrail memantau acara untuk akun Anda. Jika Anda membuat jejak, itu mengirimkan peristiwa tersebut sebagai file log ke bucket Amazon S3 Anda. Jika Anda membuat penyimpanan data acara di

CloudTrail Lake, peristiwa dicatat ke penyimpanan data acara Anda. Penyimpanan data acara tidak menggunakan bucket S3.

Topik

- CloudTrail format nama file log
- Contoh file log

CloudTrail format nama file log

CloudTrail menggunakan format nama file berikut untuk objek file log yang dikirimkan ke bucket Amazon S3 Anda:

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- Itu YYYYMM,DD,HH,, dan mm merupakan digit tahun, bulan, hari, jam, dan menit ketika file log dikirim. Jam dalam format 24 jam. ZIni menunjukkan bahwa waktunya dalam UTC.

  > **Note**
  >
  > Berkas log yang dikirimkan pada waktu tertentu dapat berisi catatan yang ditulis kapan pun sebelum waktu tersebut.

- `UniqueString`Komponen 16 karakter dari nama file log ada untuk mencegah penimpaan file. Tidak memiliki makna, dan perangkat lunak pemroses log harus mengabaikannya.
- `FileNameFormat`adalah pengkodean file. Saat ini, ini adalah`json.gz`, yang merupakan file teks JSON dalam format gzip terkompresi.

Contoh Nama File CloudTrail Log

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

Contoh file log

File log berisi satu atau lebih catatan. Contoh berikut adalah cuplikan log yang menunjukkan catatan untuk tindakan yang memulai pembuatan file log.

Untuk informasi tentang bidang catatan CloudTrail peristiwa, lihatCloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.

Daftar Isi

- Contoh log Amazon EC2
- Contoh log IAM
- Kode kesalahan dan contoh log pesan
- CloudTrail Contoh log peristiwa wawasan

Contoh log Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) menyediakan kapasitas komputasi yang dapat diubah ukurannya dalam format. AWS Cloud Anda dapat meluncurkan server virtual, mengkonfigurasi keamanan dan jaringan, dan mengelola penyimpanan. Amazon EC2 juga dapat meningkatkan atau menurunkan skala dengan cepat untuk menangani perubahan persyaratan atau lonjakan popularitas, sehingga mengurangi kebutuhan Anda untuk memperkirakan lalu lintas server. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon EC2.

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Mateo` menjalankan aws ec2 start-instances perintah untuk memanggil tindakan Amazon `StartInstances`EC2 untuk `i-EXAMPLE56126103cb` instance dan. `i-EXAMPLEaff4840c22`


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
```

```
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Nikki` menjalankan aws ec2 stop-instances perintah untuk memanggil tindakan Amazon `StopInstances`EC2 untuk menghentikan dua instance.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
```

```
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
```

```
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Arnav` menjalankan aws ec2 create-key-pair perintah untuk memanggil `CreateKeyPair`tindakan. Perhatikan bahwa `responseElements` mengandung hash dari key pair dan yang AWS menghapus materi kunci.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


Contoh log IAM

AWS Identity and Access Management (IAM) adalah layanan web yang membantu Anda mengontrol akses ke AWS sumber daya dengan aman. Dengan IAM, Anda dapat mengelola izin secara terpusat yang mengendalikan sumber daya AWS yang dapat diakses pengguna. Anda menggunakan IAM untuk mengontrol siapa yang dapat terautentikasi (masuk) dan berwenang (memiliki izin) untuk menggunakan sumber daya. Untuk informasi selengkapnya, lihat Panduan Pengguna IAM.

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Mary` menjalankan aws iam create-user perintah untuk memanggil `CreateUser`tindakan untuk membuat pengguna baru bernama`Richard`.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
```

```
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Paulo` menjalankan aws iam add-user-to-group perintah untuk memanggil AddUserToGrouptindakan untuk menambahkan pengguna bernama `Jane` ke `Admin` grup.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
```

```
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Saanvi` menjalankan aws iam create-role perintah untuk memanggil `CreateRole`tindakan untuk membuat peran.

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
```

```
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",       \"Statement
\":[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "policy-statement",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


Kode kesalahan dan contoh log pesan

Contoh berikut menunjukkan bahwa pengguna IAM bernama `Terry` menjalankan aws cloudtrail update-trail perintah untuk memanggil `UpdateTrail`tindakan untuk memperbarui jejak bernamamy`Trail2`, tetapi nama jejak tidak ditemukan. Log menunjukkan kesalahan ini di `errorMessage` elemen `errorCode` dan.


```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail Contoh log peristiwa wawasan

Contoh berikut menunjukkan log peristiwa CloudTrail Insights. Peristiwa Insights sebenarnya adalah sepasang peristiwa yang menandai awal dan akhir periode aktivitas API manajemen tulis yang tidak biasa atau aktivitas respons kesalahan. `state`Bidang menunjukkan apakah acara dicatat pada awal atau akhir periode aktivitas yang tidak biasa. Nama acara,`UpdateInstanceInformation`, adalah nama yang sama dengan AWS Systems Manager API yang CloudTrail menganalisis peristiwa manajemen untuk menentukan bahwa aktivitas yang tidak biasa terjadi. Meskipun peristiwa awal dan akhir memiliki `eventID` nilai unik, mereka juga memiliki `sharedEventID` nilai yang digunakan oleh pasangan. Peristiwa Insights menunjukkan`baseline`, atau pola aktivitas normal`insight`, atau rata-rata aktivitas tidak biasa yang memicu peristiwa Wawasan awal, dan pada akhirnya peristiwa, `insight` nilai rata-rata aktivitas yang tidak biasa selama durasi acara Wawasan. Untuk informasi selengkapnya tentang CloudTrail Wawasan, lihatBekerja dengan CloudTrail Wawasan.


```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
```

```
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```


Menggunakan Pustaka CloudTrail Pemrosesan

CloudTrail Processing Library adalah perpustakaan Java yang menyediakan cara mudah untuk memproses AWS CloudTrail log. Anda memberikan detail konfigurasi tentang antrian CloudTrail SQS Anda dan menulis kode untuk memproses peristiwa. Perpustakaan CloudTrail Pemrosesan melakukan sisanya. Ini polling antrian Amazon SQS Anda, membaca dan mengurai pesan antrian, CloudTrail mengunduh file log, mem-parsing peristiwa dalam file log, dan meneruskan peristiwa ke kode Anda sebagai objek Java.

Perpustakaan CloudTrail Pemrosesan sangat skalabel dan toleran terhadap kesalahan. Ini menangani pemrosesan paralel file log sehingga Anda dapat memproses log sebanyak yang

diperlukan. Ini menangani kegagalan jaringan yang terkait dengan batas waktu jaringan dan sumber daya yang tidak dapat diakses.

Topik berikut menunjukkan cara menggunakan Pustaka CloudTrail Pemrosesan untuk memproses CloudTrail log di proyek Java Anda.

Perpustakaan disediakan sebagai proyek sumber terbuka berlisensi Apache, tersedia di:. GitHub https://github.com/aws/aws-cloudtrail-processing-library Sumber pustaka menyertakan kode contoh yang dapat Anda gunakan sebagai basis untuk proyek Anda sendiri.

Topik

- Persyaratan minimum
- Memproses CloudTrail log
- Topik lanjutan
- Sumber daya tambahan

Persyaratan minimum

Untuk menggunakan Pustaka CloudTrail Pemrosesan, Anda harus memiliki yang berikut:

- AWS SDK untuk Java 1.11.830
- Java 1.8 (Jawa SE 8)

Memproses CloudTrail log

Untuk memproses CloudTrail log di aplikasi Java Anda:

1. Menambahkan Pustaka CloudTrail Pemrosesan ke proyek Anda
2. Mengkonfigurasi Pustaka CloudTrail Pemrosesan
3. Menerapkan prosesor acara
4. Membuat instantiasi dan menjalankan pelaksana pemrosesan

Menambahkan Pustaka CloudTrail Pemrosesan ke proyek Anda

Untuk menggunakan CloudTrail Processing Library, tambahkan ke classpath proyek Java Anda.

Daftar Isi

- Menambahkan perpustakaan ke proyek Apache Ant
- Menambahkan perpustakaan ke proyek Apache Maven
- Menambahkan perpustakaan ke proyek Eclipse
- Menambahkan pustaka ke proyek IntelliJ

Menambahkan perpustakaan ke proyek Apache Ant

Untuk menambahkan Perpustakaan CloudTrail Pemrosesan ke proyek Apache Ant

1. Unduh atau kloning kode sumber Perpustakaan CloudTrail Pemrosesan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Buat file.jar dari sumber seperti yang dijelaskan dalam README:

```
mvn clean install -Dgpg.skip=true
```

3. Salin file.jar yang dihasilkan ke proyek Anda dan tambahkan ke `build.xml` file proyek Anda. Contoh:

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Menambahkan perpustakaan ke proyek Apache Maven

Perpustakaan CloudTrail Pemrosesan tersedia untuk Apache Maven. Anda dapat menambahkannya ke proyek Anda dengan menulis dependensi tunggal dalam `pom.xml` file proyek Anda.

Untuk menambahkan Perpustakaan CloudTrail Pemrosesan ke proyek Maven

- Buka `pom.xml` file proyek Maven Anda dan tambahkan dependensi berikut:

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
```

```
</dependency>
```

Menambahkan perpustakaan ke proyek Eclipse

Untuk menambahkan Perpustakaan CloudTrail Pemrosesan ke proyek Eclipse

1. Unduh atau kloning kode sumber Perpustakaan CloudTrail Pemrosesan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Buat file.jar dari sumber seperti yang dijelaskan dalam README:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Salin aws-cloudtrail-processing-library -1.6.1.jar yang dibangun ke direktori di proyek Anda (biasanya). `lib`
4. Klik kanan nama proyek Anda di Eclipse Project Explorer, pilih Build Path, lalu pilih Configure
5. Di jendela Java Build Path, pilih tab Libraries.
6. Pilih Tambah JARs... dan arahkan ke jalur tempat Anda menyalin aws-cloudtrail-processing-library -1.6.1.jar.
7. Pilih OK untuk menyelesaikan penambahan `.jar` ke proyek Anda.

Menambahkan pustaka ke proyek IntelliJ

Untuk menambahkan Pustaka CloudTrail Pemrosesan ke proyek IntelliJ

1. Unduh atau kloning kode sumber Perpustakaan CloudTrail Pemrosesan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Buat file.jar dari sumber seperti yang dijelaskan dalam README:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Dari File, pilih Project Structure.
4. Pilih Modul dan kemudian pilih Dependensi.
5. Pilih + JARS atau Direktori dan kemudian pergi ke jalur di mana Anda membangun. `aws-cloudtrail-processing-library-1.6.1.jar`
6. Pilih Terapkan dan kemudian pilih OK untuk menyelesaikan penambahan `.jar` ke proyek Anda.

Mengkonfigurasi Pustaka CloudTrail Pemrosesan

Anda dapat mengonfigurasi Pustaka CloudTrail Pemrosesan dengan membuat file properti classpath yang dimuat saat runtime, atau dengan membuat `ClientConfiguration` objek dan opsi pengaturan secara manual.

Menyediakan file properti

Anda dapat menulis file properti classpath yang menyediakan opsi konfigurasi untuk aplikasi Anda. File contoh berikut menunjukkan opsi yang dapat Anda atur:

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10
```

```
# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

Parameter-parameter berikut diperlukan:

- `sqsUrl`— Menyediakan URL untuk menarik CloudTrail notifikasi Anda. Jika Anda tidak menentukan nilai ini, `AWSCloudTrailProcessingExecutor` melempar`IllegalStateException`.
- `accessKey`— Pengenal unik untuk akun Anda, sepertiAKIAIOSFODNN7EXAMPLE.
- `secretKey`— Pengenal unik untuk akun Anda, sepertiwJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

`secretKey`Parameter `accessKey` dan menyediakan AWS kredensyal Anda ke perpustakaan sehingga perpustakaan dapat mengakses AWS atas nama Anda.

Default untuk parameter lain diatur oleh perpustakaan. Untuk informasi selengkapnya, lihat Referensi Perpustakaan AWS CloudTrail Pemrosesan.

Menciptakan ClientConfiguration

Alih-alih mengatur opsi di properti classpath, Anda dapat memberikan opsi ke `AWSCloudTrailProcessingExecutor` dengan menginisialisasi dan menyetel opsi pada `ClientConfiguration` objek, seperti yang ditunjukkan pada contoh berikut:

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

Menerapkan prosesor acara

Untuk memproses CloudTrail log, Anda harus menerapkan `EventsProcessor` yang menerima data CloudTrail log. Berikut ini adalah contoh implementasi:

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

Saat menerapkan`EventsProcessor`, Anda menerapkan `process()` callback yang `AWSCloudTrailProcessingExecutor` digunakan untuk mengirimi Anda CloudTrail peristiwa. Acara disediakan dalam daftar `CloudTrailClientEvent` objek.

`CloudTrailClientEvent`Objek menyediakan `CloudTrailEvent` dan `CloudTrailEventMetadata` yang dapat Anda gunakan untuk membaca CloudTrail acara dan informasi pengiriman.

Contoh sederhana ini mencetak informasi acara untuk setiap acara yang diteruskan ke`SampleEventsProcessor`. Dalam implementasi Anda sendiri, Anda dapat memproses log sesuai keinginan Anda. `AWSCloudTrailProcessingExecutor`Terus mengirim acara ke Anda `EventsProcessor` selama ada acara untuk dikirim dan masih berjalan.

Membuat instantiasi dan menjalankan pelaksana pemrosesan

Setelah Anda menulis `EventsProcessor` dan menetapkan nilai konfigurasi untuk Pustaka CloudTrail Pemrosesan (baik dalam file properti atau dengan menggunakan `ClientConfiguration` kelas), Anda dapat menggunakan elemen-elemen ini untuk menginisialisasi dan menggunakan file`AWSCloudTrailProcessingExecutor`.

Untuk digunakan **`AWSCloudTrailProcessingExecutor`** untuk memproses CloudTrail acara

1. Instantiate sebuah objek. `AWSCloudTrailProcessingExecutor.Builder` `Builder`konstruktor mengambil `EventsProcessor` objek dan nama file properti classpath.
2. Panggil metode `build()` pabrik untuk mengkonfigurasi dan mendapatkan `AWSCloudTrailProcessingExecutor` objek. `Builder`
3. Gunakan `AWSCloudTrailProcessingExecutor`'s `start()` dan `stop()` metode untuk memulai dan mengakhiri pemrosesan CloudTrail acara.

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

Topik lanjutan

Topik

- Memfilter acara untuk diproses
- Memproses peristiwa data
- Melaporkan kemajuan
- Menangani kesalahan

Memfilter acara untuk diproses

Secara default, semua log di bucket S3 antrean Amazon SQS Anda dan semua peristiwa yang dikandungnya dikirim ke Anda. `EventsProcessor` Perpustakaan CloudTrail Pemrosesan menyediakan antarmuka opsional yang dapat Anda terapkan untuk memfilter sumber yang digunakan untuk mendapatkan CloudTrail log dan untuk memfilter peristiwa yang Anda minati untuk diproses.

`SourceFilter`

Anda dapat menerapkan `SourceFilter` antarmuka untuk memilih apakah Anda ingin memproses log dari sumber yang disediakan. `SourceFilter`mendeklarasikan metode callback tunggal,`filterSource()`, yang menerima objek. `CloudTrailSource` Untuk menjaga agar acara dari sumber tidak diproses, kembalilah `false` dari`filterSource()`.

Pustaka CloudTrail Pemrosesan memanggil `filterSource()` metode setelah library melakukan polling untuk log pada antrean Amazon SQS. Ini terjadi sebelum pustaka memulai pemfilteran peristiwa atau pemrosesan untuk log.

Berikut ini adalah contoh implementasi:

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

Jika Anda tidak menyediakan sendiri`SourceFilter`, maka `DefaultSourceFilter` digunakan, yang memungkinkan semua sumber diproses (selalu kembali`true`).

`EventFilter`

Anda dapat menerapkan `EventFilter` antarmuka untuk memilih apakah suatu CloudTrail acara dikirim ke Anda`EventsProcessor`. `EventFilter`mendeklarasikan metode callback tunggal,`filterEvent()`, yang menerima objek. `CloudTrailEvent` Agar acara tidak diproses, kembalilah `false` dari`filterEvent()`.

Pustaka CloudTrail Pemrosesan memanggil `filterEvent()` metode setelah pustaka melakukan polling untuk log pada antrean Amazon SQS dan setelah pemfilteran sumber. Ini terjadi sebelum pustaka memulai pemrosesan peristiwa untuk log.

Lihat contoh implementasi berikut:

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

Jika Anda tidak menyediakan milik Anda sendiri`EventFilter`, maka `DefaultEventFilter` digunakan, yang memungkinkan semua acara diproses (selalu kembali`true`).

Memproses peristiwa data

Ketika CloudTrail memproses peristiwa data, ia mempertahankan angka dalam format aslinya, apakah itu integer (`int`) atau `float` (angka yang berisi desimal). Dalam peristiwa yang memiliki bilangan bulat di bidang peristiwa data, CloudTrail secara historis memproses angka-angka ini sebagai pelampung. Saat ini, CloudTrail memproses angka di bidang ini dengan mempertahankan format aslinya.

Sebagai praktik terbaik, untuk menghindari kerusakan otomatisasi Anda, bersikaplah fleksibel dalam kode atau otomatisasi apa pun yang Anda gunakan untuk memproses atau memfilter peristiwa CloudTrail data, dan izinkan keduanya `int` dan angka yang `float` diformat. Untuk hasil terbaik, gunakan Pustaka CloudTrail Pemrosesan versi 1.4.0 atau lebih tinggi.

Contoh cuplikan berikut menunjukkan nomor `float` diformat,`2.0`, untuk `desiredCount` parameter di `ResponseParameters` blok peristiwa data.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
```

```
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

Contoh cuplikan berikut menunjukkan nomor `int` diformat,2, untuk `desiredCount` parameter di `ResponseParameters` blok peristiwa data.

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

Melaporkan kemajuan

Menerapkan `ProgressReporter` antarmuka untuk menyesuaikan pelaporan kemajuan Perpustakaan CloudTrail Pemrosesan. `ProgressReporter`menyatakan dua metode: `reportStart()` dan`reportEnd()`, yang disebut di awal dan akhir operasi berikut:

- Pesan polling dari Amazon SQS
- Mengurai pesan dari Amazon SQS
- Memproses sumber Amazon SQS untuk log CloudTrail
- Menghapus pesan dari Amazon SQS
- Mengunduh file CloudTrail log
- Memproses file CloudTrail log

Kedua metode menerima `ProgressStatus` objek yang berisi informasi tentang operasi yang dilakukan. `progressState`Anggota memegang anggota `ProgressState` enumerasi yang mengidentifikasi operasi saat ini. Anggota ini dapat berisi informasi tambahan dalam `progressInfo` anggota. Selain itu, objek apa pun yang Anda kembalikan `reportStart()` diteruskan ke`reportEnd()`, sehingga Anda dapat memberikan informasi kontekstual seperti waktu ketika acara mulai diproses.

Berikut ini adalah contoh implementasi yang memberikan informasi tentang berapa lama operasi selesai:

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

Jika Anda tidak mengimplementasikan milik Anda sendiri `ProgressReporterDefaultExceptionHandler`, maka, yang mencetak nama status yang sedang dijalankan, digunakan sebagai gantinya.

Menangani kesalahan

`ExceptionHandler`Antarmuka memungkinkan Anda untuk memberikan penanganan khusus ketika pengecualian terjadi selama pemrosesan log. `ExceptionHandler`mendeklarasikan metode callback tunggal`handleException()`,, yang menerima `ProcessingLibraryException` objek dengan konteks tentang pengecualian yang terjadi.

Anda dapat menggunakan `getStatus()` metode `ProcessingLibraryException` passed-in untuk mengetahui operasi apa yang dijalankan ketika pengecualian terjadi dan mendapatkan informasi tambahan tentang status operasi. `ProcessingLibraryException`berasal dari `Exception` kelas standar Java, sehingga Anda juga dapat mengambil informasi tentang pengecualian dengan menggunakan salah satu metode pengecualian.

Lihat contoh implementasi berikut:

```
public class SampleExceptionHandler implements ExceptionHandler{
```

```
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

Jika Anda tidak menyediakan sendiri`ExceptionHandler`, maka`DefaultExceptionHandler`, yang mencetak pesan kesalahan standar, digunakan sebagai gantinya.

> **Note**
>
> Jika `deleteMessageUponFailure` parameternya`true`, Pustaka CloudTrail Pemrosesan tidak membedakan pengecualian umum dari kesalahan pemrosesan dan dapat menghapus pesan antrian.
>
> 1. Misalnya, Anda menggunakan `SourceFilter` untuk memfilter pesan berdasarkan stempel waktu.
> 2. Namun, Anda tidak memiliki izin yang diperlukan untuk mengakses bucket S3 yang menerima file CloudTrail log. Karena Anda tidak memiliki izin yang diperlukan, sebuah `AmazonServiceException` dilemparkan. Perpustakaan CloudTrail Pemrosesan membungkus ini dalam a. `CallBackException`
> 3. `DefaultExceptionHandler`Mencatat ini sebagai kesalahan, tetapi tidak mengidentifikasi akar penyebabnya, yaitu Anda tidak memiliki izin yang diperlukan. Pustaka CloudTrail Pemrosesan menganggap ini sebagai kesalahan pemrosesan dan menghapus pesan, meskipun pesan tersebut menyertakan file CloudTrail log yang valid.
>
> Jika Anda ingin memfilter pesan`SourceFilter`, verifikasi bahwa Anda `ExceptionHandler` dapat membedakan pengecualian layanan dari kesalahan pemrosesan.

Sumber daya tambahan

Untuk informasi selengkapnya tentang Pustaka CloudTrail Pemrosesan, lihat berikut ini:

- CloudTrail Processing Library GitHub project, yang mencakup contoh kode yang menunjukkan bagaimana menerapkan aplikasi CloudTrail Processing Library.
- CloudTrail Memproses Perpustakaan Java Package Documentation.

Keamanan di AWS CloudTrail

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 menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di 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 berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku AWS CloudTrail, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

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

Topik

- Perlindungan data di AWS CloudTrail
- Identity and Access Management untuk AWS CloudTrail
- Validasi kepatuhan untuk AWS CloudTrail
- Ketahanan di AWS CloudTrail
- Keamanan infrastruktur di AWS CloudTrail
- Pencegahan "confused deputy" lintas layanan
- Praktik terbaik keamanan di AWS CloudTrail
- Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS)

Perlindungan data di AWS CloudTrail

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS CloudTrail. 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. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data AWS . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Perlindungan Data Umum (GDPR).

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan 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 CloudTrail atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

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

Secara default, file log CloudTrail peristiwa dan file intisari dienkripsi menggunakan enkripsi sisi server Amazon S3 (SSE). Anda juga dapat memilih untuk mengenkripsi file log Anda dan mencerna file dengan kunci AWS Key Management Service (AWS KMS). Anda dapat menyimpan file log Anda di ember Anda selama yang Anda inginkan. Anda juga dapat mendefinisikan aturan siklus hidup Amazon S3 untuk mengarsipkan atau menghapus berkas log secara otomatis. Jika ingin pemberitahuan tentang pengiriman dan validasi file log, Anda dapat mengatur notifikasi Amazon SNS.

Praktik terbaik keamanan berikut juga membahas perlindungan data di CloudTrail:

- Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS)
- Kebijakan bucket Amazon S3 untuk CloudTrail
- Memvalidasi CloudTrail integritas file log
- Berbagi file CloudTrail log antar AWS akun

Karena file CloudTrail log disimpan dalam bucket atau bucket di Amazon S3, Anda juga harus meninjau informasi perlindungan data di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Untuk informasi selengkapnya, lihat Perlindungan data di Amazon S3.

Identity and Access Management untuk AWS CloudTrail

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 di otorisasi (memiliki izin) untuk menggunakan CloudTrail sumber daya. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan

- Bagaimana AWS CloudTrail bekerja dengan IAM
- Identity-based Contoh kebijakan untuk AWS CloudTrail
- AWS CloudTrail contoh kebijakan berbasis sumber daya
- Kebijakan bucket Amazon S3 untuk CloudTrail
- Kebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake
- Kebijakan topik Amazon SNS untuk CloudTrail
- Pemecahan masalah AWS CloudTrail Identitas dan Akses
- Menggunakan peran terkait layanan untuk CloudTrail
- AWS kebijakan terkelola untuk AWS CloudTrail

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 Pemecahan masalah AWS CloudTrail Identitas dan Akses)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana AWS CloudTrail bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based Contoh kebijakan untuk AWS CloudTrail)

Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau 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 menyediakan SDK dan CLI untuk menandatangani permintaan kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

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.

Identitas terfederasi

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

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

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

Pengguna dan grup IAM

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

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

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI 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 melakukan operasinya.

Identity-based kebijakan

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

Identity-based kebijakan dapat berupa kebijakan sebaris (disematkan langsung ke dalam satu identitas) atau kebijakan ter kelola (kebijakan mandiri yang dilampirkan ke beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

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

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

Jenis-jenis kebijakan lain

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

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

Berbagai jenis kebijakan

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

Bagaimana AWS CloudTrail bekerja dengan IAM

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

Fitur IAM yang dapat Anda gunakan AWS CloudTrail

Fitur IAM	CloudTrail dukungan
Identity-based kebijakan	Ya

Fitur IAM	CloudTrail dukungan
Resource-based kebijakan	Parsial
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Tidak
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Service-linked peran	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara CloudTrail dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk CloudTrail

Mendukung kebijakan berbasis identitas: Ya

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

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya

tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Identity-based Contoh kebijakan untuk CloudTrail

Untuk melihat contoh kebijakan CloudTrail berbasis identitas, lihat. Identity-based Contoh kebijakan untuk AWS CloudTrail

Resource-based kebijakan di dalam CloudTrail

Mendukung kebijakan berbasis sumber daya: Sebagian

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

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

CloudTrail mendukung jenis kebijakan berbasis sumber daya berikut:

- Resource-based kebijakan tentang saluran yang digunakan untuk integrasi CloudTrail Danau dengan sumber acara di luar. AWS Kebijakan berbasis sumber daya untuk saluran menentukan entitas utama (akun, pengguna, peran, dan pengguna federasi) mana yang dapat memanggil `PutAuditEvents` saluran untuk mengirimkan peristiwa ke penyimpanan data peristiwa tujuan. Untuk informasi selengkapnya tentang membuat integrasi dengan CloudTrail Lake, lihatBuat integrasi dengan sumber acara di luar AWS.
- Resource-based kebijakan untuk mengontrol kepala sekolah mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Anda dapat menggunakan kebijakan berbasis sumber daya untuk menyediakan akses lintas akun ke penyimpanan data acara Anda.
- Resource-based kebijakan pada dasbor CloudTrail untuk memungkinkan penyegaran dasbor CloudTrail Lake pada interval yang Anda tentukan saat Anda menetapkan jadwal penyegaran

untuk dasbor. Untuk informasi selengkapnya, lihat Tetapkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol.

Contoh

Untuk melihat contoh kebijakan CloudTrail berbasis sumber daya, lihat. AWS CloudTrail contoh kebijakan berbasis sumber daya

Tindakan kebijakan untuk CloudTrail

Mendukung tindakan kebijakan: Ya

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.

Untuk melihat daftar CloudTrail tindakan, lihat Tindakan yang D itetapkan oleh AWS CloudTrail dalam Referensi Otorisasi Layanan.

Tindakan kebijakan CloudTrail menggunakan awalan berikut sebelum tindakan:

```
cloudtrail
```

Misalnya, untuk memberi seseorang izin untuk mencantumkan tag untuk jejak dengan operasi `ListTags` API, Anda menyertakan `cloudtrail:ListTags` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus menyertakan elemen `Action` atau `NotAction`. CloudTrail menentukan set tindakan sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut menggunakan koma seperti berikut:

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
```

```
      "cloudtrail:RemoveTags
```

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "cloudtrail:Get*"
```

Sumber daya kebijakan untuk CloudTrail

Mendukung sumber daya kebijakan: Ya

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": "*"
```

Untuk melihat daftar jenis CloudTrail sumber daya dan ARN-nya, lihat Sumber Daya yang Ditet apkan oleh AWS CloudTrail dalam Refer ensi O torisasi Layanan. Untuk mempelajari dengan tindakan mana Anda dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS CloudTrail.

Di CloudTrail, ada empat jenis sumber daya: jejak, penyimpanan data peristiwa, dasbor, dan saluran. Setiap sumber daya memiliki Nama Sumber Daya Amazon (ARN) unik yang terkait dengannya. Dalam kebijakan, Anda menggunakan ARN untuk mengidentifikasi sumber daya yang diterapkan kebijakan tersebut. CloudTrail saat ini tidak mendukung jenis sumber daya lain, yang kadang-kadang disebut sebagai subresource.

Sumber daya CloudTrail jejak memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

Sumber daya penyimpanan data CloudTrail peristiwa memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

Sumber daya CloudTrail dasbor memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/{DashboardName}
```

Sumber daya CloudTrail saluran memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

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

Misalnya, untuk sebuah Akun AWS dengan ID*123456789012*, untuk menentukan jejak bernama *My-Trail* yang ada di Wilayah AS Timur (Ohio) dalam pernyataan Anda, gunakan ARN berikut:

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

Untuk menentukan semua jalur yang dimiliki akun tertentu di dalamnya Wilayah AWS, gunakan wildcard (*):

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

Beberapa CloudTrail tindakan, seperti untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Banyak tindakan CloudTrail API melibatkan banyak sumber daya. Misalnya, `CreateTrail` memerlukan bucket Amazon S3 untuk menyimpan file log, sehingga pengguna harus memiliki izin untuk menulis ke bucket. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARN dengan koma.

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

```
    "resource2"
```

Kunci kondisi kebijakan untuk CloudTrail

Mendukung kunci kondisi kebijakan khusus layanan: Tidak

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.

CloudTrail tidak menentukan kunci kondisinya sendiri, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat K AWS unci Konteks Kondisi Global di Panduan Pengguna IAM.

Untuk melihat daftar kunci CloudTrail kondisi, lihat Kunci Kondisi untuk AWS CloudTrail di Referensi O torisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana Anda dapat menggunakan kunci kondisi, lihat Tindakan yang Ditetapkan oleh AWS CloudTrail.

ACL dalam CloudTrail

Mendukung ACL: Tidak

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

ABAC dengan CloudTrail

Mendukung ABAC (tanda dalam kebijakan): Ya

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

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

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

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

Anda dapat melampirkan tag ke CloudTrail sumber daya atau meneruskan tag dalam permintaan ke CloudTrail. Untuk informasi selengkapnya tentang menandai CloudTrail sumber daya, lihat Membuat jejak dengan CloudTrail konsol danMembuat, memperbarui, dan mengelola jalur dengan AWS CLI.

Menggunakan kredenSIAL sementara dengan CloudTrail

Mendukung kredensial sementara: Ya

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

Teruskan sesi akses untuk CloudTrail

Mendukung sesi akses terusan (FAS): Ya

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

Peran layanan untuk CloudTrail

Mendukung peran layanan: Ya

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

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fung CloudTrail sionalitas. Edit peran layanan hanya jika CloudTrail memberikan panduan untuk melakukannya.

Service-linked peran untuk CloudTrail

Mendukung peran terkait layanan: Ya

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

CloudTrail mendukung peran terkait layanan untuk integrasi dengan. AWS Organizations Peran ini diperlukan untuk pembuatan jejak organisasi atau penyimpanan data acara. Jejak organisasi dan data peristiwa menyimpan peristiwa log untuk semua Akun AWS dalam organisasi. Untuk informasi selengkapnya tentang membuat atau mengelola CloudTrail peran terkait layanan, lihat. Menggunakan peran terkait layanan untuk CloudTrail

Identity-based Contoh kebijakan untuk AWS CloudTrail

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

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh CloudTrail, termasuk format ARN untuk setiap jenis sumber daya, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS CloudTrail di Refer ensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Contoh: Mengizinkan dan menolak tindakan untuk jejak tertentu
- Contoh: Membuat dan menerapkan kebijakan untuk tindakan pada jalur tertentu

- Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag
- Menggunakan CloudTrail konsol
- Izinkan para pengguna untuk melihat izin mereka sendiri
- Memberikan izin khusus untuk CloudTrail pengguna

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus CloudTrail 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:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS ola 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 kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah

ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root 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.

CloudTrail tidak memiliki kunci konteks khusus layanan yang dapat Anda gunakan dalam `Condition` elemen pernyataan kebijakan.

Contoh: Mengizinkan dan menolak tindakan untuk jejak tertentu

Contoh berikut menunjukkan kebijakan yang memungkinkan pengguna dengan kebijakan untuk melihat status dan konfigurasi jejak serta memulai dan menghentikan pencatatan untuk jejak bernama*My-First-Trail*. Jejak ini dibuat di Wilayah AS Timur (Ohio) (Wilayah asalnya) Akun AWS dengan ID*123456789012*.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
```

```
            ]
        }
    ]
}
```

Contoh berikut menunjukkan kebijakan yang secara eksplisit menolak CloudTrail tindakan untuk jejak apa pun yang tidak diberi nama*My-First-Trail*.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

Contoh: Membuat dan menerapkan kebijakan untuk tindakan pada jalur tertentu

Anda dapat menggunakan izin dan kebijakan untuk mengontrol kemampuan pengguna untuk melakukan tindakan tertentu di CloudTrail jalur.

Misalnya, Anda tidak ingin pengguna grup pengembang perusahaan Anda memulai atau menghentikan log pada jejak tertentu. Namun, Anda mungkin ingin memberi mereka izin untuk melakukan `GetTrailStatus` tindakan `DescribeTrails` dan di jalan setapak. Anda ingin pengguna grup pengembang melakukan `StopLogging` tindakan `StartLogging` atau pada jalur yang mereka kelola.

Anda dapat membuat dua pernyataan kebijakan dan melampirkannya ke grup pengembang yang Anda buat di IAM. Untuk informasi selengkapnya tentang grup di IAM, lihat Grup IAM di Panduan Pengguna IAM.

Dalam kebijakan pertama, Anda menolak `StopLogging` tindakan `StartLogging` dan untuk jejak ARN yang Anda tentukan. Dalam contoh berikut, jejak ARN adalah`arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

Dalam kebijakan kedua, `GetTrailStatus` tindakan `DescribeTrails` dan diizinkan pada semua CloudTrail sumber daya:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
            "Resource": [
```

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

Jika pengguna grup pengembang mencoba memulai atau menghentikan pencatatan pada jejak yang Anda tentukan dalam kebijakan pertama, pengguna tersebut akan mendapatkan pengecualian akses ditolak. Pengguna grup pengembang dapat memulai dan menghentikan pencatatan pada jalur yang mereka buat dan kelola.

Contoh berikut menunjukkan bahwa grup pengembang yang dikonfigurasi dalam AWS CLI profil bernama`devgroup`. Pertama, pengguna `devgroup` menjalankan `describe-trails` perintah.

```
$ aws --profile devgroup cloudtrail describe-trails
```

Perintah selesai dengan sukses dengan output berikut:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "amzn-s3-demo-bucket",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

Pengguna kemudian menjalankan `get-trail-status` perintah pada jejak yang Anda tentukan dalam kebijakan pertama.

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

Perintah selesai dengan sukses dengan output berikut:

```
{
```

```
    "LatestDeliveryTime": 1449517556.256,
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

Selanjutnya, pengguna dalam `devgroup` grup menjalankan `stop-logging` perintah pada jejak yang sama.

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

Perintah mengembalikan pengecualian akses ditolak, seperti berikut ini:

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

Pengguna menjalankan `start-logging` perintah di jalur yang sama.

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

Sekali lagi perintah mengembalikan pengecualian akses ditolak, seperti berikut ini:

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag

Dalam contoh kebijakan berikut, izin untuk membuat penyimpanan data peristiwa `CreateEventDataStore` ditolak jika setidaknya salah satu dari kondisi berikut tidak terpenuhi:

- Penyimpanan data acara tidak memiliki kunci tag yang `stage` diterapkan pada dirinya sendiri
- Nilai tag stage bukan`alpha`,, `beta`gamma, atau`prod`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

Dalam contoh kebijakan berikut, izin untuk menghapus penyimpanan data peristiwa dengan ditolak `DeleteEventDataStore` adalah jika penyimpanan data peristiwa memiliki `stage` tag dengan nilai`prod`. Kebijakan seperti ini dapat membantu melindungi penyimpanan data peristiwa dari penghapusan yang tidak disengaja.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Menggunakan CloudTrail konsol

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

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

Pemberian izin untuk CloudTrail administrasi

Untuk mengizinkan peran atau pengguna IAM mengelola CloudTrail sumber daya, seperti jejak, penyimpanan data peristiwa, atau saluran, Anda harus memberikan izin eksplisit untuk melakukan tindakan yang terkait dengan CloudTrail tugas. Dalam sebagian besar situasi, Anda dapat menggunakan kebijakan terkel AWS ola yang berisi izin yang telah ditentukan sebelumnya.

> **Note**
>
> Izin yang Anda berikan kepada pengguna untuk melakukan tugas CloudTrail administrasi tidak sama dengan izin yang diperlukan CloudTrail untuk mengirimkan file log ke bucket Amazon S3 atau mengirim pemberitahuan ke topik Amazon SNS. Untuk informasi selengkapnya tentang izin tersebut, lihatKebijakan bucket Amazon S3 untuk CloudTrail. Jika Anda mengonfigurasi integrasi dengan Amazon CloudWatch Logs, CloudTrail juga memerlukan peran yang dapat diasumsikan untuk mengirimkan peristiwa ke grup CloudWatch log Amazon Logs. Anda harus membuat peran yang CloudTrail menggunakan. Untuk informasi selengkapnya, lihat Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol dan Mengirim acara ke CloudWatch Log.

Kebijakan ter AWS kelola berikut tersedia untuk CloudTrail:

- AWSCloudTrail_FullAccessKebijakan ini menyediakan akses penuh ke CloudTrail tindakan pada CloudTrail sumber daya, seperti jalur, penyimpanan data acara, dan saluran. Kebijakan ini memberikan izin yang diperlukan untuk membuat, memperbarui, dan menghapus CloudTrail jejak, penyimpanan data peristiwa, dan saluran.

  Kebijakan ini juga memberikan izin untuk mengelola bucket Amazon S3, grup CloudWatch log untuk Log, dan topik Amazon SNS untuk jejak. Namun, kebijakan `AWSCloudTrail_FullAccess` terkelola tidak memberikan izin untuk menghapus bucket Amazon S3, grup CloudWatch log untuk Log, atau topik Amazon SNS. Untuk informasi tentang kebijakan terkelola untuk kebijakan lain Layanan AWS, lihat Panduan Refer AWS ensi Kebijakan Terkelola .

  > **Note**
  >
  > AWSCloudTrail_FullAccessKebijakan ini tidak dimaksudkan untuk dibagikan secara luas di seluruh Anda Akun AWS. Pengguna dengan peran ini dapat mematikan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di dalamnya. Akun AWS Untuk alasan ini, Anda hanya harus menerapkan kebijakan ini kepada administrator akun. Anda harus mengontrol dan memantau penggunaan kebijakan ini secara ketat.

- AWSCloudTrail_ReadOnlyAccessKebijakan ini memberikan izin untuk melihat CloudTrail konsol, termasuk peristiwa terbaru dan riwayat acara. Kebijakan ini juga memungkinkan Anda untuk melihat jalur yang ada, penyimpanan data acara, dan saluran. Peran dan pengguna

dengan kebijakan ini dapat mengunduh riwayat acara, tetapi mereka tidak dapat membuat atau memperbarui jejak, penyimpanan data acara, atau saluran.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Sumber daya tambahan

Untuk mempelajari lebih lanjut tentang menggunakan IAM untuk memberikan identitas, seperti pengguna dan peran, akses ke sumber daya di akun Anda, lihat Men yiapkan IAM dan Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM.

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.

Izinkan para pengguna untuk melihat izin mereka sendiri

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

```
{
```

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

Memberikan izin khusus untuk CloudTrail pengguna

CloudTrail kebijakan memberikan izin kepada pengguna yang bekerja dengan CloudTrail. Jika Anda perlu memberikan izin yang berbeda kepada pengguna, Anda dapat melampirkan CloudTrail kebijakan ke grup IAM atau pengguna. Anda dapat mengedit kebijakan untuk menyertakan atau mengecualikan izin tertentu. Anda juga dapat membuat kebijakan kustom Anda sendiri. Kebijakan adalah dokumen JSON yang menentukan tindakan yang diizinkan untuk dilakukan pengguna dan sumber daya yang diizinkan pengguna untuk melakukan tindakan tersebut. Untuk contoh spesifik, lihat Contoh: Mengizinkan dan menolak tindakan untuk jejak tertentu danContoh: Membuat dan menerapkan kebijakan untuk tindakan pada jalur tertentu.

Daftar Isi

- Read-only akses
- Akses penuh
- Memberikan izin untuk melihat AWS Config informasi tentang CloudTrail konsol
- Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol
- Informasi tambahan

Read-only akses

Contoh berikut menunjukkan kebijakan yang memberikan akses read-only ke CloudTrail jalur. Ini setara dengan kebijakan yang dikelola AWSCloudTrail_ReadOnlyAccess. Ini memberi pengguna izin untuk melihat informasi jejak, tetapi tidak untuk membuat atau memperbarui jalur.

JSON

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

Dalam pernyataan kebijakan, `Effect` elemen menentukan apakah tindakan diizinkan atau ditolak. `Action`Elemen mencantumkan tindakan spesifik yang diizinkan untuk dilakukan pengguna. `Resource`Elemen mencant AWS umkan sumber daya yang diizinkan pengguna untuk melakukan tindakan tersebut. Untuk kebijakan yang mengontrol akses ke CloudTrail tindakan, `Resource` elemen biasanya disetel ke*, wildcard yang berarti “semua sumber daya.”

Nilai dalam `Action` elemen sesuai dengan API yang didukung layanan. Tindakan didahului `cloudtrail:` dengan menunjukkan bahwa mereka mengacu pada CloudTrail tindakan. Anda dapat menggunakan karakter * wildcard dalam `Action` elemen, seperti dalam contoh berikut:

- `"Action": ["cloudtrail:*Logging"]`

  Ini memungkinkan semua CloudTrail tindakan yang diakhiri dengan "Logging" (`StartLogging`,`StopLogging`).
- `"Action": ["cloudtrail:*"]`

  Ini memungkinkan semua CloudTrail tindakan, tetapi bukan tindakan untuk AWS layanan lain.
- `"Action": ["*"]`

  Ini memungkinkan semua AWS tindakan. Izin ini cocok untuk pengguna yang bertindak sebagai AWS administrator untuk akun Anda.

Kebijakan baca-saja tidak memberikan izin pengguna untuk`CreateTrail`,, `UpdateTrail``StartLogging`, dan `StopLogging` tindakan. Pengguna dengan kebijakan ini tidak diizinkan untuk membuat jalur, memperbarui jalur, atau mengaktifkan dan menonaktifkan logging. Untuk daftar CloudTrail tindakan, lihat Referensi AWS CloudTrail API.

Akses penuh

Contoh berikut menunjukkan kebijakan yang memberikan akses penuh ke CloudTrail. Ini setara dengan kebijakan yang dikelola AWSCloudTrail_FullAccess. Ini memberi pengguna izin untuk melakukan semua CloudTrail tindakan. Ini juga memungkinkan pengguna mencatat peristiwa data di Amazon S3 dan AWS Lambda, mengelola file di bucket Amazon S3, mengelola cara CloudWatch CloudTrail Log memantau peristiwa log, dan mengelola topik Amazon SNS di akun yang dikaitkan dengan pengguna.

> **Important**
>
> AWSCloudTrail_FullAccessKebijakan atau izin yang setara tidak dimaksudkan untuk dibagikan secara luas di seluruh AWS akun Anda. Pengguna dengan peran ini atau akses yang setara memiliki kemampuan untuk menonaktifkan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di AWS akun mereka. Untuk alasan ini, kebijakan ini harus diterapkan hanya untuk administrator akun, dan penggunaan kebijakan ini harus dikontrol dan dipantau secara ketat.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-logging-bucket1*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

Memberikan izin untuk melihat AWS Config informasi tentang CloudTrail konsol

Anda dapat melihat informasi acara di CloudTrail konsol, termasuk sumber daya yang terkait dengan acara tersebut. Untuk sumber daya ini, Anda dapat memilih AWS Config ikon untuk melihat garis waktu untuk sumber daya tersebut di AWS Config konsol. Lampirkan kebijakan ini ke pengguna Anda untuk memberi mereka akses baca-saja AWS Config . Kebijakan tidak memberi mereka izin untuk mengubah setelan di AWS Config.

JSON

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

```
}
```

Untuk informasi selengkapnya, lihat Melihat sumber daya yang direferensikan dengan AWS Config.

Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol

Anda dapat melihat dan mengonfigurasi pengiriman acara ke CloudWatch Log di CloudTrail konsol jika Anda memiliki izin yang cukup. Ini adalah izin yang mungkin di luar yang diberikan untuk CloudTrail administrator. Lampirkan kebijakan ini ke administrator yang akan mengonfigurasi dan mengelola CloudTrail integrasi dengan CloudWatch Log. Kebijakan tidak memberi mereka izin di dalam CloudTrail atau di CloudWatch Log secara langsung, melainkan memberikan izin yang diperlukan untuk membuat dan mengonfigurasi peran yang CloudTrail akan diasumsikan agar berhasil mengirimkan peristiwa ke grup CloudWatch Log Anda.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

Untuk informasi selengkapnya, lihat Memantau File CloudTrail Log dengan CloudWatch Log Amazon.

Informasi tambahan

Untuk mempelajari lebih lanjut tentang menggunakan IAM untuk memberikan identitas, seperti pengguna dan peran, akses ke sumber daya di akun Anda, lihat Mem ulai dan Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM.

AWS CloudTrail contoh kebijakan berbasis sumber daya

Bagian ini memberikan contoh kebijakan berbasis sumber daya untuk dasbor CloudTrail Lake, penyimpanan data peristiwa, dan saluran.

CloudTrail mendukung jenis kebijakan berbasis sumber daya berikut:

- Resource-based kebijakan tentang saluran yang digunakan untuk integrasi CloudTrail Danau dengan sumber acara di luar. AWS Kebijakan berbasis sumber daya untuk saluran menentukan entitas utama (akun, pengguna, peran, dan pengguna federasi) mana yang dapat memanggil `PutAuditEvents` saluran untuk mengirimkan peristiwa ke penyimpanan data peristiwa tujuan. Untuk informasi selengkapnya tentang membuat integrasi dengan CloudTrail Lake, lihatBuat integrasi dengan sumber acara di luar AWS.
- Resource-based kebijakan untuk mengontrol kepala sekolah mana yang dapat melakukan tindakan pada penyimpanan data acara Anda. Anda dapat menggunakan kebijakan berbasis sumber daya untuk menyediakan akses lintas akun ke penyimpanan data acara Anda.
- Resource-based kebijakan pada dasbor CloudTrail untuk memungkinkan penyegaran dasbor CloudTrail Lake pada interval yang Anda tentukan saat Anda menetapkan jadwal penyegaran untuk dasbor. Untuk informasi selengkapnya, lihat Tetapkan jadwal penyegaran untuk dasbor khusus dengan CloudTrail konsol.

Contoh:

- Resource-based contoh kebijakan untuk saluran
- Resource-based contoh kebijakan untuk penyimpanan data acara
- Resource-based contoh kebijakan untuk dasbor

Resource-based contoh kebijakan untuk saluran

Kebijakan berbasis sumber daya untuk saluran menentukan entitas utama (akun, pengguna, peran, dan pengguna federasi) mana yang dapat memanggil `PutAuditEvents` saluran untuk mengirimkan peristiwa ke penyimpanan data peristiwa tujuan.

Informasi yang diperlukan untuk kebijakan ditentukan oleh jenis integrasi.

- Untuk integrasi arah, CloudTrail kebijakan harus memuat Akun AWS ID mitra, dan mengharuskan Anda memasukkan ID eksternal unik yang disediakan oleh mitra. CloudTrail secara otomatis menambahkan Akun AWS ID mitra ke kebijakan sumber daya saat Anda membuat integrasi menggunakan CloudTrail konsol. Lihat dokumentasi mitra untuk mempelajari cara mendapatkan Akun AWS nomor yang diperlukan untuk polis.
- Untuk integrasi solusi, Anda harus menentukan setidaknya satu Akun AWS ID sebagai kepala sekolah, dan dapat secara opsional memasukkan ID eksternal untuk mencegah wakil yang bingung.

Berikut ini adalah persyaratan untuk kebijakan berbasis sumber daya:

- Kebijakan tersebut berisi setidaknya satu pernyataan. Kebijakan tersebut dapat memiliki maksimal 20 pernyataan.
- Setiap pernyataan berisi setidaknya satu prinsip. Prinsipal adalah akun, pengguna, peran, atau pengguna federasi. Sebuah pernyataan dapat memiliki maksimal 50 kepala sekolah.
- Sumber daya ARN yang ditentukan dalam kebijakan harus sesuai dengan saluran ARN yang dilampirkan kebijakan.
- Kebijakan hanya berisi satu tindakan: `cloudtrail-data:PutAuditEvents`

Pemilik saluran dapat memanggil `PutAuditEvents` API di saluran kecuali kebijakan menolak akses pemilik ke sumber daya.

Topik

- Contoh: Menyediakan akses saluran ke kepala sekolah
- Contoh: Menggunakan ID eksternal untuk mencegah wakil yang bingung

Contoh: Menyediakan akses saluran ke kepala sekolah

Contoh berikut memberikan izin kepada prinsipal dengan ARN`arn:aws:iam::111122223333:root`,`arn:aws:iam::444455556666:root`, dan `arn:aws:iam::123456789012:root` untuk memanggil PutAuditEvents API pada CloudTrail saluran dengan ARN. `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Contoh: Menggunakan ID eksternal untuk mencegah wakil yang bingung

Contoh berikut menggunakan ID eksternal untuk mengatasi dan mencegah wakil yang bingung. Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan.

Mitra integrasi membuat ID eksternal untuk digunakan dalam kebijakan. Kemudian, ia memberikan ID eksternal kepada Anda sebagai bagian dari pembuatan integrasi. Nilai dapat berupa string unik apa pun, seperti frasa sandi atau nomor akun.

Contoh ini memberikan izin kepada prinsipal dengan ARN, `arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root`, dan `arn:aws:iam::123456789012:root` untuk memanggil PutAuditEvents API pada sumber daya CloudTrail saluran jika panggilan ke `PutAuditEvents` API menyertakan nilai ID eksternal yang ditentukan dalam kebijakan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
        }
    ]
}
```

Resource-based contoh kebijakan untuk penyimpanan data acara

Resource-based kebijakan memungkinkan Anda mengontrol prinsipal mana yang dapat melakukan tindakan pada penyimpanan data acara Anda.

Anda dapat menggunakan kebijakan berbasis sumber daya untuk menyediakan akses lintas akun untuk mengizinkan kepala sekolah yang dipilih untuk menanyakan penyimpanan data acara Anda, membuat daftar dan membatalkan kueri, serta melihat hasil kueri.

Untuk dasbor CloudTrail Lake, kebijakan berbasis sumber daya digunakan CloudTrail untuk memungkinkan menjalankan kueri di penyimpanan data acara Anda untuk mengisi data untuk widget dasbor saat dasbor diperbarui. CloudTrail Lake memberi Anda opsi untuk melampirkan kebijakan berbasis sumber daya default ke penyimpanan data acara Anda saat Anda membuat dasbor khusus atau mengaktifkan dasbor Sorotan di CloudTrail konsol.

Tindakan berikut didukung dalam kebijakan berbasis sumber daya untuk penyimpanan data peristiwa:

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

Saat membuat atau memperbarui penyimpanan data peristiwa, atau mengelola dasbor di CloudTrail konsol, Anda diberi opsi untuk menambahkan kebijakan berbasis sumber daya ke penyimpanan data acara Anda. Anda juga dapat menjalankan perintah put-resource-policy untuk melampirkan kebijakan berbasis sumber daya ke penyimpanan data peristiwa.

Kebijakan berbasis sumber daya terdiri dari satu atau lebih pernyataan. Misalnya, dapat menyertakan satu pernyataan yang memungkinkan CloudTrail untuk menanyakan penyimpanan data peristiwa untuk dasbor dan pernyataan lain yang memungkinkan akses lintas akun untuk menanyakan penyimpanan data peristiwa. Anda dapat memperbarui kebijakan berbasis sumber daya penyimpanan data peristiwa yang ada dari halaman detail penyimpanan data peristiwa di CloudTrail konsol.

Untuk penyimpanan data peristiwa organisasi, buat CloudTrail kebijakan berbasis sumber daya default yang mencantumkan tindakan yang diizinkan untuk dilakukan oleh akun administrator yang didelegasikan pada penyimpanan data acara organisasi. Izin dalam kebijakan ini berasal dari izin

administrator yang didelegasikan di AWS Organizations. Kebijakan ini diperbarui secara otomatis setelah perubahan pada penyimpanan data acara organisasi atau organisasi (misalnya, akun administrator yang di CloudTrail delegasikan terdaftar atau dihapus).

Contoh:

- Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor
- Contoh: Izinkan akun lain untuk menanyakan penyimpanan data peristiwa dan melihat hasil kueri

Contoh: Iz CloudTrail inkan menjalankan kueri untuk menyegarkan dasbor

Untuk mengisi data di dasbor CloudTrail Lake selama penyegaran, Anda harus mengiz CloudTrail inkan menjalankan kueri atas nama Anda. Untuk melakukan ini, lampirkan kebijakan berbasis sumber daya ke setiap penyimpanan data peristiwa yang terkait dengan widget dasbor yang menyertakan pernyataan yang memungkinkan CloudTrail untuk melakukan `StartQuery` operasi untuk mengisi data untuk widget.

Berikut ini adalah persyaratan untuk pernyataan:

- Satu-satunya `Principal` adalah`cloudtrail.amazonaws.com`.
- Satu-satunya yang `Action` diizinkan adalah`cloudtrail:StartQuery`.
- `Condition`Satu-satunya termasuk dasbor ARN (s) dan Akun AWS ID. Untuk`AWS:SourceArn`, Anda dapat menyediakan array ARN dasbor.

Kebijakan contoh berikut mencakup pernyataan yang memungkinkan CloudTrail menjalankan kueri pada penyimpanan data peristiwa untuk dua dasbor kustom bernama `example-dashboard1` `example-dashboard2` dan dasbor Sorotan dinamai `AWSCloudTrail-Highlights` untuk akun`123456789012`.

JSON

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

```
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartQuery"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
               "StringLike": {
                  "AWS:SourceArn": [
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard1",
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard2",
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
AWSCloudTrail-Highlights"
                  ],
                  "AWS:SourceAccount": "123456789012"
               }
            }
        }
    ]
}
```

Contoh: Izinkan akun lain untuk menanyakan penyimpanan data peristiwa dan melihat hasil kueri

Anda dapat menggunakan kebijakan berbasis sumber daya untuk menyediakan akses lintas akun ke penyimpanan data acara agar akun lain dapat menjalankan kueri di penyimpanan data acara Anda.

Kebijakan contoh berikut mencakup pernyataan yang memungkinkan pengguna root di akun111122223333,, 777777777777999999999999, dan 111111111111 untuk menjalankan kueri dan mendapatkan hasil kueri pada penyimpanan data peristiwa yang dimiliki oleh ID akun555555555555.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "policy1",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::777777777777:root",
            "arn:aws:iam::999999999999:root",
            "arn:aws:iam::111111111111:root"
        ]
      },
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetQueryResults"
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:555555555555:eventdatastore/
example80-699f-4045-a7d2-730dbf313ccf"
    }
  ]
}
```

Resource-based contoh kebijakan untuk dasbor

Anda dapat mengatur jadwal penyegaran untuk dasbor CloudTrail Lake, yang memungkinkan CloudTrail untuk menyegarkan dasbor atas nama Anda pada interval yang Anda tentukan saat Anda mengatur jadwal penyegaran. Untuk melakukan ini, Anda perlu melampirkan kebijakan berbasis sumber daya ke dasbor CloudTrail untuk memungkinkan melakukan `StartDashboardRefresh` operasi di dasbor Anda.

Berikut ini adalah persyaratan untuk kebijakan berbasis sumber daya:

- Satu-satunya `Principal` adalah`cloudtrail.amazonaws.com`.
- Satu-satunya yang `Action` diizinkan dalam kebijakan adalah`cloudtrail:StartDashboardRefresh`.
- `Condition`Satu-satunya termasuk dasbor ARN dan Akun AWS ID.

Kebijakan contoh berikut memungkinkan CloudTrail untuk menyegarkan dasbor yang diberi nama `exampleDash` untuk akun`123456789012`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartDashboardRefresh"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn": "arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash",
                    "AWS:SourceAccount":"123456789012"
                }
            }
        }
    ]
}
```

Kebijakan bucket Amazon S3 untuk CloudTrail

Secara default, ember dan objek Amazon S3 bersifat pribadi. Hanya pemilik sumber daya (AWS akun yang membuat bucket) yang dapat mengakses bucket dan objek yang dikandungnya. Pemilik sumber daya dapat memberikan izin akses ke sumber daya dan pengguna lain dengan menulis kebijakan akses.

Untuk membuat atau memodifikasi bucket Amazon S3 agar menerima file log untuk jejak organisasi, Anda harus mengubah kebijakan bucket. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dengan AWS CLI.

Untuk mengirimkan file log ke bucket S3, CloudTrail harus memiliki izin yang diperlukan, dan file tersebut tidak dapat dikonfigurasi sebagai bucket Requester Pays.

CloudTrail menambahkan bidang berikut dalam kebijakan untuk Anda:

- Yang diizinkan SIDs
- Nama ember
- Nama utama layanan untuk CloudTrail
- Nama folder tempat file log disimpan, termasuk nama bucket, awalan (jika Anda menentukan satu), dan ID AWS akun Anda

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan bucket Amazon S3. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk jejak atau jalur tertentu. Nilai `aws:SourceArn` selalu ARN dari jejak (atau array jejak ARNs) yang menggunakan ember untuk menyimpan log. Pastikan untuk menambahkan kunci `aws:SourceArn` kondisi ke kebijakan bucket S3 untuk jalur yang ada.

> **Note**
>
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan attempted-to-deliver peristiwa ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Kebijakan berikut memungkinkan CloudTrail untuk menulis file log ke bucket dari yang didukung Wilayah AWS. Ganti *`amzn-s3-demo-bucket[optionalPrefix]/`*,*`myAccountID`*,,*`region`*,, dan *`trailName`* dengan nilai yang sesuai untuk konfigurasi Anda.

Kebijakan bucket S3

JSON

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

```
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Untuk informasi lebih lanjut tentang Wilayah AWS, lihatCloudTrail Daerah yang didukung.

Daftar Isi

- Menentukan bucket yang ada untuk pengiriman CloudTrail log
- Menerima file log dari akun lain
- Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi
- Memecahkan masalah kebijakan bucket Amazon S3
  - Kesalahan konfigurasi kebijakan Amazon S3 yang umum
  - Mengubah awalan untuk bucket yang ada

- Sumber daya tambahan

Menentukan bucket yang ada untuk pengiriman CloudTrail log

Jika Anda menetapkan bucket S3 yang ada sebagai lokasi penyimpanan untuk pengiriman file log, Anda harus melampirkan kebijakan ke bucket yang memungkinkan CloudTrail untuk menulis ke bucket.

> **Note**
>
> Sebagai praktik terbaik, gunakan bucket S3 khusus untuk CloudTrail log.

Untuk menambahkan CloudTrail kebijakan yang diperlukan ke bucket Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih bucket tempat Anda CloudTrail ingin mengirimkan file log, lalu pilih Izin.
3. Pilih Edit.
4. Salin S3 bucket policy ke jendela Bucket Policy Editor. Ganti placeholder dalam huruf miring dengan nama bucket, awalan, dan nomor akun Anda. Jika Anda menentukan awalan ketika Anda membuat jejak Anda, sertakan di sini. Awalan adalah tambahan opsional untuk kunci objek S3 yang membuat organisasi seperti folder di bucket Anda.

   > **Note**
   >
   > Jika bucket yang ada sudah memiliki satu atau beberapa kebijakan yang dilampirkan, tambahkan pernyataan untuk CloudTrail akses ke kebijakan atau kebijakan tersebut. Evaluasi kumpulan izin yang dihasilkan untuk memastikan bahwa izin tersebut sesuai untuk pengguna yang akan mengakses bucket.

Menerima file log dari akun lain

Anda dapat mengonfigurasi CloudTrail untuk mengirimkan file log dari beberapa AWS akun ke satu bucket S3. Untuk informasi selengkapnya, lihat Menerima file CloudTrail log dari beberapa akun.

Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi

Anda harus menentukan bucket Amazon S3 untuk menerima file log untuk jejak organisasi. Bucket ini harus memiliki kebijakan yang memungkinkan CloudTrail untuk menempatkan file log untuk organisasi ke dalam bucket.

Berikut ini adalah contoh kebijakan untuk bucket Amazon S3 bernama*amzn-s3-demo-bucket*, yang dimiliki oleh akun manajemen organisasi. Ganti *amzn-s3-demo-bucketregion*,*managementAccountID*,*trailName*,, dan *o-organizationID* dengan nilai-nilai untuk organisasi Anda

Kebijakan bucket ini berisi tiga pernyataan.

- Pernyataan pertama memungkinkan CloudTrail untuk memanggil `GetBucketAcl` tindakan Amazon S3 di ember Amazon S3.
- Pernyataan kedua memungkinkan pencatatan jika jejak diubah dari jejak organisasi menjadi jejak untuk akun itu saja.
- Pernyataan ketiga memungkinkan pencatatan untuk jejak organisasi.

Kebijakan contoh menyertakan kunci `aws:SourceArn` kondisi untuk kebijakan bucket Amazon S3. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk jejak atau jalur tertentu. Dalam jejak organisasi, nilai `aws:SourceArn` harus berupa jejak ARN yang dimiliki oleh akun manajemen, dan menggunakan ID akun manajemen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/
AWSLogs/managementAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/AWSLogs/o-
organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
```

```
            }
        }
    ]
}
```

Kebijakan contoh ini tidak mengizinkan pengguna dari akun anggota untuk mengakses file log yang dibuat untuk organisasi. Secara default, file log organisasi hanya dapat diakses oleh akun manajemen. Untuk informasi tentang cara mengizinkan akses baca ke bucket Amazon S3 untuk pengguna IAM di akun anggota, lihat. Berbagi file CloudTrail log antar AWS akun

Memecahkan masalah kebijakan bucket Amazon S3

Bagian berikut menjelaskan cara memecahkan masalah kebijakan bucket S3.

> **Note**
>
> Jika Anda salah mengonfigurasi jejak Anda (misalnya, bucket S3 tidak dapat dijangkau), CloudTrail akan mencoba mengirimkan ulang file log ke bucket S3 Anda selama 30 hari, dan attempted-to-deliver peristiwa ini akan dikenakan biaya standar. CloudTrail Untuk menghindari tagihan pada jejak yang salah konfigurasi, Anda perlu menghapus jejak.

Kesalahan konfigurasi kebijakan Amazon S3 yang umum

Saat Anda membuat bucket baru sebagai bagian dari membuat atau memperbarui jejak, CloudTrail lampirkan izin yang diperlukan ke bucket Anda. Kebijakan bucket menggunakan nama utama layanan`"cloudtrail.amazonaws.com"`, yang memungkinkan CloudTrail pengiriman log untuk semua Wilayah.

Jika CloudTrail tidak mengirimkan log untuk Wilayah, kemungkinan bucket Anda memiliki kebijakan lama yang menentukan CloudTrail akun IDs untuk setiap Wilayah. Kebijakan ini memberikan CloudTrail izin untuk mengirimkan log hanya untuk Wilayah yang ditentukan.

Sebagai praktik terbaik, perbarui kebijakan untuk menggunakan izin dengan kepala CloudTrail layanan. Untuk melakukan ini, ganti ID akun ARNs dengan nama utama layanan:`"cloudtrail.amazonaws.com"`. Ini memberikan CloudTrail izin untuk mengirimkan log untuk Wilayah saat ini dan yang baru. Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` atau `aws:SourceAccount` kondisi ke kebijakan bucket Amazon

S3. Ini membantu mencegah akses akun yang tidak sah ke bucket S3 Anda. Jika Anda memiliki jalur yang ada, pastikan untuk menambahkan satu atau lebih kunci kondisi. Contoh berikut menunjukkan konfigurasi kebijakan yang direkomendasikan. Ganti *amzn-s3-demo-bucket[optionalPrefix]/*,*myAccountID*,,*region*,, dan *trailName* dengan nilai yang sesuai untuk konfigurasi Anda.

Example Contoh kebijakan bucket dengan nama utama layanan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

Mengubah awalan untuk bucket yang ada

Jika Anda mencoba menambahkan, memodifikasi, atau menghapus awalan file log untuk bucket S3 yang menerima log dari jejak, Anda mungkin melihat kesalahan: Ada masalah dengan kebijakan bucket. Kebijakan bucket dengan awalan yang salah dapat mencegah jejak Anda mengirimkan log ke bucket. Untuk mengatasi masalah ini, gunakan konsol Amazon S3 untuk memperbarui awalan dalam kebijakan bucket, lalu gunakan CloudTrail konsol untuk menentukan awalan yang sama untuk bucket di trail.

Untuk memperbarui awalan file log untuk bucket Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih bucket yang ingin Anda ubah awalan, lalu pilih Izin.
3. Pilih Edit.
4. Dalam kebijakan bucket, di bawah `s3:PutObject` tindakan, edit `Resource` entri untuk menambah, memodifikasi, atau menghapus file log *`prefix/`* sesuai kebutuhan.

```
"Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*",
```

5. Pilih Simpan.
6. Buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
7. Pilih jejak Anda dan untuk lokasi Penyimpanan, klik ikon pensil untuk mengedit pengaturan bucket Anda.
8. Untuk bucket S3, pilih bucket dengan awalan yang Anda ubah.
9. Untuk awalan file Log, perbarui awalan agar sesuai dengan awalan yang Anda masukkan dalam kebijakan bucket.
10. Pilih Simpan.

Sumber daya tambahan

Untuk informasi selengkapnya tentang bucket dan kebijakan S3, lihat Menggunakan kebijakan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Kebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake

Secara default, ember dan objek Amazon S3 bersifat pribadi. Hanya pemilik sumber daya (AWS akun yang membuat bucket) yang dapat mengakses bucket dan objek yang dikandungnya. Pemilik sumber daya dapat memberikan izin akses ke sumber daya dan pengguna lain dengan menulis kebijakan akses.

Untuk mengirimkan hasil kueri CloudTrail Lake ke bucket S3, CloudTrail harus memiliki izin yang diperlukan, dan tidak dapat dikonfigurasi sebagai bucket Requester Pays.

CloudTrail menambahkan bidang berikut dalam kebijakan untuk Anda:

- Yang diizinkan SIDs
- Nama ember
- Nama utama layanan untuk CloudTrail

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan bucket Amazon S3. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menulis ke bucket S3 hanya untuk penyimpanan data acara.

Kebijakan berikut memungkinkan CloudTrail untuk mengirimkan hasil kueri ke bucket dari yang didukung Wilayah AWS. Ganti *`amzn-s3-demo-bucket`*, *`myAccountID`*, dan *`myQueryRunningRegion`* dengan nilai yang sesuai untuk konfigurasi Anda. *`myAccountID`*Ini adalah ID AWS akun yang digunakan CloudTrail, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

> **Note**
>
> Jika kebijakan bucket Anda menyertakan pernyataan untuk kunci KMS, sebaiknya gunakan ARN kunci KMS yang memenuhi syarat sepenuhnya. Jika Anda menggunakan alias kunci KMS sebagai gantinya, AWS KMS selesaikan kunci dalam akun pemohon. Perilaku ini dapat menghasilkan data yang dienkripsi dengan kunci KMS milik pemohon, dan bukan pemilik bucket.
> Jika ini adalah penyimpanan data acara organisasi, ARN penyimpanan data acara harus menyertakan ID AWS akun untuk akun manajemen. Ini karena akun manajemen mempertahankan kepemilikan semua sumber daya organisasi.

Kebijakan bucket S3

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
```

```
            }
        }
    ]
}
```

Daftar Isi

- Menentukan bucket yang ada untuk hasil kueri CloudTrail Lake
- Sumber daya tambahan

Menentukan bucket yang ada untuk hasil kueri CloudTrail Lake

Jika Anda menetapkan bucket S3 yang ada sebagai lokasi penyimpanan untuk pengiriman hasil kueri CloudTrail Lake, Anda harus melampirkan kebijakan ke bucket yang memungkinkan CloudTrail untuk mengirimkan hasil kueri ke bucket.

> **Note**
>
> Sebagai praktik terbaik, gunakan bucket S3 khusus untuk hasil kueri CloudTrail Lake.

Untuk menambahkan CloudTrail kebijakan yang diperlukan ke bucket Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Pilih bucket tempat Anda CloudTrail ingin mengirimkan hasil kueri Lake, lalu pilih Izin.
3. Pilih Edit.
4. Salin S3 bucket policy for query results ke jendela Bucket Policy Editor. Ganti placeholder dalam huruf miring dengan nama bucket, Region, dan ID akun Anda.

> **Note**
>
> Jika bucket yang ada sudah memiliki satu atau beberapa kebijakan yang dilampirkan, tambahkan pernyataan untuk CloudTrail akses ke kebijakan atau kebijakan tersebut. Evaluasi kumpulan izin yang dihasilkan untuk memastikan bahwa izin tersebut sesuai untuk pengguna yang mengakses bucket.

Sumber daya tambahan

Untuk informasi selengkapnya tentang bucket dan kebijakan S3, lihat Menggunakan kebijakan bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Kebijakan topik Amazon SNS untuk CloudTrail

Untuk mengirim pemberitahuan ke topik SNS, CloudTrail harus memiliki izin yang diperlukan. CloudTrailsecara otomatis melampirkan izin yang diperlukan ke topik saat Anda membuat topik Amazon SNS sebagai bagian dari membuat atau memperbarui jejak di konsol. CloudTrail

> **Important**
>
> Sebagai praktik keamanan terbaik, untuk membatasi akses ke topik SNS Anda, kami sangat menyarankan bahwa setelah Anda membuat atau memperbarui jejak untuk mengirim pemberitahuan SNS, Anda secara manual mengedit kebijakan IAM yang dilampirkan ke topik SNS untuk menambahkan kunci kondisi. Untuk informasi lebih lanjut, lihat the section called "Praktik terbaik keamanan untuk kebijakan topik SNS" di topik ini.

CloudTrail menambahkan pernyataan berikut ke kebijakan untuk Anda dengan bidang berikut:

- Yang diizinkan SIDs.
- Nama utama layanan untuk CloudTrail.
- Topik SNS, termasuk Wilayah, ID akun, dan nama topik.

Kebijakan berikut memungkinkan CloudTrail untuk mengirim pemberitahuan tentang pengiriman file log dari Wilayah yang didukung. Untuk informasi selengkapnya, lihat CloudTrail Daerah yang didukung. Ini adalah kebijakan default yang dilampirkan ke kebijakan topik SNS baru atau yang sudah ada saat Anda membuat atau memperbarui jejak, dan memilih untuk mengaktifkan notifikasi SNS.

Kebijakan topik SNS

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:SNSTopicName"
        }
    ]
}
```

Untuk menggunakan topik Amazon AWS KMS SNS yang dienkripsi untuk mengirim notifikasi, Anda juga harus mengaktifkan kompatibilitas antara sumber peristiwa (CloudTrail) dan topik terenkripsi dengan menambahkan pernyataan berikut ke kebijakan. AWS KMS key

Kebijakan kunci KMS

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Mengaktifkan Kompatibilitas antara Sumber Peristiwa dari AWS Layanan dan Topik Terenkripsi.

Daftar Isi

- Praktik terbaik keamanan untuk kebijakan topik SNS
- Menentukan topik yang ada untuk mengirim notifikasi
- Memecahkan masalah kebijakan topik SNS
  - CloudTrail tidak mengirim notifikasi untuk Wilayah
  - CloudTrail tidak mengirimkan pemberitahuan untuk akun anggota di organisasi
- Sumber daya tambahan

Praktik terbaik keamanan untuk kebijakan topik SNS

Secara default, pernyataan kebijakan IAM yang CloudTrail melekat pada topik Amazon SNS Anda memungkinkan CloudTrail kepala layanan untuk mempublikasikan ke topik SNS, yang diidentifikasi oleh ARN. Untuk membantu mencegah penyerang mendapatkan akses ke topik SNS Anda, dan mengirim pemberitahuan atas nama penerima topik, edit kebijakan topik CloudTrail SNS Anda secara manual untuk menambahkan kunci `aws:SourceArn` kondisi ke pernyataan kebijakan yang dilampirkan oleh. CloudTrail CloudTrail Nilai kunci ini adalah ARN jejak, atau susunan jejak yang menggunakan ARNs topik SNS. Karena mencakup ID jejak tertentu dan ID akun yang memiliki jejak, ini membatasi akses topik SNS hanya ke akun yang memiliki izin untuk mengelola jejak. Sebelum menambahkan kunci kondisi ke kebijakan topik SNS Anda, dapatkan nama topik SNS dari setelan jejak Anda di CloudTrail konsol.

Kunci `aws:SourceAccount` kondisi juga didukung, tetapi tidak disarankan.

Untuk menambahkan kunci **`aws:SourceArn`** kondisi ke kebijakan topik SNS Anda

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi, pilih Pengguna.
3. Pilih topik SNS yang ditampilkan di pengaturan jejak Anda, lalu pilih Edit.
4. Perluas Kebijakan akses.
5. Di editor JSON kebijakan Access, cari blok yang menyerupai contoh berikut.

```
  {
    "Sid": "AWSCloudTrailSNSPolicy20150319",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Tambahkan blok baru untuk suatu kondisi`aws:SourceArn`, seperti yang ditunjukkan pada contoh berikut. Nilai `aws:SourceArn` adalah ARN dari jejak yang Anda kirimi notifikasi ke SNS.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. Setelah selesai mengedit kebijakan topik SNS, pilih Simpan perubahan.

Untuk menambahkan kunci **`aws:SourceAccount`** kondisi ke kebijakan topik SNS Anda

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Di panel navigasi, pilih Pengguna.
3. Pilih topik SNS yang ditampilkan di pengaturan jejak Anda, lalu pilih Edit.
4. Perluas Kebijakan akses.
5. Di editor JSON kebijakan Access, cari blok yang menyerupai contoh berikut.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. Tambahkan blok baru untuk suatu kondisi`aws:SourceAccount`, seperti yang ditunjukkan pada contoh berikut. Nilai `aws:SourceAccount` adalah ID akun yang memiliki CloudTrail jejak. Contoh ini membatasi akses ke topik SNS hanya untuk pengguna yang dapat masuk ke AWS akun 123456789012.

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. Setelah selesai mengedit kebijakan topik SNS, pilih Simpan perubahan.

Menentukan topik yang ada untuk mengirim notifikasi

Anda dapat menambahkan izin untuk topik Amazon SNS secara manual ke kebijakan topik Anda di konsol Amazon SNS, lalu menentukan topik di konsol. CloudTrail

Untuk memperbarui kebijakan topik SNS secara manual

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/ v3/home.
2. Pilih Topik dan kemudian pilih topik.
3. Pilih Edit lalu gulir ke bawah ke kebijakan Access.

4. Tambahkan pernyataan dari SNS topic policy dengan nilai yang sesuai untuk Wilayah, ID akun, dan nama topik.
5. Jika topik Anda adalah topik terenkripsi, Anda harus mengizinkan CloudTrail untuk memiliki `kms:GenerateDataKey*` dan izin. `kms:Decrypt` Untuk informasi selengkapnya, lihat Encrypted SNS topic KMS key policy.
6. Pilih Simpan perubahan.
7. Kembali ke CloudTrail konsol dan tentukan topik untuk jejak.

Memecahkan masalah kebijakan topik SNS

Bagian berikut menjelaskan cara memecahkan masalah kebijakan topik SNS.

Skenario:

- CloudTrail tidak mengirim notifikasi untuk Wilayah
- CloudTrail tidak mengirimkan pemberitahuan untuk akun anggota di organisasi

CloudTrail tidak mengirim notifikasi untuk Wilayah

Saat Anda membuat topik baru sebagai bagian dari membuat atau memperbarui jejak, CloudTrail lampirkan izin yang diperlukan ke topik Anda. Kebijakan topik menggunakan nama utama layanan`"cloudtrail.amazonaws.com"`, yang memungkinkan CloudTrail untuk mengirim pemberitahuan untuk semua Wilayah.

Jika CloudTrail tidak mengirimkan notifikasi untuk Wilayah, kemungkinan topik Anda memiliki kebijakan lama yang menentukan CloudTrail akun IDs untuk setiap Wilayah. Jenis kebijakan ini memberikan CloudTrail izin untuk mengirim pemberitahuan hanya untuk Wilayah yang ditentukan.

Sebagai praktik terbaik, perbarui kebijakan untuk menggunakan izin dengan kepala CloudTrail layanan. Untuk melakukan ini, ganti ID akun ARNs dengan nama utama layanan:`"cloudtrail.amazonaws.com"`.

Kebijakan contoh berikut memberikan CloudTrail izin untuk mengirim pemberitahuan untuk Wilayah saat ini dan yang baru:

Example kebijakan topik dengan nama utama layanan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

Verifikasi bahwa kebijakan memiliki nilai yang benar:

- Di `Resource` bidang, tentukan nomor akun pemilik topik. Untuk topik yang Anda buat, tentukan nomor akun Anda.
- Tentukan nilai yang sesuai untuk nama topik Wilayah dan SNS.

CloudTrail tidak mengirimkan pemberitahuan untuk akun anggota di organisasi

Ketika akun anggota dengan jejak AWS Organizations organisasi tidak mengirimkan notifikasi Amazon SNS, mungkin ada masalah dengan konfigurasi kebijakan topik SNS. CloudTrail membuat jejak organisasi di akun anggota meskipun validasi sumber daya gagal, misalnya, topik SNS jejak organisasi tidak menyertakan semua akun anggota. IDs Jika kebijakan topik SNS salah, kegagalan otorisasi terjadi.

Untuk memeriksa apakah kebijakan topik SNS jejak mengalami kegagalan otorisasi:

- Dari CloudTrail konsol, periksa halaman detail jejak. Jika ada kegagalan otorisasi, halaman detail menyertakan peringatan `SNS authorization failed` dan menunjukkan untuk memperbaiki kebijakan topik SNS.
- Dari AWS CLI, jalankan get-trail-statusperintah. Jika ada kegagalan otorisasi, output perintah menyertakan `LastNotificationError` bidang dengan nilai. `AuthorizationError`

Sumber daya tambahan

Untuk informasi selengkapnya tentang topik SNS dan berlangganannya, lihat Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Pemecahan masalah AWS CloudTrail Identitas dan Akses

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di CloudTrail
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses CloudTrail sumber daya saya
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya mendapatkan peng NoManagementAccountSLRExistsException ecualian saat mencoba membuat jejak organisasi atau penyimpanan data acara

Saya tidak berwenang untuk melakukan tindakan di CloudTrail

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

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

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `cloudtrail:`*`GetWidget`*.

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

Jika member Konsol Manajemen AWS itahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentang jejak tetapi tidak memiliki kebijakan terkelola yang sesuai CloudTrail (AWSCloudTrail_FullAccessatau AWSCloudTrail_ReadOnlyAccess) atau izin setara yang diterapkan ke akunnya.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses informasi jejak dan status di konsol.

Jika Anda masuk dengan pengguna atau peran IAM yang memiliki kebijakan terkel AWSCloudTrail_FullAccess ola atau izin yang setara, dan Anda tidak dapat mengonfigurasi AWS Config atau integrasi Amazon CloudWatch Logs dengan jejak, Anda mungkin kehilangan izin yang diperlukan untuk integrasi dengan layanan tersebut. Untuk informasi selengkapnya, lihat Memberikan izin untuk melihat AWS Config informasi tentang CloudTrail konsol dan Memberikan izin untuk melihat dan mengonfigurasi informasi Amazon CloudWatch Log di CloudTrail konsol.

Saya tidak berwenang untuk melakukan **`iam: PassRole`**

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran CloudTrail.

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

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di CloudTrail. 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 mengizinkan orang-orang di luar saya Akun AWS untuk mengakses CloudTrail sumber daya saya

Anda dapat membuat peran dan berbagi CloudTrail informasi di antara beberapa Akun AWS. Untuk informasi selengkapnya, lihat Berbagi file CloudTrail log antar AWS akun.

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah CloudTrail mendukung fitur-fitur ini, lihatBagaimana AWS CloudTrail bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyedi Akun AWS akan akses milik pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Saya tidak berwenang untuk melakukan **`iam: PassRole`**

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran CloudTrail.

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

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol tersebut untuk melakukan tindakan di CloudTrail. 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 mendapatkan peng **`NoManagementAccountSLRExistsException`** ecualian saat mencoba membuat jejak organisasi atau penyimpanan data acara

Peng `NoManagementAccountSLRExistsException` ecualian dilemparkan ketika akun manajemen tidak memiliki peran terkait layanan.

Saat Anda menambahkan administrator yang didelegasikan menggunakan operasi AWS Organizations CLI atau API, CloudTrail peran terkait layanan tidak akan dibuat secara otomatis jika tidak ada. Peran terkait layanan hanya dibuat saat Anda melakukan panggilan dari akun manajemen langsung ke layanan. CloudTrail Misalnya, saat Anda menambahkan administrator yang didelegasikan atau membuat jejak organisasi atau penyimpanan data peristiwa menggunakan CloudTrail konsol, AWS CLI atau CloudTrail API, AWSServiceRoleForCloudTrail peran terkait layanan dibuat.

Ketika Anda menambahkan administrator yang didelegasikan menggunakan operasi AWS CloudTrail; CLI atau API, CloudTrail akan membuat peran AWSServiceRoleForCloudTrail dan peran terkait AWSServiceRoleForCloudTrailEventContext layanan.

Saat Anda menggunakan akun manajemen organisasi untuk menambahkan administrator yang didelegasikan atau membuat jejak organisasi atau penyimpanan data peristiwa di CloudTrail konsol, atau dengan menggunakan CloudTrail API or, CloudTrail secara otomatis membuat

AWSServiceRoleForCloudTrail peran terkait layanan untuk akun manajemen Anda jika itu belum ada. AWS CLI Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk CloudTrail.

Jika Anda belum menambahkan administrator yang didelegasikan, gunakan CloudTrail konsol, AWS CLI atau CloudTrail API untuk menambahkan administrator yang didelegasikan. Untuk informasi selengkapnya tentang menambahkan administrator yang didelegasikan, lihat Menambahkan administrator yang CloudTrail didelegasikan dan RegisterOrganizationDelegatedAdmin (API).

Jika Anda telah menambahkan administrator yang didelegasikan, gunakan akun manajemen untuk membuat jejak organisasi atau penyimpanan data peristiwa di CloudTrail konsol, atau dengan menggunakan CloudTrail API AWS CLI or. Untuk informasi selengkapnya tentang membuat jejak organisasi, lihatMembuat jejak untuk organisasi Anda di konsol,Membuat jejak untuk organisasi dengan AWS CLI, dan CreateTrail (API).

Menggunakan peran terkait layanan untuk CloudTrail

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

Topik

- Menggunakan peran untuk membuat dan mengelola jalur CloudTrail organisasi dan penyimpanan data acara organisasi CloudTrail Danau di CloudTrail
- Wilayah yang Didukung untuk CloudTrail peran terkait layanan
- Menggunakan peran untuk membuat dan mengelola konteks CloudTrail acara di CloudTrail
- Wilayah yang Didukung untuk CloudTrail peran terkait layanan

Menggunakan peran untuk membuat dan mengelola jalur CloudTrail organisasi dan penyimpanan data acara organisasi CloudTrail Danau di CloudTrail

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

Peran terkait layanan membuat pengaturan CloudTrail lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. CloudTrail mendefinisikan izin peran terkait

layanan, dan kecuali ditentukan lain, hanya CloudTrail dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi CloudTrail sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk CloudTrail

CloudTrail menggunakan peran terkait layanan bernama AWSServiceRoleForCloudTrail— Peran terkait layanan ini digunakan untuk mendukung jejak organisasi dan penyimpanan data acara organisasi.

Peran AWSService RoleForCloudTrail terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `cloudtrail.amazonaws.com`

Kebijakan izin peran bernama CloudTrailServiceRolePolicy memungkinkan CloudTrail untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan pada semua CloudTrail sumber daya:
  - `All`
- Tindakan pada semua AWS Organizations sumber daya:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- Tindakan pada semua sumber daya Organizations untuk prinsipal CloudTrail layanan untuk mencantumkan administrator yang didelegasikan untuk organisasi:
  - `organizations:ListDelegatedAdministrators`

- Tindakan untuk menonaktifkan federasi Danau pada penyimpanan data acara organisasi:
  - `glue:DeleteTable`
  - `lakeformation:DeRegisterResource`

Anda harus mengonfigurasi izin agar pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang kebijakan terkelola yang terkait dengan AWSServiceRoleForCloudTrail, lihatAWS kebijakan terkelola untuk AWS CloudTrail.

Membuat peran terkait layanan untuk CloudTrail

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat jejak organisasi atau penyimpanan data peristiwa organisasi, atau menambahkan administrator yang didelegasikan di CloudTrail konsol, di Konsol Manajemen AWS, atau AWS API AWS CLI, akan CloudTrail membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda membuat jejak organisasi atau penyimpanan data peristiwa organisasi, atau menambahkan administrator yang didelegasikan di CloudTrail konsol, akan CloudTrail membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk CloudTrail

CloudTrail tidak memungkinkan Anda untuk mengedit peran AWSService RoleForCloudTrail terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk CloudTrail

Anda tidak perlu menghapus AWSService RoleForCloudTrail peran secara manual. Jika Akun AWS dihapus dari organisasi Organizations, AWSServiceRoleForCloudTrail peran tersebut secara otomatis dihapus dari itu Akun AWS. Anda tidak dapat melepaskan atau menghapus kebijakan dari peran AWSServiceRoleForCloudTrail terkait layanan di akun manajemen organisasi tanpa menghapus akun dari organisasi.

Anda juga dapat menggunakan konsol IAM, AWS CLI atau AWS API untuk menghapus peran terkait layanan secara manual. Untuk melakukan ini, Anda harus membersihkan sumber daya peran terkait layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika CloudTrail layanan menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya yang digunakan oleh AWSServiceRoleForCloudTrail peran, Anda dapat melakukan salah satu hal berikut:

- Hapus Akun AWS dari organisasi di Organizations.
- Perbarui jejak sehingga tidak lagi menjadi jejak organisasi. Untuk informasi selengkapnya, lihat Memperbarui jejak dengan CloudTrail konsol.
- Perbarui penyimpanan data acara sehingga tidak lagi menjadi penyimpanan data acara organisasi. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan data acara dengan konsol.
- Hapus jejak. Untuk informasi selengkapnya, lihat Menghapus jejak dengan konsol CloudTrail.
- Hapus penyimpanan data acara. Untuk informasi selengkapnya, lihat Menghapus penyimpanan data acara dengan konsol.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForCloudTrail terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk CloudTrail peran terkait layanan

CloudTrail mendukung penggunaan peran terkait layanan di semua Wilayah AWS tempat dan CloudTrail Organizations keduanya tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan titik akhir di Referensi Umum AWS.

Menggunakan peran untuk membuat dan mengelola konteks CloudTrail acara di CloudTrail

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

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

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi CloudTrail sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk CloudTrail

CloudTrail menggunakan peran terkait layanan bernama AWSServiceRoleForCloudTrailEventContext— Peran terkait layanan ini digunakan untuk mengelola Konteks CloudTrail Acara dan EventBridge aturan.

Peran AWSService RoleForCloudTrailEventContext terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `context.cloudtrail.amazonaws.com`

Kebijakan izin peran bernama CloudTrailEventContext memungkinkan CloudTrail untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan pada tag sumber daya:
  - `tag:GetResources`

- Tindakan pada semua EventBridge sumber daya Amazon untuk prinsipal CloudTrail layanan untuk membuat aturan:
  - `events:PutRule`
- Tindakan pada semua EventBridge sumber daya Amazon untuk prinsipal CloudTrail layanan untuk mengelola aturan yang dibuatnya:
  - `events:PutTargets`
  - `events:DeleteRule`
  - `events:RemoveTargets`
  - `events:RemoveTargets`
- Tindakan pada semua EventBridge sumber daya Amazon untuk prinsipal CloudTrail layanan untuk menjelaskan aturan yang dibuatnya:
  - `events:DescribeRule`
  - `events:DeRegisterResource`
- Tindakan pada semua EventBridge sumber daya Amazon:
  - `events:ListRules`

Anda harus mengonfigurasi izin agar pengguna, grup, atau peran Anda membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran terkait layanan dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang kebijakan terkelola yang terkait dengan AWSServiceRoleForCloudTrailEventContext, lihatAWS kebijakan terkelola untuk AWS CloudTrail.

Membuat peran terkait layanan untuk CloudTrail

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mulai menggunakan fitur event konteks di Konsol Manajemen AWS, the AWS CLI, atau AWS API, CloudTrail buat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda mulai menggunakan fitur event konteks, CloudTrail buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk CloudTrail

CloudTrail tidak memungkinkan Anda untuk mengedit peran AWSService RoleForCloudTrailEventContext terkait layanan. Setelah membuat peran terkait layanan, Anda tidak

dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait AWSService RoleForCloudTrailEventContext layanan untuk CloudTrail

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran AWSService RoleForCloudTrailEventContext terkait layanan, sebaiknya hapus peran tersebut. Dengan begitu, Anda tidak perlu lagi memantau atau memelihara entitas yang tidak digunakan. Namun, Anda harus membersihkan sumber daya untuk peran terkait layanan sebelum Anda dapat menghapusnya secara manual dengan menghapus TagContext kunci dari penyimpanan data peristiwa.

> **Note**
>
> Jika CloudTrail layanan menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus CloudTrail sumber daya yang digunakan oleh peran terkait AWSService RoleForCloudTrailEventContext layanan

1. Di terminal atau baris perintah, jalankan put-event-configuration perintah untuk toko acara tempat Anda ingin menghapus `TagContext` kuncinya. Misalnya, untuk menghapus `TagContext` kunci dari toko acara di *111122223333* akun di Wilayah AS Timur (Ohio) dengan ARN *arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111* `TagContext` di mana satu-satunya pemilih kunci konteks, Anda akan menggunakan perintah tanpa nilai put-event-configuration yang ditentukan untuk: `--context-key-selectors`

   ```
   aws cloudtrail put-event-configuration --event-data-store arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --max-event-size Large --context-key-selectors
   ```

2. Ulangi perintah ini untuk setiap penyimpanan data di setiap Wilayah di partisi. Untuk informasi selengkapnya, lihat Mengidentifikasi AWS sumber daya dengan Nama Sumber Daya Amazon (ARNs).

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSService RoleForCloudTrailEventContext terkait layanan. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk CloudTrail peran terkait layanan

CloudTrail mendukung penggunaan peran terkait layanan di semua Wilayah di mana CloudTrail dan EventBridge tersedia. Untuk informasi selengkapnya, lihat AWS Wilayah dan titik akhir.

AWS kebijakan terkelola untuk AWS CloudTrail

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: **`AWSCloudTrail_FullAccess`**

Identitas pengguna yang memiliki AWSCloudTrail_FullAccesskebijakan yang melekat pada perannya memiliki akses administratif penuh CloudTrail.

Untuk daftar JSON tentang detail kebijakan, lihat AWSCloudTrail_FullAccessdi panduan referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: **AWSCloudTrail_ReadOnlyAccess**

Identitas pengguna yang memiliki AWSCloudTrail_ReadOnlyAccesskebijakan yang melekat pada perannya dapat melakukan tindakan hanya-baca dalam CloudTrail, seperti `Get*` `List*`, dan `Describe*` tindakan pada jalur, penyimpanan data peristiwa CloudTrail Lake, atau kueri Lake.

Untuk daftar JSON tentang detail kebijakan, lihat AWSCloudTrail_ReadOnlyAccessdi panduan referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: **AWSServiceRoleForCloudTrail**

CloudTrailServiceRolePolicyKebijakan ini memungkinkan AWS CloudTrail untuk melakukan tindakan pada jalur organisasi dan penyimpanan data acara organisasi atas nama Anda. Kebijakan ini mencakup AWS Organizations izin yang diperlukan untuk mendeskripsikan dan mencantumkan akun organisasi dan administrator yang didelegasikan dalam organisasi. AWS Organizations

Kebijakan ini juga mencakup persyaratan AWS Glue dan AWS Lake Formation izin untuk menonaktifkan federasi Danau di penyimpanan data acara organisasi.

Kebijakan ini dilampirkan pada peran AWSServiceRoleForCloudTrailterkait layanan yang memungkinkan CloudTrail untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Untuk daftar JSON tentang detail kebijakan, lihat CloudTrailServiceRolePolicydi panduan referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: **CloudTrailEventContext**

CloudTrailEventContextKebijakan ini memungkinkan AWS CloudTrail untuk mengelola Konteks CloudTrail Acara dan EventBridge aturan atas nama Anda. Kebijakan ini mencakup EventBridge izin yang diperlukan untuk membuat, mengelola, dan menjelaskan aturan yang dibuatnya untuk Anda.

Kebijakan ini dilampirkan pada peran AWSServiceRoleForCloudTrailEventContextterkait layanan yang memungkinkan CloudTrail untuk melakukan tindakan atas nama Anda. Anda tidak dapat melampirkan kebijakan ini ke pengguna, grup, atau peran Anda.

Untuk daftar JSON tentang detail kebijakan, lihat CloudTrailEventContextdi panduan referensi Kebijakan AWS Terkelola.

CloudTrail pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk CloudTrail. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan ke umpan RSS pada halaman CloudTrail Riwayat dokumen.

Perubahan	Deskripsi	Date
`CloudTrailEventContext` — Kebijakan baru yang digunakan oleh peran terkait `AWSServiceRoleForCloudTrailEventContext` layanan	Menambahkan kebijakan dan peran baru yang digunakan untuk fitur acara yang CloudTrail diperkaya.	19 Mei 2025
`CloudTrailServiceRolePolicy` – Pembaruan ke kebijakan yang ada	Kebijakan yang diperbarui untuk mengizinkan tindakan berikut pada penyimpanan data acara organisasi saat federasi dinonaktifkan: • `glue:DeleteTable` • `lakeformation:DeregisterResource`	26 November 2023
`AWSCloudTrail_ReadOnlyAccess` – Pembaruan ke kebijakan yang ada	CloudTrail mengubah nama `AWSCloudTrailReadOnlyAccess` kebijakan menjadi`AWSCloudTrail_ReadOnlyAccess`. Selain itu, ruang lingkup izin dalam kebijakan telah dikurangi menjadi CloudTrail tindakan. Ini tidak lagi menyertakan Amazon S3, AWS KMS, atau izin AWS Lambda tindakan.	6 Juni 2022

Perubahan	Deskripsi	Date
CloudTrail mulai melacak perubahan	CloudTrail mulai melacak perubahan untuk kebijakan yang AWS dikelola.	6 Juni 2022

Validasi kepatuhan untuk AWS CloudTrail

Third-party auditor menilai keamanan dan kepatuhan AWS CloudTrail sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat mendaftar untuk AWS (lanjutan) atau mengaktifkan fitur lanjutan untuk lingkungan Anda AWS .

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

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 CloudTrail

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 Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data. Jika Anda secara khusus perlu

mereplikasi file CloudTrail log Anda pada jarak geografis yang lebih jauh, Anda dapat menggunakan Replikasi Lintas Wilayah untuk bucket Amazon S3 jejak Anda, yang memungkinkan penyalinan objek secara otomatis dan asinkron di seluruh bucket di berbagai Wilayah. AWS

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

Selain infrastruktur AWS global, CloudTrail menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Jejak dan data acara menyimpan yang mencatat peristiwa di semua Wilayah AWS

Saat Anda membuat jejak Multi-wilayah, CloudTrail buat jejak dengan konfigurasi identik di semua yang diaktifkan Wilayah AWS di akun Anda.

Saat Anda membuat penyimpanan data acara Multi-wilayah, CloudTrail kumpulkan peristiwa yang terjadi Wilayah AWS di semua akun Anda.

Pembuatan versi, konfigurasi siklus hidup, dan perlindungan kunci objek untuk data log CloudTrail

Karena CloudTrail menggunakan bucket Amazon S3 untuk menyimpan file log, Anda juga dapat menggunakan fitur yang disediakan oleh Amazon S3 untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda. Untuk informasi selengkapnya, lihat Ketahanan di Amazon S3.

Keamanan infrastruktur di AWS CloudTrail

Sebagai layanan terkelola, AWS CloudTrail dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses CloudTrail melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Praktik terbaik keamanan berikut juga membahas keamanan infrastruktur di CloudTrail:

- Pertimbangkan titik akhir Amazon VPC untuk akses jejak.
- Pertimbangkan titik akhir Amazon VPC untuk akses bucket Amazon S3. Untuk informasi selengkapnya, lihat Mengontrol akses dari titik akhir VPC dengan kebijakan bucket.
- Identifikasi dan audit semua bucket Amazon S3 yang berisi CloudTrail file log. Pertimbangkan untuk menggunakan tag untuk membantu mengidentifikasi CloudTrail jejak Anda dan bucket Amazon S3 yang CloudTrail berisi file log. Anda kemudian dapat menggunakan grup sumber daya untuk CloudTrail sumber daya Anda. Lihat informasi yang lebih lengkap di AWS Resource Groups.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memengaruhi entitas yang memiliki hak akses lebih tinggi untuk melakukan tindakan. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan pemanggilan dapat dimanipulasi menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak dilakukannya kecuali bila memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan dalam kebijakan sumber daya untuk membatasi izin yang AWS CloudTrail memberikan layanan lain ke sumber daya. Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang akan dikaitkan dengan akses lintas layanan. Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah "confused deputy" adalah dengan menggunakan kunci konteks kondisi global `aws:SourceArn` dengan ARN lengkap sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan kunci kondisi konteks `aws:SourceArn` global dengan wildcard (`*`) untuk bagian ARN yang tidak diketahui. Misalnya, `"arn:aws:cloudtrail:*:AccountID:trail/*"`. Ketika Anda menyertakan wildcard, Anda juga harus menggunakan operator `StringLike` kondisi.

Nilai `aws:SourceArn` harus ARN dari jejak, penyimpanan data peristiwa, atau saluran yang menggunakan sumber daya.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kunci konteks kondisi `aws:SourceAccount` global `aws:SourceArn` dan CloudTrail untuk mencegah masalah wakil yang membingungkan:Kebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake.

Praktik terbaik keamanan di AWS CloudTrail

AWS CloudTrail menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Topik

- CloudTrail praktik terbaik keamanan detektif
- CloudTrail praktik terbaik keamanan preventif

CloudTrail praktik terbaik keamanan detektif

Buat jejak

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, Anda harus membuat jejak. Meskipun CloudTrail menyediakan 90 hari informasi riwayat acara untuk acara manajemen di CloudTrail konsol tanpa membuat jejak, itu bukan catatan permanen, dan tidak memberikan informasi tentang semua jenis peristiwa yang mungkin. Untuk catatan yang sedang berlangsung, dan untuk catatan yang berisi semua jenis peristiwa yang Anda tentukan, Anda harus membuat jejak, yang mengirimkan file log ke bucket Amazon S3 yang Anda tentukan.

Untuk membantu mengelola CloudTrail data Anda, pertimbangkan untuk membuat satu jejak yang mencatat peristiwa manajemen di semua Wilayah AWS, lalu membuat jejak tambahan yang mencatat jenis peristiwa tertentu untuk sumber daya, seperti aktivitas AWS Lambda atau fungsi bucket Amazon S3.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Buat jejak untuk AWS akun Anda.
- Buat jejak untuk organisasi.

Buat jejak Multi-wilayah

Untuk mendapatkan catatan lengkap peristiwa yang diambil oleh identitas IAM, atau layanan di AWS akun Anda, buat jejak Multi-wilayah. Multi-Region melacak peristiwa log di semua Wilayah AWS yang diaktifkan di Anda. Akun AWS Dengan mencatat peristiwa di semua yang diaktifkan Wilayah AWS, Anda memastikan bahwa Anda menangkap aktivitas di semua Wilayah yang diaktifkan di wilayah Anda Akun AWS. Ini termasuk mencatat peristiwa layanan global, yang dicatat ke layanan Wilayah AWS tertentu. Semua jalur yang dibuat menggunakan CloudTrail konsol adalah jalur Multi-wilayah.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Buat jejak untuk AWS akun Anda.
- Ubah jejak wilayah Tunggal yang ada menjadi jejak Multi-wilayah.
- Menerapkan kontrol detektif yang sedang berlangsung untuk membantu memastikan semua jejak yang dibuat mencatat peristiwa di semua Wilayah AWS dengan menggunakan aturan multi-region-cloud-trail-enabled di. AWS Config

Aktifkan integritas file CloudTrail log

File log yang divalidasi sangat berharga dalam penyelidikan keamanan dan forensik. Misalnya, file log yang divalidasi memungkinkan Anda untuk menegaskan secara positif bahwa file log itu sendiri tidak berubah, atau bahwa kredenal identitas IAM tertentu melakukan aktivitas API tertentu. Proses validasi integritas file CloudTrail log juga memungkinkan Anda mengetahui apakah file log telah dihapus atau diubah, atau menegaskan secara positif bahwa tidak ada file log yang dikirim ke akun Anda selama periode waktu tertentu. CloudTrail validasi integritas file log menggunakan algoritma standar industri: SHA-256 untuk hashing dan SHA-256 dengan RSA untuk penandatanganan digital. Ini membuatnya secara komputasi tidak layak untuk memodifikasi, menghapus, atau memalsukan CloudTrail file log tanpa deteksi. Untuk informasi selengkapnya, lihat Mengaktifkan validasi dan memvalidasi file.

Integrasikan dengan Amazon CloudWatch Logs

CloudWatch Log memungkinkan Anda untuk memantau dan menerima peringatan untuk peristiwa tertentu yang ditangkap oleh CloudTrail. Peristiwa yang dikirim ke CloudWatch Log adalah peristiwa yang dikonfigurasi untuk dicatat oleh jejak Anda, jadi pastikan Anda telah mengonfigurasi jejak atau jejak Anda untuk mencatat jenis peristiwa (peristiwa manajemen peristiwa data peristiwa peristiwa aktivitas and/or jaringan) yang ingin Anda pantau.

Misalnya, Anda dapat memantau keamanan kunci dan peristiwa manajemen terkait jaringan, seperti peristiwa login yang gagal Konsol Manajemen AWS.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Tinjau contoh Integrasi CloudWatch log untuk CloudTrail.
- Konfigurasikan jejak Anda untuk mengirim acara ke CloudWatch Log.
- Pertimbangkan untuk menerapkan kontrol detektif yang sedang berlangsung untuk membantu memastikan semua jejak mengirimkan peristiwa ke CloudWatch Log untuk dipantau dengan menggunakan aturan cloud-trail-cloud-watch-logs-enabled di. AWS Config

Gunakan Amazon GuardDuty

Amazon GuardDuty adalah layanan deteksi ancaman yang membantu Anda melindungi akun, wadah, beban kerja, dan data di AWS lingkungan Anda. Dengan menggunakan model machine learning (ML), serta kemampuan deteksi anomali dan ancaman, GuardDuty terus memantau berbagai sumber log untuk mengidentifikasi, dan memprioritaskan potensi risiko keamanan dan aktivitas berbahaya di lingkungan Anda.

Misalnya, GuardDuty akan mendeteksi potensi eksfiltrasi kredenal jika mendeteksi kredenal yang dibuat secara eksklusif untuk instans Amazon EC2 melalui peran peluncuran instans tetapi digunakan dari akun lain di dalamnya. AWS Untuk informasi selengkapnya, lihat Panduan GuardDuty Pengguna Amazon.

Gunakan AWS Security Hub CSPM

Pantau penggunaan Anda CloudTrail karena berkaitan dengan praktik terbaik keamanan dengan menggunakan AWS Security Hub CSPM. Security Hub CSPM menggunakan kontrol keamanan detektif untuk mengevaluasi konfigurasi sumber daya dan standar keamanan untuk membantu Anda mematuhi berbagai kerangka kerja kepatuhan. Untuk informasi selengkapnya tentang penggunaan CSPM Security Hub untuk mengevaluasi CloudTrail sumber daya, lihat AWS CloudTrail kontrol di AWS Security Hub Panduan Pengguna.

CloudTrail praktik terbaik keamanan preventif

Praktik terbaik berikut ini CloudTrail dapat membantu mencegah insiden keamanan.

Masuk ke bucket Amazon S3 yang berdedikasi dan terpusat

CloudTrail file log adalah log audit tindakan yang diambil oleh identitas IAM atau AWS layanan. Integritas, kelengkapan, dan ketersediaan log ini sangat penting untuk tujuan forensik dan audit.

Dengan masuk ke bucket Amazon S3 khusus dan terpusat, Anda dapat menerapkan kontrol keamanan, akses, dan pemisahan tugas yang ketat.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Buat AWS akun terpisah sebagai akun arsip log. Jika Anda menggunakan AWS Organizations, daftarkan akun ini di organisasi, dan pertimbangkan untuk membuat jejak organisasi untuk mencatat data semua AWS akun di organisasi Anda.
- Jika Anda tidak menggunakan Organizations tetapi ingin mencatat data untuk beberapa AWS akun, buat jejak untuk mencatat aktivitas di akun arsip log ini. Batasi akses ke akun ini hanya untuk pengguna administratif tepercaya yang harus memiliki akses ke akun dan data audit.
- Sebagai bagian dari membuat jejak, apakah itu jejak organisasi atau jejak untuk satu AWS akun, buat bucket Amazon S3 khusus untuk menyimpan file log untuk jejak ini.
- Jika Anda ingin mencatat aktivitas untuk lebih dari satu AWS akun, ubah kebijakan bucket untuk mengizinkan pencatatan dan penyimpanan file log untuk semua AWS akun yang ingin Anda log aktivitas AWS akun.
- Jika Anda tidak menggunakan jejak organisasi, buat jejak di semua AWS akun Anda, tentukan bucket Amazon S3 di akun arsip log.

Gunakan enkripsi sisi server dengan kunci terkelola AWS KMS

Secara default, file log yang dikirimkan CloudTrail ke bucket S3 Anda dienkripsi dengan menggunakan enkripsi sisi server dengan kunci KMS (SSE-KMS). Untuk menggunakan SSE-KMS dengan CloudTrail, Anda membuat dan mengelola AWS KMS key, juga dikenal sebagai kunci KMS.

> **Note**
>
> Jika Anda menggunakan SSE-KMS dan validasi file log, dan Anda telah memodifikasi kebijakan bucket Amazon S3 agar hanya mengizinkan file terenkripsi SSE-KMS, Anda tidak akan dapat membuat jejak yang menggunakan bucket tersebut kecuali Anda mengubah kebijakan bucket untuk mengizinkan enkripsi secara khusus, seperti yang ditunjukkan pada contoh baris kebijakan berikut. AES256
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Tinjau keuntungan mengenkripsi file log Anda dengan SSE-KMS.
- Buat kunci KMS yang akan digunakan untuk mengenkripsi file log.
- Konfigurasikan enkripsi file log untuk jejak Anda.
- Pertimbangkan untuk menerapkan kontrol detektif yang sedang berlangsung untuk membantu memastikan semua jejak mengenkripsi file log dengan SSE-KMS dengan menggunakan aturan di. cloud-trail-encryption-enabled AWS Config

Menambahkan kunci kondisi ke kebijakan topik Amazon SNS default

Saat Anda mengonfigurasi jejak untuk mengirim notifikasi ke Amazon SNS, CloudTrail tambahkan pernyataan kebijakan ke kebijakan akses topik SNS Anda yang memungkinkan CloudTrail untuk mengirim konten ke topik SNS. Sebagai praktik terbaik keamanan, sebaiknya tambahkan kunci kondisi `aws:SourceArn` (atau opsional`aws:SourceAccount`) ke pernyataan kebijakan topik Amazon SNS. Ini membantu mencegah akses akun yang tidak sah ke topik SNS Anda. Untuk informasi selengkapnya, lihat Kebijakan topik Amazon SNS untuk CloudTrail.

Menerapkan akses hak istimewa paling sedikit ke bucket Amazon S3 tempat Anda menyimpan file log

CloudTrail melacak peristiwa log ke bucket Amazon S3 yang Anda tentukan. File log ini berisi log audit tindakan yang diambil oleh identitas dan AWS layanan IAM. Integritas dan kelengkapan file log ini sangat penting untuk tujuan audit dan forensik. Untuk membantu memastikan integritas tersebut, Anda harus mematuhi prinsip hak istimewa paling sedikit saat membuat atau memodifikasi akses ke bucket Amazon S3 apa pun yang digunakan untuk CloudTrail menyimpan file log.

Lakukan langkah berikut:

- Tinjau kebijakan bucket Amazon S3 untuk setiap dan semua bucket tempat Anda menyimpan file log dan sesuaikan jika perlu untuk menghapus akses yang tidak perlu. Kebijakan bucket ini akan dibuat untuk Anda jika Anda membuat jejak menggunakan CloudTrail konsol, tetapi juga dapat dibuat dan dikelola secara manual.
- Sebagai praktik keamanan terbaik, pastikan untuk menambahkan kunci `aws:SourceArn` kondisi secara manual ke kebijakan bucket. Untuk informasi selengkapnya, lihat Kebijakan bucket Amazon S3 untuk CloudTrail.
- Jika Anda menggunakan bucket Amazon S3 yang sama untuk menyimpan file log untuk beberapa AWS akun, ikuti panduan untuk menerima file log untuk beberapa akun.

- Jika Anda menggunakan jejak organisasi, pastikan Anda mengikuti panduan untuk jalur organisasi, dan tinjau kebijakan contoh untuk bucket Amazon S3 untuk jejak organisasi. Membuat jejak untuk organisasi dengan AWS CLI
- Tinjau dokumentasi keamanan Amazon S3 dan contoh panduan untuk mengamankan bucket.

Aktifkan penghapusan MFA di bucket Amazon S3 tempat Anda menyimpan file log

Saat Anda mengonfigurasi otentikasi multi-faktor (MFA), upaya mengubah status pembuatan versi bucket, atau menghapus versi objek dalam bucket, memerlukan autentikasi tambahan. Dengan cara ini, bahkan jika pengguna memperoleh kata sandi pengguna IAM dengan izin untuk menghapus objek Amazon S3 secara permanen, Anda masih dapat mencegah operasi yang dapat membahayakan file log Anda.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Tinjau panduan penghapusan MFA di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
- Tambahkan kebijakan bucket Amazon S3 untuk meminta MFA.

> **Note**
>
> Anda tidak dapat menggunakan penghapusan MFA dengan konfigurasi siklus hidup. Untuk informasi selengkapnya tentang konfigurasi siklus hidup dan cara berinteraksi dengan konfigurasi lain, lihat Siklus Hidup dan konfigurasi bucket lainnya di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Konfigurasikan manajemen siklus hidup objek di bucket Amazon S3 tempat Anda menyimpan file log

Default CloudTrail jejak adalah menyimpan file log tanpa batas waktu di bucket Amazon S3 yang dikonfigurasi untuk jejak. Anda dapat menggunakan aturan manajemen siklus hidup objek Amazon S3 untuk menentukan kebijakan retensi Anda sendiri agar lebih memenuhi kebutuhan bisnis dan audit Anda. Misalnya, Anda mungkin ingin mengarsipkan file log yang berusia lebih dari satu tahun ke Amazon Glacier, atau menghapus file log setelah jangka waktu tertentu berlalu.

> **Note**
>
> Konfigurasi Siklus Hidup pada bucket dengan autentikasi multi-faktor (MFA) yang diaktifkan tidak didukung.

Batasi akses ke AWSCloudTrail_FullAccess kebijakan

Pengguna dengan AWSCloudTrail_FullAccesskebijakan memiliki kemampuan untuk menonaktifkan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di akun mereka AWS . Kebijakan ini tidak dimaksudkan untuk dibagikan atau diterapkan secara luas pada identitas IAM di akun Anda. AWS Batasi penerapan kebijakan ini untuk sesedikit mungkin individu, mereka yang Anda harapkan untuk bertindak sebagai administrator AWS akun.

Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS)

Secara default, file log dan file digest yang dikirimkan CloudTrail ke bucket Anda dienkripsi dengan menggunakan enkripsi sisi server dengan kunci KMS (SSE-KMS). Jika Anda tidak mengaktifkan enkripsi SSE-KMS, file log dan file digest Anda dienkripsi menggunakan enkripsi SSE-S3.

> **Note**
>
> Jika Anda menggunakan bucket S3 yang sudah ada dengan Kunci bucket S3, izin CloudTrail harus diizinkan dalam kebijakan kunci untuk menggunakan AWS KMS tindakan `GenerateDataKey` dan. `DescribeKey` Jika izin `cloudtrail.amazonaws.com` tersebut tidak diberikan dalam kebijakan utama, Anda tidak dapat membuat atau memperbarui jejak.

Untuk menggunakan SSE-KMS dengan CloudTrail, Anda membuat dan mengelola file. AWS KMS key Anda melampirkan kebijakan ke kunci yang menentukan pengguna mana yang dapat menggunakan kunci untuk mengenkripsi dan mendekripsi file CloudTrail log dan mencerna file. Dekripsi mulus melalui S3. Ketika pengguna resmi kunci membaca file CloudTrail log atau mencerna file, S3 mengelola dekripsi, dan pengguna yang berwenang dapat membaca file dalam bentuk yang tidak terenkripsi.

Pendekatan ini memiliki keuntungan sebagai berikut:

- Anda dapat membuat dan mengelola kunci KMS sendiri.
- Anda dapat menggunakan satu kunci KMS untuk mengenkripsi dan mendekripsi file log dan mencerna file untuk beberapa akun di semua Wilayah.
- Anda memiliki kendali atas siapa yang dapat menggunakan kunci Anda untuk mengenkripsi dan mendekripsi file CloudTrail log dan mencerna file. Anda dapat menetapkan izin untuk kunci kepada pengguna di organisasi Anda sesuai dengan kebutuhan Anda.
- Anda telah meningkatkan keamanan. Dengan fitur ini, untuk membaca file log atau mencerna file, izin berikut diperlukan:
  - Pengguna harus memiliki izin baca S3 untuk bucket yang berisi file log dan mencerna file.
  - Pengguna juga harus memiliki kebijakan atau peran yang diterapkan yang memungkinkan izin dekripsi oleh kebijakan kunci KMS.
- Karena S3 secara otomatis mendekripsi file log dan mencerna file untuk permintaan dari pengguna yang berwenang untuk menggunakan kunci KMS, enkripsi SSE-KMS untuk file tersebut kompatibel dengan aplikasi yang membaca data log. CloudTrail

> **Note**
>
> Kunci KMS yang Anda pilih harus dibuat di AWS Wilayah yang sama dengan bucket Amazon S3 yang menerima file log dan mencerna file Anda. Misalnya, jika file log dan file digest akan disimpan dalam bucket di Wilayah AS Timur (Ohio), Anda harus membuat atau memilih kunci KMS yang dibuat di Wilayah tersebut. Untuk memverifikasi Wilayah untuk bucket Amazon S3, periksa propertinya di konsol Amazon S3.

Secara default, penyimpanan data acara dienkripsi oleh. CloudTrail Anda memiliki opsi untuk menggunakan kunci KMS Anda sendiri untuk enkripsi saat Anda membuat atau memperbarui penyimpanan data acara.

Mengaktifkan enkripsi file log

> **Note**
>
> Jika Anda membuat kunci KMS di CloudTrail konsol, CloudTrail tambahkan bagian kebijakan kunci KMS yang diperlukan untuk Anda. Ikuti prosedur ini jika Anda membuat kunci di konsol

IAM atau AWS CLI dan Anda perlu menambahkan bagian kebijakan yang diperlukan secara manual.

Untuk mengaktifkan enkripsi SSE-KMS untuk file CloudTrail log, lakukan langkah-langkah tingkat tinggi berikut:

1. Buat kunci KMS.

   - Untuk informasi tentang membuat kunci KMS dengan Konsol Manajemen AWS, lihat Membuat Kunci di Panduan AWS Key Management Service Pengembang.
   - Untuk informasi tentang membuat kunci KMS dengan AWS CLI, lihat create-key.

   Note

   Kunci KMS yang Anda pilih harus berada di Wilayah yang sama dengan bucket S3 yang menerima file log dan mencerna file Anda. Untuk memverifikasi Region untuk bucket S3, periksa properti bucket di konsol S3.

2. Tambahkan bagian kebijakan ke kunci yang memungkinkan CloudTrail untuk mengenkripsi dan pengguna untuk mendekripsi file log dan mencerna file.

   - Untuk informasi tentang apa yang harus disertakan dalam kebijakan, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

     Warning

     Pastikan untuk menyertakan izin dekripsi dalam kebijakan untuk semua pengguna yang perlu membaca file log atau mencerna file. Jika Anda tidak melakukan langkah ini sebelum menambahkan kunci ke konfigurasi jejak Anda, pengguna tanpa izin dekripsi tidak dapat membaca file terenkripsi sampai Anda memberi mereka izin tersebut.

   - Untuk informasi tentang mengedit kebijakan dengan konsol IAM, lihat Mengedit Kebijakan Utama di Panduan AWS Key Management Service Pengembang.
   - Untuk informasi tentang melampirkan kebijakan ke kunci KMS dengan AWS CLI, lihat. put-key-policy

3. Perbarui penyimpanan data jejak atau acara Anda untuk menggunakan kunci KMS yang kebijakannya Anda modifikasi. CloudTrail

   - Untuk memperbarui penyimpanan data jejak atau peristiwa menggunakan CloudTrail konsol, lihatMemperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol.
   - Untuk memperbarui penyimpanan data jejak atau peristiwa menggunakan AWS CLI, lihatMengaktifkan dan menonaktifkan enkripsi untuk file CloudTrail log, mencerna file dan penyimpanan data peristiwa dengan AWS CLI.

CloudTrail juga mendukung kunci AWS KMS Multi-wilayah. Untuk informasi selengkapnya tentang kunci Multi-region, lihat Menggunakan kunci Multi-region di Panduan AWS Key Management Service Pengembang.

Bagian selanjutnya menjelaskan bagian kebijakan yang diperlukan oleh kebijakan kunci KMS Anda untuk digunakan. CloudTrail

Memberikan izin untuk membuat kunci KMS

Anda dapat memberikan izin kepada pengguna untuk membuat AWS KMS key dengan `AWSKeyManagementServicePowerUser`kebijakan tersebut.

Untuk memberikan izin untuk membuat kunci KMS

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pilih grup atau pengguna yang ingin Anda berikan izin.
3. Pilih tab Izin.
4. Dari daftar Tambahkan izin, pilih Lampirkan kebijakan.
5. Cari AWSKeyManagementServicePowerUser, pilih kebijakan, lalu pilih Lampirkan kebijakan.

   Pengguna sekarang memiliki izin untuk membuat kunci KMS. Untuk informasi selengkapnya tentang membuat kebijakan, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Konfigurasi AWS KMS kebijakan utama untuk CloudTrail

Anda dapat membuat AWS KMS key dalam tiga cara:

- Kon CloudTrail sol

- Konsol AWS Manajemen
- Yang AWS CLI

> **Note**
>
> Jika Anda membuat kunci KMS di CloudTrail konsol, CloudTrail tambahkan kebijakan kunci KMS yang diperlukan untuk Anda. Anda tidak perlu menambahkan pernyataan kebijakan secara manual. Lihat Kebijakan kunci KMS default dibuat di konsol CloudTrail.

Jika Anda membuat kunci KMS di Konsol Manajemen AWS atau AWS CLI, Anda harus menambahkan bagian kebijakan ke kunci tersebut sehingga Anda dapat menggunakannya dengan CloudTrail. Kebijakan harus mengizinkan penggunaan kunci CloudTrail untuk mengenkripsi file log, file ringkasan, dan penyimpanan data peristiwa, dan mengizinkan pengguna yang Anda tentukan untuk membaca file log dan file ringkasan dalam bentuk tidak terenkripsi.

Lihat sumber daya berikut:

- Untuk membuat kunci KMS dengan AWS CLI, lihat cre ate-key.
- Untuk mengedit kebijakan kunci KMS untuk CloudTrail, lihat Meng edit Kebijakan Kunci di Panduan Peng AWS Key Management Service embang.
- Untuk detail teknis tentang cara CloudTrail penggunaan AWS KMS, lihatBagaimana AWS CloudTrail menggunakan AWS KMS.

Topik

- Bagian kebijakan kunci KMS yang diperlukan untuk digunakan dengan CloudTrail
- Memberikan izin enkripsi untuk jalur
- Memberikan izin enkripsi untuk penyimpanan data acara
- Memberikan izin dekripsi untuk jalur
- Memberikan izin dekripsi untuk penyimpanan data acara
- Aktif CloudTrail kan untuk mendeskripsikan properti kunci KMS
- Kebijakan kunci KMS default dibuat di konsol CloudTrail

Bagian kebijakan kunci KMS yang diperlukan untuk digunakan dengan CloudTrail

Jika Anda membuat kunci KMS dengan konsol AWS Manajemen atau AWS CLI, maka Anda harus, setidaknya, menambahkan pernyataan berikut ke kebijakan kunci KMS agar dapat digunakan. CloudTrail

Topik

- Elemen kebijakan utama KMS yang diperlukan untuk jalur
- Elemen kebijakan kunci KMS yang diperlukan untuk penyimpanan data acara

Elemen kebijakan utama KMS yang diperlukan untuk jalur

1. Berikan izin untuk mengenkripsi file CloudTrail log dan intisari. Untuk informasi selengkapnya, lihat Memberikan izin enkripsi untuk jalur.
2. Berikan izin untuk mendekripsi CloudTrail log dan file intisari. Untuk informasi selengkapnya, lihat Memberikan izin dekripsi untuk jalur. Jika Anda menggunakan bucket S3 yang ada dengan Kunci Bucket S3, `kms:Decrypt` izin diperlukan untuk membuat atau memperbarui jejak dengan SSE-KMS enkripsi diaktifkan.
3. Aktif CloudTrail kan untuk menjelaskan properti kunci KMS. Untuk informasi selengkapnya, lihat Aktif CloudTrail kan untuk mendeskripsikan properti kunci KMS.

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu. Nilai `aws:SourceArn` selalu jejak ARN (atau array trail ARN) yang menggunakan kunci KMS. Pastikan untuk menambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS untuk jalur yang ada.

K `aws:SourceAccount` unci kondisi juga didukung, tetapi tidak disarankan. Nilai `aws:SourceAccount` adalah ID akun pemilik jejak, atau untuk jejak organisasi, ID akun manajemen.

> **Important**
>
> Saat menambahkan bagian baru ke kebijakan kunci KMS, jangan ubah bagian yang ada dalam kebijakan.

Jika enkripsi diaktifkan pada jejak, dan kunci KMS dinonaktifkan, atau kebijakan kunci KMS tidak dikonfigurasi dengan benar CloudTrail, tidak CloudTrail dapat mengirimkan log.

Elemen kebijakan kunci KMS yang diperlukan untuk penyimpanan data acara

1. Berikan izin untuk mengenkripsi penyimpanan data peristiwa CloudTrail Lake. Untuk informasi selengkapnya, lihat Memberikan izin enkripsi untuk penyimpanan data acara.
2. Berikan izin untuk mendekripsi penyimpanan data peristiwa CloudTrail Lake. Untuk informasi selengkapnya, lihat Memberikan izin dekripsi untuk penyimpanan data acara.

   Saat Anda membuat penyimpanan data peristiwa dan mengenkripsinya dengan kunci KMS, atau menjalankan kueri pada penyimpanan data peristiwa yang Anda enkripsi dengan kunci KMS, Anda harus memiliki akses tulis ke kunci KMS. Kebijakan kunci KMS harus memiliki akses ke CloudTrail, dan kunci KMS harus dikelola oleh pengguna yang menjalankan operasi (seperti kueri) pada penyimpanan data peristiwa.
3. Aktif CloudTrail kan untuk menjelaskan properti kunci KMS. Untuk informasi selengkapnya, lihat Aktif CloudTrail kan untuk mendeskripsikan properti kunci KMS.

CloudTrail Lake mendukung kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi dalam kebijakan kunci KMS untuk penyimpanan data peristiwa.

Important

Saat menambahkan bagian baru ke kebijakan kunci KMS, jangan ubah bagian yang ada dalam kebijakan.
Jika enkripsi diaktifkan pada penyimpanan data peristiwa, dan kunci KMS dinonaktifkan atau dihapus, atau kebijakan kunci KMS tidak dikonfigurasi dengan benar CloudTrail, tidak CloudTrail dapat mengirimkan peristiwa ke penyimpanan data acara Anda.

Memberikan izin enkripsi untuk jalur

Example Izinkan CloudTrail untuk mengenkripsi file log dan mencerna file atas nama akun tertentu

CloudTrail memerlukan izin eksplisit untuk menggunakan kunci KMS untuk mengenkripsi file log dan mencerna file atas nama akun tertentu. Untuk menentukan akun, tambahkan pernyataan wajib berikut ke kebijakan kunci KMS Anda dan ganti*`account-id`*,*`region`*, dan *`trailName`*

dengan nilai yang sesuai untuk konfigurasi Anda. Anda dapat menambahkan ID akun tambahan ke `EncryptionContext` bagian untuk mengaktifkan akun tersebut digunakan CloudTrail untuk menggunakan kunci KMS Anda untuk mengenkripsi file log dan file ringkasan.

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS untuk jejak. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu.

```
{
   "Sid": "AllowCloudTrailEncryptLogs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
             "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
         }
    }
}
```

Example

Contoh pernyataan kebijakan berikut menggambarkan bagaimana akun lain dapat menggunakan kunci KMS Anda untuk mengenkripsi file CloudTrail log dan file ringkasan.

Skenario

- Kunci KMS Anda ada di akun*111111111111*.
- Baik Anda dan akun *222222222222* akan mengenkripsi log.

Dalam kebijakan, Anda menambahkan satu atau beberapa akun yang dienkripsi dengan kunci Anda ke CloudTrail EncryptionContext. Ini membatasi penggunaan kunci Anda CloudTrail untuk mengenkripsi file log dan file ringkasan hanya untuk akun yang Anda tentukan. Saat Anda

memberikan *222222222222* izin root akun untuk mengenkripsi file log dan file ringkasan, itu mendelegasikan izin kepada administrator akun untuk mengenkripsi izin yang diperlukan kepada pengguna lain di akun tersebut. Administrator akun melakukan ini dengan mengubah kebijakan yang terkait dengan pengguna IAM tersebut.

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur yang ditentukan.

Pernyataan kebijakan utama KMS:

```
{
  "Sid": "EnableCloudTrailEncryptPermissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Untuk informasi selengkapnya tentang mengedit kebijakan kunci KMS untuk digunakan CloudTrail, lihat Mengedit kebijakan kunci di Panduan Peng AWS Key Management Service embang.

Memberikan izin enkripsi untuk penyimpanan data acara

CloudTrail Lake mendukung kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi dalam kebijakan kunci KMS untuk penyimpanan data peristiwa. Tambahkan kondisi ini setelah Anda membuat penyimpanan data acara. Contoh berikut memungkinkan satu penyimpanan data peristiwa untuk menggunakan kunci KMS.

```
{
    "Sid": "AllowCloudTrailEncryptEds",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id",
          "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:eventdatastore/event-
data-store-id"
        }
      }
}
```

Untuk akun yang sama, kueri wilayah yang sama yang bergabung dengan beberapa penyimpanan data peristiwa, setel `aws:SourceArn` ke array dari setiap penyimpanan data acara yang berpartisipasi ARN pada setiap kunci KMS yang digunakan oleh kueri.

Memberikan izin dekripsi untuk jalur

Sebelum menambahkan kunci KMS ke CloudTrail konfigurasi, penting untuk memberikan izin dekripsi kepada semua pengguna yang membutuhkannya. Pengguna yang memiliki izin enkripsi tetapi tidak memiliki izin mendekripsi tidak dapat membaca log terenkripsi. Jika Anda menggunakan bucket S3 yang ada dengan Kunci Bucket S3, `kms:Decrypt` izin diperlukan untuk membuat atau memperbarui jejak dengan SSE-KMS enkripsi diaktifkan.

Aktif CloudTrail kan izin dekripsi log

Pengguna kunci Anda harus diberi izin eksplisit untuk membaca file log yang CloudTrail telah dienkripsi. Untuk memungkinkan pengguna membaca log terenkripsi, tambahkan pernyataan wajib berikut ke kebijakan kunci KMS Anda, memodifikasi `Principal` bagian untuk menambahkan baris untuk setiap prinsip yang ingin Anda dapat mendekripsi dengan menggunakan kunci KMS Anda.

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Berikut ini adalah contoh kebijakan yang diperlukan untuk mengizinkan prinsipal CloudTrail layanan mendekripsi log jejak.

```
{
      "Sid": "AllowCloudTrailDecryptTrail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Izinkan pengguna di akun Anda untuk mendekripsi log jejak dengan kunci KMS Anda

Contoh

Pernyataan kebijakan ini menggambarkan cara mengizinkan pengguna atau peran di akun Anda menggunakan kunci Anda untuk membaca log terenkripsi di bucket S3 akun Anda.

Example Skenario

- Kunci KMS Anda, bucket S3, dan pengguna IAM Bob ada di akun. *111111111111*
- Anda memberikan izin Bob kepada pengguna IAM untuk mendekripsi CloudTrail log di bucket S3.

Dalam kebijakan utama, Anda mengaktifkan izin de CloudTrail kripsi log untuk pengguna IAM Bob.

Pernyataan kebijakan utama KMS:

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Izinkan pengguna di akun lain untuk mendekripsi log jejak dengan kunci KMS Anda

Anda dapat mengizinkan pengguna di akun lain untuk menggunakan kunci KMS Anda untuk mendekripsi log jejak. Perubahan yang diperlukan pada kebijakan kunci Anda bergantung pada apakah bucket S3 ada di akun Anda atau di akun lain.

Izinkan pengguna bucket di akun lain untuk mendekripsi log

Contoh

Pernyataan kebijakan ini menggambarkan cara mengizinkan pengguna atau peran IAM di akun lain menggunakan kunci Anda untuk membaca log terenkripsi dari bucket S3 di akun lain.

Skenario

- Kunci KMS Anda ada di akun*111111111111*.
- Pengguna IAM Alice dan bucket S3 ada di akun*222222222222*.

Dalam hal ini, Anda memberikan CloudTrail izin untuk mendekripsi log di bawah akun*222222222222*, dan Anda memberikan izin kebijakan pengguna IAM Alice untuk menggunakan kunci Anda*KeyA*, yang ada di akun*111111111111*.

Pernyataan kebijakan utama KMS:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:111111111111:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Pernyataan kebijakan pengguna IAM Alice:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

Izinkan pengguna di akun lain untuk mendekripsi log jejak dari bucket Anda

Example

Kebijakan ini menggambarkan bagaimana akun lain dapat menggunakan kunci Anda untuk membaca log terenkripsi dari bucket S3 Anda.

Example Skenario

- Kunci KMS dan bucket S3 Anda ada di akun*111111111111*.
- Pengguna yang membaca log dari bucket Anda ada di akun*222222222222*.

Untuk mengaktifkan skenario ini, Anda mengaktifkan izin dekripsi untuk peran IAM CloudTrailReadRole di akun Anda, lalu berikan izin akun lain untuk mengambil peran tersebut.

Pernyataan kebijakan utama KMS:

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRolepernyataan kebijakan entitas kepercayaan:

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
   {
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

Untuk informasi tentang mengedit kebijakan kunci KMS untuk digunakan CloudTrail, lihat Meng edit Kebijakan Utama di Panduan Peng AWS Key Management Service embang.

Memberikan izin dekripsi untuk penyimpanan data acara

Kebijakan dekripsi untuk kunci KMS yang digunakan dengan penyimpanan data CloudTrail peristiwa Lake mirip dengan yang berikut ini. ARN pengguna atau peran yang ditentukan sebagai nilai untuk `Principal` perlu mendekripsi izin untuk membuat atau memperbarui penyimpanan data peristiwa, menjalankan kueri, atau mendapatkan hasil kueri.

```
{
      "Sid": "EnableUserKeyPermissionsEds",
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

Berikut ini adalah contoh kebijakan yang diperlukan untuk mengizinkan prinsi CloudTrail pal layanan mendekripsi penyimpanan data peristiwa.

```
{
      "Sid": "AllowCloudTrailDecryptEds",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Aktif CloudTrail kan untuk mendeskripsikan properti kunci KMS

CloudTrail membutuhkan kemampuan untuk menggambarkan properti kunci KMS. Untuk mengaktifkan fungsi ini, tambahkan pernyataan wajib berikut sebagaimana adanya ke kebijakan kunci KMS Anda. Pernyataan ini tidak memberikan izin CloudTrail apa pun di luar izin lain yang Anda tentukan.

Sebagai praktik terbaik keamanan, tambahkan kunci `aws:SourceArn` kondisi ke kebijakan kunci KMS. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu.

```
{
  "Sid": "AllowCloudTrailAccess",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

Untuk informasi selengkapnya tentang mengedit kebijakan kunci KMS, lihat Mengedit Kebijakan Utama di Panduan Peng AWS Key Management Service embang.

Kebijakan kunci KMS default dibuat di konsol CloudTrail

Jika Anda membuat AWS KMS key di CloudTrail konsol, kebijakan berikut dibuat secara otomatis untuk Anda. Kebijakan ini mengizinkan izin ini:

- Mengizinkan izin Akun AWS (root) untuk kunci KMS.
- Memungkinkan CloudTrail untuk mengenkripsi file log dan mencerna file di bawah kunci KMS dan menjelaskan kunci KMS.
- Memungkinkan semua pengguna di akun yang ditentukan untuk mendekripsi file log dan file mencerna.
- Memungkinkan semua pengguna di akun yang ditentukan untuk membuat alias KMS untuk kunci KMS.
- Mengaktifkan dekripsi log lintas akun untuk ID akun akun yang membuat jejak.

Topik

- Kebijakan kunci KMS default untuk jalur

- Kebijakan kunci KMS default untuk penyimpanan data acara CloudTrail Lake

Kebijakan kunci KMS default untuk jalur

Berikut ini adalah kebijakan default yang dibuat untuk AWS KMS key yang Anda gunakan dengan jejak.

> **Note**
>
> Kebijakan ini mencakup pernyataan untuk mengizinkan akun silang mendekripsi file log dan mencerna file dengan kunci KMS.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111111111111:root",
                    "arn:aws:iam::111111111111:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:trail/trail-name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
```

```
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        }
    ]
}
```

Kebijakan kunci KMS default untuk penyimpanan data acara CloudTrail Lake

Berikut ini adalah kebijakan default yang dibuat untuk AWS KMS key yang Anda gunakan dengan penyimpanan data peristiwa di CloudTrail Lake.

JSON

```
{
      "Version":"2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores.
 Created ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
```

```
        },
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
                "AWS": "arn:aws:iam::111111111111:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
               "AWS" : "arn:aws:sts::111111111111:assumed-role/example-role-name"
        },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol

Di CloudTrail konsol, perbarui jejak atau penyimpanan data acara untuk menggunakan kunci KMS. Ketahuilah bahwa menggunakan kunci KMS Anda sendiri menimbulkan AWS KMS biaya untuk enkripsi dan dekripsi. Untuk informasi selengkapnya, silakan lihat Harga AWS Key Management Service.

Topik

- Perbarui jejak untuk menggunakan kunci KMS
- Memperbarui penyimpanan data acara untuk menggunakan kunci KMS

Perbarui jejak untuk menggunakan kunci KMS

Untuk memperbarui jejak untuk menggunakan AWS KMS key yang Anda modifikasi CloudTrail, selesaikan langkah-langkah berikut di CloudTrail konsol.

> **Note**
>
> Jika Anda menggunakan bucket S3 yang sudah ada dengan Kunci Bucket S3, izin CloudTrail harus diizinkan dalam kebijakan kunci untuk menggunakan AWS KMS tindakan `GenerateDataKey` dan. `DescribeKey` Jika izin `cloudtrail.amazonaws.com` tersebut tidak diberikan dalam kebijakan utama, Anda tidak dapat membuat atau memperbarui jejak.

Untuk memperbarui jejak menggunakan AWS CLI, lihatMengaktifkan dan menonaktifkan enkripsi untuk file CloudTrail log, mencerna file dan penyimpanan data peristiwa dengan AWS CLI.

Untuk memperbarui jejak untuk menggunakan kunci KMS Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pilih Trails dan kemudian pilih nama jejak.
3. Dalam Detail umum, pilih Edit.
4. Untuk enkripsi file Log SSE-KMS, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda dan mencerna file menggunakan enkripsi SSE-KMS alih-alih enkripsi SSE-S3. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan enkripsi SSE-KMS, file log dan file digest Anda dienkripsi menggunakan enkripsi SSE-S3. Untuk informasi selengkapnya tentang enkripsi SSE-KMS, lihat Menggunakan enkripsi sisi server dengan (SSE-KMS). AWS Key Management Service Untuk informasi selengkapnya tentang enkripsi SSE-S3, lihat Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3).

   Pilih yang Ada untuk memperbarui jejak Anda dengan Anda AWS KMS key. Pilih kunci KMS yang berada di Wilayah yang sama dengan bucket S3 yang menerima file log Anda. Untuk memverifikasi Region untuk bucket S3, lihat propertinya di konsol S3.

   > **Note**
   >
   > Anda juga dapat mengetikkan ARN kunci dari akun lain. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol.

Kebijakan kunci harus mengizinkan penggunaan kunci CloudTrail untuk mengenkripsi file log dan mencerna file, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log atau mencerna file dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.

Di AWS KMS Alias, tentukan alias yang Anda ubah kebijakan untuk digunakan CloudTrail, dalam format. `alias/` *`MyAliasName`* Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol.

Anda dapat mengetikkan nama alias, ARN, atau ID kunci unik global. Jika kunci KMS milik akun lain, verifikasi bahwa kebijakan kunci memiliki izin yang memungkinkan Anda menggunakannya. Nilai dapat berupa salah satu format berikut:

- Nama Alias: `alias/`*`MyAliasName`*
- Alias ARN: `arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
- Kunci ARN: `arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID kunci unik secara global: `12345678-1234-1234-1234-123456789012`

5. Pilih Perbarui jejak.

> **Note**
>
> Jika kunci KMS yang Anda pilih dinonaktifkan atau tertunda penghapusan, Anda tidak dapat menyimpan jejak dengan kunci KMS itu. Anda dapat mengaktifkan tombol KMS atau memilih yang lain. Untuk informasi selengkapnya, lihat Status kunci: Efek pada kunci KMS Anda di Panduan AWS Key Management Service Pengembang.

Memperbarui penyimpanan data acara untuk menggunakan kunci KMS

Untuk memperbarui penyimpanan data acara agar menggunakan AWS KMS key yang Anda modifikasi CloudTrail, selesaikan langkah-langkah berikut di CloudTrail konsol.

Untuk memperbarui penyimpanan data acara dengan menggunakan AWS CLI, lihatPerbarui penyimpanan data acara dengan AWS CLI.

> **Important**
>
> Menonaktifkan atau menghapus kunci KMS, atau menghapus CloudTrail izin pada kunci, CloudTrail mencegah masuknya peristiwa ke dalam penyimpanan data peristiwa, dan mencegah pengguna melakukan kueri data di penyimpanan data peristiwa yang dienkripsi dengan kunci. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah. Sebelum Anda menonaktifkan atau menghapus kunci KMS yang Anda gunakan dengan penyimpanan data acara, hapus atau cadangkan penyimpanan data acara Anda.

Untuk memperbarui penyimpanan data acara untuk menggunakan kunci KMS Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Penyimpanan data acara di Danau. Pilih penyimpanan data acara untuk diperbarui.
3. Dalam Detail umum, pilih Edit.
4. Untuk Enkripsi, jika belum diaktifkan, pilih Gunakan milik saya AWS KMS key untuk mengenkripsi penyimpanan data acara Anda dengan kunci KMS Anda sendiri.

   Pilih yang Ada untuk memperbarui penyimpanan data acara Anda dengan kunci KMS Anda. Pilih kunci KMS yang berada di Wilayah yang sama dengan penyimpanan data acara. Kunci dari akun lain tidak didukung.

   Di Masukkan AWS KMS Alias, tentukan alias yang Anda ubah kebijakan untuk digunakan CloudTrail, dalam format. `alias/` *`MyAliasName`* Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda dengan konsol.

   Anda dapat memilih alias, atau menggunakan ID kunci yang unik secara global. Nilai dapat berupa salah satu format berikut:

   - Nama Alias: `alias/`*`MyAliasName`*
   - Alias ARN: `arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - Kunci ARN: `arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-123456789012`
   - ID kunci unik secara global: `12345678-1234-1234-1234-123456789012`

5. Pilih Simpan perubahan.

> **Note**
>
> Jika kunci KMS yang Anda pilih dinonaktifkan atau tertunda penghapusan, Anda tidak dapat menyimpan konfigurasi penyimpanan data peristiwa dengan kunci KMS tersebut. Anda dapat mengaktifkan tombol KMS, atau memilih kunci yang berbeda. Untuk informasi selengkapnya, lihat Status kunci: Efek pada kunci KMS Anda di Panduan AWS Key Management Service Pengembang.

Mengaktifkan dan menonaktifkan enkripsi untuk file CloudTrail log, mencerna file dan penyimpanan data peristiwa dengan AWS CLI

Topik ini menjelaskan cara mengaktifkan dan menonaktifkan enkripsi SSE-KMS untuk file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan menggunakan file. AWS CLI Untuk informasi latar belakang, lihat Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS).

Topik

- Mengaktifkan enkripsi untuk file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan menggunakan AWS CLI
- Menonaktifkan enkripsi untuk file log dan mencerna file dengan menggunakan AWS CLI

Mengaktifkan enkripsi untuk file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan menggunakan AWS CLI

- Aktifkan file log dan intisari enkripsi file untuk jejak
- Aktifkan enkripsi untuk penyimpanan data acara

Aktifkan enkripsi untuk file log dan mencerna file untuk jejak

1. Buat kunci dengan AWS CLI. Kunci yang Anda buat harus berada di Region yang sama dengan bucket S3 yang menerima file CloudTrail log Anda. Untuk langkah ini, Anda menggunakan AWS KMS create-keyperintah.

2. Dapatkan kebijakan kunci yang ada sehingga Anda dapat memodifikasinya untuk digunakan CloudTrail. Anda dapat mengambil kebijakan kunci dengan AWS KMS get-key-policyperintah.
3. Tambahkan bagian yang diperlukan ke kebijakan kunci sehingga CloudTrail dapat mengenkripsi dan pengguna dapat mendekripsi file log Anda dan mencerna file. Pastikan bahwa semua pengguna yang membaca file log diberikan izin dekripsi. Jangan mengubah bagian kebijakan yang ada. Untuk informasi tentang bagian kebijakan yang akan disertakan, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.
4. Lampirkan file kebijakan JSON yang dimodifikasi ke kunci dengan menggunakan AWS KMS put-key-policyperintah.
5. Jalankan `update-trail` perintah CloudTrail `create-trail` or dengan `--kms-key-id` parameter. Perintah ini memungkinkan enkripsi file log dan mencerna file.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

`--kms-key-id`Parameter menentukan kunci yang kebijakannya Anda modifikasi. CloudTrail Ini bisa berupa salah satu dari format berikut:

- Nama Alias. Contoh: `alias/MyAliasName`
- Alias ARN. Contoh: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- Kunci ARN. Contoh: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID kunci unik secara global. Contoh: `12345678-1234-1234-1234-123456789012`

Berikut adalah respons contohnya:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

Kehadiran `KmsKeyId` elemen menunjukkan bahwa enkripsi untuk file log Anda telah diaktifkan. Jika validasi file log telah diaktifkan (ditunjukkan oleh `LogFileValidationEnabled` elemen

yang disetel ke true), ini juga menunjukkan bahwa enkripsi telah diaktifkan untuk file intisari Anda. File log terenkripsi dan file digest akan muncul di bucket S3 yang dikonfigurasi untuk jejak dalam waktu sekitar 5 menit.

Aktifkan enkripsi untuk penyimpanan data acara

1. Buat kunci dengan AWS CLI. Kunci yang Anda buat harus berada di Wilayah yang sama dengan penyimpanan data acara. Untuk langkah ini, jalankan AWS KMS create-keyperintah.
2. Dapatkan kebijakan kunci yang ada untuk diedit untuk digunakan CloudTrail. Anda bisa mendapatkan kebijakan kunci dengan menjalankan AWS KMS get-key-policyperintah.
3. Tambahkan bagian yang diperlukan ke kebijakan kunci sehingga CloudTrail dapat mengenkripsi dan pengguna dapat mendekripsi penyimpanan data acara Anda. Pastikan bahwa semua pengguna yang membaca penyimpanan data acara diberikan izin dekripsi. Jangan mengubah bagian kebijakan yang ada. Untuk informasi tentang bagian kebijakan yang akan disertakan, lihatKonfigurasi AWS KMS kebijakan utama untuk CloudTrail.
4. Lampirkan file kebijakan JSON yang diedit ke kunci dengan menjalankan perintah. AWS KMS put-key-policy
5. Jalankan `update-event-data-store` perintah CloudTrail `create-event-data-store` or, dan tambahkan `--kms-key-id` parameter. Perintah ini memungkinkan enkripsi penyimpanan data acara.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

`--kms-key-id`Parameter menentukan kunci yang kebijakannya Anda modifikasi. CloudTrail Ini bisa berupa salah satu dari empat format berikut:

- Nama Alias. Contoh: `alias/MyAliasName`
- Alias ARN. Contoh: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`
- Kunci ARN. Contoh: `arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012`
- ID kunci unik secara global. Contoh: `12345678-1234-1234-1234-123456789012`

Berikut adalah respons contohnya:

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

Kehadiran `KmsKeyId` elemen menunjukkan bahwa enkripsi untuk penyimpanan data peristiwa telah diaktifkan.

Menonaktifkan enkripsi untuk file log dan mencerna file dengan menggunakan AWS CLI

Untuk berhenti mengenkripsi file log dan mencerna file untuk jejak, jalankan `update-trail` dan berikan string kosong ke parameter: `kms-key-id`

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Berikut adalah respons contohnya:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "amzn-s3-demo-bucket"
```

```
}
```

Tidak adanya `KmsKeyId` nilai menunjukkan bahwa enkripsi untuk file log dan file digest tidak lagi diaktifkan.

> **Important**
>
> Anda tidak dapat menghentikan enkripsi untuk penyimpanan data acara.

Bagaimana AWS CloudTrail menggunakan AWS KMS

Bagian ini menjelaskan cara AWS KMS kerja dengan CloudTrail jejak yang dienkripsi dengan kunci SSE-KMS.

> **Important**
>
> AWS CloudTrail dan Amazon S3 hanya mendukung simetris. AWS KMS keys Anda tidak dapat menggunakan kunci KMS asimetris untuk mengenkripsi Log Anda. CloudTrail Untuk bantuan menentukan apakah kunci KMS simetris atau asimetris, lihat Mengidentifikasi tipe kunci yang berbeda dalam Panduan PengembangAWS Key Management Service .

Anda tidak membayar biaya penggunaan kunci saat CloudTrail membaca atau menulis file log yang dienkripsi dengan kunci SSE-KMS. Namun, Anda membayar biaya penggunaan kunci saat mengakses file CloudTrail log yang dienkripsi dengan kunci SSE-KMS. Untuk informasi tentang AWS KMS harga, lihat AWS Key Management Service Harga. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail harga.

Memahami kapan kunci KMS Anda digunakan untuk jejak Anda

Mengenkripsi file CloudTrail log dengan AWS KMS build pada fitur Amazon S3 yang disebut enkripsi sisi server dengan (SSE-KMS). AWS KMS key Untuk mempelajari lebih lanjut tentang SSE-KMS, lihat Menggunakan enkripsi sisi server dengan AWS KMS kunci (SSE-KMS) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Ketika Anda mengonfigurasi AWS CloudTrail untuk menggunakan SSE-KMS untuk mengenkripsi file log Anda, dan Amazon CloudTrail S3 menggunakan Anda AWS KMS keys saat Anda melakukan tindakan tertentu dengan layanan tersebut. Bagian berikut menjelaskan kapan dan bagaimana

layanan tersebut dapat menggunakan kunci KMS Anda, dan memberikan informasi tambahan yang dapat Anda gunakan untuk memvalidasi penjelasan ini.

Tindakan yang menyebabkan CloudTrail dan Amazon S3 menggunakan kunci KMS Anda

- Anda mengonfigurasi CloudTrail untuk mengenkripsi file log dengan AWS KMS key
- CloudTrail menempatkan file log ke bucket S3 Anda
- Anda mendapatkan berkas log yang dienkripsi dari bucket S3 Anda

Anda mengonfigurasi CloudTrail untuk mengenkripsi file log dengan AWS KMS key

Ketika Anda memperbarui CloudTrail konfigurasi Anda untuk menggunakan kunci KMS Anda, CloudTrail mengirimkan `GenerateDataKey`permintaan AWS KMS untuk memverifikasi bahwa kunci KMS ada dan yang CloudTrail memiliki izin untuk menggunakannya untuk enkripsi. CloudTrail tidak menggunakan kunci data yang dihasilkan.

Permintaan `GenerateDataKey` tersebut mencakup informasi berikut untuk konteks enkripsi:

- Nama Sumber Daya Amazon (ARN) dari jalan setapak CloudTrail
- ARN dari bucket S3 dan jalur tempat file CloudTrail log dikirim

`GenerateDataKey`Permintaan menghasilkan entri di CloudTrail log Anda yang mirip dengan contoh berikut. Ketika Anda melihat entri log seperti ini, Anda dapat menentukan yang CloudTrail disebut AWS KMS `GenerateDataKey` operasi untuk jejak tertentu. AWS KMS membuat kunci data di bawah kunci KMS tertentu.


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T20:14:46Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "keySpec": "AES_256",
```

```
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770",
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
management-events",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket-123456789012-9af1fb49/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2010Z_TO50OLMG1hIQ1png.json.gz"
        }
    },
    "responseElements": null,
    "requestID": "a0555e85-7e8a-4765-bd8f-2222295558e1",
    "eventID": "e4f3557e-7dbd-4e37-a00a-d86c137d1111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770"
         }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "ce71d6be-0846-498e-851f-111a1af9078f",
    "eventCategory": "Management"
}
```

CloudTrail menempatkan file log ke bucket S3 Anda

Setiap kali CloudTrail memasukkan file log ke bucket S3 Anda, Amazon S3 mengirimkan `GenerateDataKey`permintaan AWS KMS ke atas nama. CloudTrail Menanggapi permintaan ini, AWS KMS buat kunci data unik dan kemudian mengirimkan Amazon S3 dua salinan kunci data, satu dalam teks biasa dan satu yang dienkripsi dengan kunci KMS yang ditentukan. Amazon S3 menggunakan kunci data plaintext untuk mengenkripsi file CloudTrail log dan kemudian menghapus kunci data plaintext dari memori sesegera mungkin setelah digunakan. Amazon S3 menyimpan kunci data terenkripsi sebagai metadata dengan file log terenkripsi. CloudTrail

Permintaan `GenerateDataKey` tersebut mencakup informasi berikut untuk konteks enkripsi:

- Nama Sumber Daya Amazon (ARN) dari jalan setapak CloudTrail

- ARN dari objek S3 (file log) CloudTrail

Setiap `GenerateDataKey` permintaan menghasilkan entri di CloudTrail log Anda yang mirip dengan contoh berikut. Ketika Anda melihat entri log seperti ini, Anda dapat menentukan yang CloudTrail disebut AWS KMS `GenerateDataKey` operasi untuk jejak tertentu untuk melindungi file log tertentu. AWS KMS membuat kunci data di bawah kunci KMS yang ditentukan, ditampilkan dua kali dalam entri log yang sama.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T21:49:28Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1::trail/insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2150Z_hVXmrJzjZk2wAM2V.json.gz"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
    },
    "responseElements": null,
    "requestID": "11117d14-9232-414a-b3d1-01bab4dc9f99",
    "eventID": "999e9a50-512c-4e2a-84a3-111a5f511111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "5e663acc-b7fd-4cdd-8328-0eff862952fa",
    "eventCategory": "Management"
}
```

Anda mendapatkan berkas log yang dienkripsi dari bucket S3 Anda

Setiap kali Anda mendapatkan file CloudTrail log terenkripsi dari bucket S3 Anda, Amazon S3 mengirimkan `Decrypt`permintaan ke AWS KMS atas nama Anda untuk mendekripsi kunci data terenkripsi file log. Menanggapi permintaan ini, AWS KMS gunakan kunci KMS Anda untuk mendekripsi kunci data dan kemudian mengirimkan kunci data teks biasa ke Amazon S3. Amazon S3 menggunakan kunci data plaintext untuk mendekripsi file CloudTrail log dan kemudian menghapus kunci data plaintext dari memori sesegera mungkin setelah digunakan.

Permintaan `Decrypt` tersebut mencakup informasi berikut untuk konteks enkripsi:

- Nama Sumber Daya Amazon (ARN) dari jalan setapak CloudTrail
- ARN dari objek S3 (file log) CloudTrail

Setiap `Decrypt` permintaan menghasilkan entri di CloudTrail log Anda yang mirip dengan contoh berikut. Ketika Anda melihat entri log seperti ini, Anda dapat menentukan bahwa peran yang diasumsikan disebut AWS KMS `Decrypt` operasi untuk jejak tertentu dan file log tertentu. AWS KMS mendekripsi kunci data di bawah kunci KMS tertentu.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-12-06T22:04:04Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-12-06T22:26:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T0000Z_aAAsHbGBdye3jp2R.json.gz"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "1ab2d2d2-111a-2222-a59b-11a2b3832b53",
    "eventID": "af4d4074-2849-4b3d-1a11-a1aaa111a111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
```

```
}
```

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi untuk AWS CloudTrail. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Versi API: 2013-11-01
-

Perubahan	Deskripsi	Tanggal
Support untuk `userIdentity.arn` bidang dalam pemilih acara aktivitas jaringan	Anda sekarang dapat memfilter peristiwa aktivitas CloudTrail jaringan di jalur menggunakan bidang pemilih acara `userIdentity.arn` lanjutan. Untuk informasi selengkapnya, lihat Acara aktivitas jaringan.	Juli 15, 2026
Support untuk `signInSessionArn` lapangan	Ditambahkan dukungan untuk `signInSessionArn` `sessionContext` bidang di `userIdentity` elemen. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity dalam panduan ini.	Juni 30, 2026
AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026.	AWS CloudTrail Danau tidak akan lagi terbuka untuk pelanggan baru mulai 31 Mei 2026. Jika Anda ingin menggunakan CloudTrail Danau, daftar sebelum tanggal tersebut. Pelanggan yang sudah ada dapat terus	Maret 31, 2026

	menggunakan layanan ini seperti biasa. Untuk informasi lebih lanjut, lihat Perubahan ketersediaan CloudTrail Danau.	
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa aktivitas CloudTrail jaringan tambahan. Untuk informasi selengkapnya, lihat Acara aktivitas jaringan.	Oktober 15, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data tambahan untuk Amazon Bedrock Amazon Elastic Container Service, dan Amazon Quick. Untuk informasi selengkapnya, lihat Peristiwa data.	Oktober 15, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa aktivitas CloudTrail jaringan tambahan. Untuk informasi selengkapnya, lihat Acara aktivitas jaringan.	September 15, 2025

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data tambahan untuk Amazon Q Business, Amazon Quick, Amazon SageMaker AI, Amazon Bedrock, Amazon Elastic Compute Cloud, dan Amazon Kinesis Video Streams. Untuk informasi selengkapnya, lihat Peristiwa data.	September 12, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data tambahan untuk Amazon Aurora DSQL, Amazon Bedrock, Amazon Elastic Kubernetes Service, Amazon S3, dan Amazon Keyspaces (untuk Apache Cassandra). Untuk informasi selengkapnya, lihat Peristiwa data.	Juli 1, 2025
Menambahkan dukungan layanan	Rilis ini mendukung panggilan API Multi-party persetujuan Logging. Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung.	Juni 17, 2025

Ditambahkan fungsionalitas	Logging `DeleteObject` operasi peristiwa data Amazon S3 sekarang mencakup informasi tentang semua objek individual yang dihapus oleh panggilan. Anda dapat memilih untuk menyaring informasi tambahan ini. Untuk informasi selengkapnya, lihat AWS CLI contoh untuk memfilter peristiwa data.	Juni 9, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa aktivitas jaringan untuk layanan tambahan. Untuk informasi selengkapnya, lihat Acara aktivitas jaringan.	30 Mei 2025
Fungsionalitas baru	Anda sekarang dapat memperkaya peristiwa CloudTrail manajemen dan peristiwa data untuk meningkatkan hasil saat Anda mengkategorikan, mencari, dan menganalisis peristiwa. CloudTrail Untuk informasi selengkapnya, lihat Memperkaya CloudTrail peristiwa dengan menambahkan kunci tag sumber daya dan kunci kondisi global IAM.	29 Mei 2025

Fungsionalitas baru	Menambahkan dokumentasi dan informasi kebijakan untuk peran terkait `AWSServiceRoleForCloudTrailEventContext` layanan. Untuk informasi selengkapnya, lihat Menggunakan peran untuk membuat dan mengelola konteks CloudTrail acara di CloudTrail.	29 Mei 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mengenkripsi file log dan mencerna file dengan AWS KMS keys ()SSE-KMS. Untuk informasi selengkapnya, lihat Mengenkripsi file CloudTrail log dengan AWS KMS keys () SSE-KMS.	22 Mei 2025
Ditambahkan fungsionalitas	Anda sekarang dapat menggunakan pemilih acara lanjutan tambahan dan templat yang telah ditentukan untuk mencatat peristiwa data ke jejak Anda. Untuk informasi selengkapnya, lihat Peristiwa data.	April 10, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa aktivitas jaringan untuk AWS Lambda dan Amazon Comprehend. Untuk informasi selengkapnya, lihat Acara aktivitas jaringan.	April 10, 2025

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di set konfigurasi Amazon Simple Email Service, identitas email, dan templat. Untuk informasi selengkapnya, lihat Peristiwa data.	April 10, 2025
Ditambahkan fungsionalitas	AWS CloudTrail sekarang mendukung kebijakan titik akhir VPC. Untuk informasi selengkapnya, lihat Menggunakan AWS CloudTrail dengan titik akhir VPC Amazon.	April 9, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa aktivitas CloudTrail jaringan untuk AWS IoT FleetWise.	April 8, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data di sesi Amazon Bedrock dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Maret 19, 2025

Dokumentasi diperbarui	Memperbarui skema SQL untuk acara CloudTrail Lake Insights. Menambahkan topik baru untuk menjelaskan bidang catatan acara Wawasan untuk jejak dan penyimpanan data acara. Untuk informasi selengkapnya tentang skema SQL yang didukung untuk acara CloudTrail Lake Insights, lihat Skema yang didukung untuk bidang catatan peristiwa CloudTrail Insights.	Maret 13, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di aplikasi Amazon GameLift Streams dan grup streaming dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	7 Maret 2025
Menambahkan dukungan layanan	Rilis ini mendukung integrasi Terkelola untuk AWS IoT Device Management. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail.	Maret 3, 2025

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di aplikasi penargetan seluler Amazon Pinpoint dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Februari 24, 2025
Ketersediaan umum acara aktivitas jaringan	Acara aktivitas jaringan sekarang tersedia secara umum. Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.	Februari 13, 2025
Dokumentasi diperbarui	Menambahkan Memahami jalur Multi-wilayah dan topik Wilayah keikutsertaan untuk menggambarkan jalur Multi-wilayah dan Wilayah keikutsertaan.	Februari 10, 2025
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di titik akhir regional Amazon Timestream dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Januari 31, 2025

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di prompt dan AWS Step Functions aktivitas Amazon Bedrock dengan menggunak an pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Januari 24, 2025
Dokumentasi diperbarui	Menambahkan topik kueri Optimize CloudTrail Lake untuk memberikan panduan tentang cara mengoptim alkan kueri CloudTrail Danau untuk meningkatkan kinerja dan keandalan. Topik ini mencakup teknik pengoptim alan khusus serta solusi untuk kegagalan kueri umum.	Januari 22, 2025
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Meksiko (Tengah). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	Januari 13, 2025
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Asia Pasifik (Thailand). Untuk informasi selengkap nya, lihat Wilayah yang CloudTrail didukung.	Januari 7, 2025

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada pekerjaan AWS Backup pencarian dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Desember 30, 2024
Dokumentasi diperbarui	Mengonversi topik peristiwa Logging Insights menjadi sebuah chapter bernama Working with CloudTrail Insights. Bab ini mencakup bagian baru tentang biaya acara Wawasan dan melihat peristiwa Wawasan untuk penyimpanan data acara.	Desember 23, 2024
Support untuk IPv6	CloudTrail menambahkan dukungan untuk IPv6.	Desember 20, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS Signer penandatanganan pekerjaan dan profil dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Desember 20, 2024

Dokumentasi diperbarui	Memperbarui bagian layanan dan integrasi yang CloudTrail didukung untuk menyertakan deskripsi integrasi AWS Config, AWS Audit Manager, dan Amazon Athena dengan Lake. CloudTrail	Desember 18, 2024
Menambahkan dukungan layanan	Rilis ini mendukung AWS Migration Hub Journeys. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging AWS Migration Hub Journeys API call dengan AWS CloudTrail.	Desember 3, 2024
Menambahkan dukungan layanan	Rilis ini mendukung Oracle AWS Database@. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging Oracle Database@AWS API Calls dengan. AWS CloudTrail	Desember 1, 2024
Menambahkan dukungan layanan	Rilis ini mendukung AWS Security Incident Response. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging AWS Security Incident Response API call menggunakan AWS CloudTrail.	Desember 1, 2024

Ditambahkan fungsionalitas	CloudTrail Lake menambahkan dukungan untuk dasbor khusus, dasbor Sorotan, dan dasbor terkelola baru. Anda dapat membuat dasbor khusus dan menambahkan hingga 10 widget ke setiap dasbor khusus. Anda dapat mengaktifkan dasbor Sorotan untuk melihat ikhtisar sekilas tentang AWS aktivitas yang dikumpulkan oleh penyimpanan data acara di akun Anda. Untuk informasi lebih lanjut, lihat Dasbor CloudTrail danau.	November 21, 2024
Ditambahkan fungsionalitas	CloudTrail Lake menambahkan dukungan untuk kebijakan berbasis sumber daya pada penyimpanan data acara. Anda dapat menggunakan kebijakan berbasis sumber daya untuk menyediakan akses lintas akun untuk mengizinkan prinsipal yang dipilih menanyakan penyimpanan data acara, mencantumkan dan membatalkan kueri, serta melihat hasil kueri. Untuk informasi selengkapnya, lihat contoh Resource-based kebijakan untuk penyimpanan data peristiwa.	November 21, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS AppSync GraphQL API dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	November 19, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada percakapan AWS IoT SiteWise Asisten dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	November 18, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada pesan SMS AWS End User Messaging dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	November 15, 2024
Ditambahkan fungsionalitas	Ditambahkan dukungan untuk `assumedRoot` `sessionContext` bidang untuk `userIdentity` elemen. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity dalam panduan ini dan Lacak tugas istimewa CloudTrail di Panduan Pengguna IAM.	November 14, 2024

Ketersediaan umum asisten kueri CloudTrail Lake	Asisten kueri CloudTrail Danau sekarang tersedia secara umum. Asisten kueri memungkinkan Anda membuat kueri SQL dari petunjuk bahasa alami dalam bahasa Inggris. Untuk informasi selengkapnya, lihat Membuat kueri CloudTrail Danau dari petunjuk bahasa alami.	November 12, 2024
Ditambahkan fungsionalitas	Memperkenalkan fitur pratinjau untuk kueri CloudTrail Lake yang menggunakan kemampuan kecerdasan buatan generatif (AI generatif) untuk meringkas hasil kueri. Untuk informasi selengkap nya, lihat Meringkas hasil kueri dalam bahasa alami.	November 12, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mengonfigurasi bidang pemilih acara lanjutan tambahan untuk penyimpanan data acara CloudTrail Lake, yang memberi Anda kontrol lebih besar atas CloudTrail peristiwa mana yang dicerna ke dalam penyimpanan data acara Anda. Anda dapat memfilter peristiwa manajemen pada bidang pemilih acara lanjutan berikut: `eventName` (baru),`eventSource` , `eventType` (baru)`readOnly`, `sessionCredentialFromConsole` (baru), dan `userIdentity.arn` (baru). Anda dapat memfilter peristiwa data pada bidang pemilih acara lanjutan berikut:`eventName` , `eventSource` (baru), `eventType` (baru),,`resources.type` , `resources.ARN` `readOnly`, `sessionCredentialFromConsole` (baru), dan `userIdentity.arn` (baru). Untuk informasi selengkapnya, lihat Membuat penyimpanan data CloudTrail acara untuk acara dengan konsol (langkah 16 dan 17).	November 11, 2024

Diperbarui versi acara	Diperbarui `eventVersion` ke `1.11` dan menambahkan `inScopeOf` bidang untuk `userIdentity` elemen. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.	Oktober 29, 2024
Menambahkan dukungan layanan	Rilis ini mendukung SMS Pesan Pengguna AWS Akhir. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Pencatatan panggilan API SMS Pesan Pengguna AWS Akhir menggunakan AWS CloudTrail.	Oktober 22, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada identitas originasi SMS AWS End User Messaging dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Oktober 22, 2024
Menambahkan dukungan layanan	Rilis ini mendukung AWS End User Messaging Social. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Pencatatan panggilan API Sosial Pesan Pengguna AWS Akhir menggunakan AWS CloudTrail.	Oktober 10, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada ID nomor telepon Sosial Pesan Pengguna AWS Akhir dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Oktober 10, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada model dan AWS Data Exchange aset Amazon Bedrock dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	September 27, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mengonfigurasi jejak dan penyimpanan data peristiwa untuk mencatat peristiwa aktivitas CloudTrail jaringan (dalam pratinjau). Peristiwa aktivitas jaringan memungkinkan pemilik titik akhir VPC merekam panggilan AWS API yang dilakukan menggunakan titik akhir VPC mereka dari VPC pribadi ke. Layanan AWS Rilis ini mendukung pencatatan peristiwa aktivitas jaringan untuk sumber peristiwa berikut:`cloudtrail.amazonaws.com` ,`ec2.amazonaws.com` ,`kms.amazonaws.com` , dan`secretsmanager.amazonaws.com` . Untuk informasi selengkapnya, lihat Mencatat peristiwa aktivitas jaringan.	September 24, 2024
Menambahkan dukungan layanan	Rilis ini mendukung Directory Service Data. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging Directory Service Data API menggunakan panggilan AWS CloudTrail.	September 18, 2024

Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Asia Pasifik (Malaysia). Untuk informasi selengkap nya, lihat Wilayah yang CloudTrail didukung.	Agustus 22, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data di monitor aplikasi Amazon CloudWatch RUM dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Juli 25, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mengontrol akses ke jalur menggunakan tag. Untuk informasi lebih lanjut, lihat ABAC dengan CloudTrail.	Juli 23, 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada pengguna Amazon One Enterprise dan UKeys dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Juli 23, 2024

Ditambahkan fungsionalitas	Sekarang Anda dapat mencatat peristiwa CloudTrail data di alias dan pagar pembatas aliran Amazon Bedrock, dan aktivitas API tingkat objek Amazon S3 di bucket direktori dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	9 Juli 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS Payment Cryptography kunci dan alias dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Juli 5, 2024
Ditambahkan fungsionalitas	Memperkenalkan fitur pratinjau untuk kueri CloudTrail Lake yang menggunakan kemampuan kecerdasan buatan generatif (AI generatif) untuk menghasilkan kueri SQL dari prompt bahasa Inggris. Untuk informasi selengkapnya, lihat Membuat kueri CloudTrail Lake dari petunjuk bahasa Inggris.	Juni 11, 2024

Ditambahkan fungsionalitas	Sekarang Anda dapat mencatat peristiwa CloudTrail data di CloudWatch metrik Amazon, model Amazon Machine Learning, dan AWS Private CA dengan menggunakan penyeleksi peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Juni 5, 2024
Dokumentasi diperbarui	Menambahkan bagian untuk menjelaskan cara memfilter peristiwa data dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Memfilter peristiwa data menggunakan pemilih peristiwa lanjutan.	29 Mei 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di Amazon Kinesis Data Streams dan streaming konsumen dengan menggunakan pemilih peristiwa tingkat lanjut. Untuk informasi selengkapnya, lihat Peristiwa data.	21 Mei 2024

Dokumentasi diperbarui	Memperbarui halaman Wilayah yang didukung CloudTrail Danau untuk menambahkan Wilayah Asia Pasifik (Hyderabad) (ap-south-2), Wilayah Eropa (Zurich) (eu-central-2), dan Wilayah Israel (Tel Aviv) (il-central-1).	16 Mei 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada mesin AWS Step Functions status dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	16 Mei 2024
Dokumentasi diperbarui	Menambahkan bagian tentang melihat CloudTrail biaya dan penggunaan penggunaan AWS Cost Explorer. Untuk informasi selengkapnya, lihat Melihat CloudTrail biaya dan penggunaan Anda dengan AWS Cost Explorer.	14 Mei 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di Amazon Q Apps dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	1 Mei 2024

Dokumentasi diperbarui	Perbaikan organisasi umum pada bagian panduan pengguna dan judul halaman, yang meliputi: Mengubah judul halaman referensi peristiwa CloudTrail log menjadi Memahami CloudTrail peristiwa dan menambahkan deskripsi peristiwa manajemen, peristiwa data, dan peristiwa Wawasan. Mengubah judul halaman Pengaturan menjadi Konfigurasi CloudTrail pengaturan. Memindahkan peristiwa data Logging, peristiwa manajemen logging, dan halaman peristiwa Wawasan Logging ke bagian Memahami CloudTrail peristiwa. Memindahkan halaman contoh file CloudTrail CloudTrail log ke bagian file log. Menambahkan halaman terpisah untuk mencantumkan AWS CLI perintah untuk penyimpanan, kueri, dan integrasi data acara CloudTrail Lake.	April 10, 2024
Dokumentasi diperbarui	Memperbarui halaman Wilayah yang didukung CloudTrail Danau untuk menambahkan Wilayah Eropa (Spanyol) (eu-south-2).	April 10, 2024

Menambahkan dukungan layanan	Rilis ini mendukung Katalog AWS Kontrol. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail panggilan API Katalog AWS Kontrol Logging yang menggunakan AWS CloudTrail.	April 8, 2024
Menambahkan dukungan layanan	Rilis ini mendukung AWS Deadline Cloud. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail.	April 2, 2024
Diperbarui versi acara	Versi AWS CloudTrail acara sekarang 1.10. Untuk informasi selengkapnya, lihat CloudTrail merekam konten.	26 Maret 2024
Menambahkan dukungan layanan	Rilis ini mendukung AWS Billing Conductor. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging panggilan AWS Billing Conductor API menggunakan AWS CloudTrail.	Maret 12, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS X-Ray jejak dan node AWS Systems Manager terkelola dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	7 Maret 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di domain Amazon Simple Workflow Service (Amazon SWF) dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	Februari 14, 2024
Ditambahkan fungsionalitas	CloudTrail menambahkan `ListInsightsMetricData` API. `ListInsightsMetricData` API menampilkan data metrik Insights untuk jejak yang telah mengaktifkan Insights. Untuk informasi selengkapnya, lihat ListInsightsMetricData di dalam Referensi API AWS CloudTrail .	Februari 6, 2024

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data untuk AWS IoT, AWS IoT SiteWise, dan AWS AppConfig dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	4 Januari 2024
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data AWS IoT Greengrass dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	22 Desember 2023
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Kanada Barat (Calgary). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	20 Desember 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data untuk Amazon Keyspaces (untuk Apache Cassandra), AWS IoT TwinMaker Amazon RDS, dan Rantai Pasokan AWS dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	20 Desember 2023

Kebijakan AWS terkelola yang diperbarui	Memperbarui kebijakan CloudTrailServiceRolePolicy terkelola untuk mengizinkan tindakan berikut pada penyimpanan data acara organisasi saat federasi dinonaktifkan: `glue:DeleteTable` dan `lakeformation:DeregisterResource` .	26 November 2023
Ditambahkan fungsionalitas	Anda sekarang dapat menggabungkan penyimpanan data peristiwa CloudTrail Lake untuk melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog AWS Glue Data dan menjalankan kueri SQL pada data peristiwa menggunakan Amazon Athena. Metadata tabel yang disimpan dalam Katalog AWS Glue Data memungkinkan mesin kueri Athena mengetahui cara menemukan, membaca, dan memproses data yang ingin Anda kueri. Untuk informasi selengkapnya, lihat Menggabungkan penyimpanan data peristiwa.	26 November 2023

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data AWS Cloud Map dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	16 November 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data pada pesan Amazon SQS dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	16 November 2023

Ditambahkan fungsionalitas	CloudTrail Lake sekarang menawarkan dua opsi harga untuk penyimpanan data acara: harga retensi yang dapat diperpanjang satu tahun dan harga retensi tujuh tahun. Opsi penetapan harga menentukan biaya untuk menelan dan menyimpan peristiwa, dan periode retensi default dan maksimum untuk penyimpanan data acara. Sebelum rilis ini, semua penyimpanan data acara menggunakan opsi harga retensi tujuh tahun. Anda dapat mengalihkan penyimpanan data peristiwa dari menggunakan opsi penetapan harga retensi tujuh tahun menjadi menggunak an harga retensi yang dapat diperpanjang satu tahun dengan menggunakan CloudTrailkonsol AWS CLI, atau operasi API. UpdateEve ntDataStore Untuk informasi selengkapnya tentang opsi AWS CloudTrail penetapan harga, lihat Opsi harga penyimpanan data dan acara.	15 November 2023

Ditambahkan fungsionalitas	Anda sekarang dapat mengumpulkan acara Wawasan di CloudTrail Danau. AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan tingkat panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen. Untuk mengumpulkan peristiwa Wawasan di CloudTrail Danau, Anda memerlukan penyimpanan data peristiwa sumber yang mencatat peristiwa manajemen dan mengaktifkan Wawasan dan penyimpanan data acara tujuan yang mengumpul kan peristiwa Wawasan berdasarkan aktivitas peristiwa manajemen yang tidak biasa di penyimpanan data acara sumber. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk peristiwa CloudTrai l Wawasan dan peristiwa Wawasan Pencatatan.	9 November 2023

Menambahkan dukungan layanan	Rilis ini mendukung AWS Launch Wizard. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging panggilan AWS Launch Wizard API menggunakan AWS CloudTrail.	8 November 2023
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Bedrock. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Log panggilan Amazon Bedrock API menggunakan AWS CloudTrail.	23 Oktober 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di CodeWhisperer kustomisasi Amazon dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	18 Oktober 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di database dan tabel Amazon Timestream dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	28 September 2023

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada topik Amazon SNS dan titik akhir platform dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	28 September 2023
Dokumentasi diperbarui	Tabel yang ditambahkan untuk menampilkan tugas yang dapat dilakukan oleh akun manajemen, akun administrator yang didelegasikan, dan akun anggota dalam AWS Organizations CloudTrail organisasi. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan organisasi.	25 September 2023
Menambahkan dukungan layanan	Rilis ini mendukung AWS Marketplace Perjanjian. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail dan Logging Agreements API Calls menggunakan AWS CloudTrail.	1 September 2023

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di aliran video Amazon Kinesis dan titik akhir Amazon SageMaker AI dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	31 Agustus 2023
Menambahkan dukungan layanan	Rilis ini mendukung Layanan Transformasi AWS Aplikasi. AWS Layanan Transformasi Aplikasi adalah layanan backend yang digunakan oleh layanan seperti AWS Microservice Extractor untuk.NET. Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung.	Agustus 26, 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS Private CA Connector for Active Directory dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	24 Agustus 2023

Dokumentasi diperbarui	Menambahkan skenario CloudTrail Lake baru untuk menunjukkan cara membuat penyimpanan data peristiwa , melihat dasbor CloudTrai l Danau, menyalin peristiwa jejak ke penyimpanan data peristiwa, melihat dan menjalankan kueri sampel, dan menyimpan hasil kueri ke bucket Amazon S3 menggunakan. Konsol Manajemen AWS Untuk informasi lebih lanjut, lihat Skenario untuk CloudTrail Danau	16 Agustus 2023
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Israel (Tel Aviv). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	1 Agustus 2023
Menambahkan dukungan layanan	Rilis ini mendukung AWS HealthImaging. Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung serta panggilan Logging AWS HealthImaging API menggunakan AWS CloudTrai l.	26 Juli 2023

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada penyimpanan AWS HealthImaging data dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	26 Juli 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di saluran AWS Systems Manager kontrol dan jaringan Amazon Managed Blockchain dengan menggunakan pemilih acara tingkat lanjut. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	Juni 21, 2023
Ditambahkan fungsionalitas	Anda sekarang dapat memverifikasi hasil kueri yang disimpan CloudTrail Lake Anda menggunakan aws cloudtrail verify-query-resul ts perintah. Untuk informasi selengkapnya, lihat Memvalida si hasil kueri yang disimpan dengan. AWS CLI	Juni 21, 2023

Menambahkan dukungan layanan	Rilis ini mendukung Izin Terverifikasi Amazon. Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung dan Pencatatan panggilan API Izin Terverifikasi Amazon menggunakan. AWS CloudTrail	13 Juni 2023
Ditambahkan fungsionalitas	Anda sekarang dapat menggunakan dasbor CloudTrail Danau untuk memvisualisasikan peristiwa di penyimpanan data acara. Untuk informasi selengkapnya, lihat Lihat dasbor Danau.	13 Juni 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di toko kebijakan Izin Terverifikasi Amazon dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	13 Juni 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di CodeWhisperer profil Amazon dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	6 Juni 2023

Ditambahkan fungsionalitas	Anda sekarang dapat memulai dan menghentikan konsumsi acara di penyimpanan data CloudTrail acara. Untuk informasi tentang menghentikan konsumsi acara menggunakan konsol, lihat Menghentikan penyimpanan data peristiwa dari menelan peristiwa. Untuk informasi tentang menghentikan konsumsi acara menggunakan AWS CLI, lihat Menghentikan konsumsi pada penyimpanan data acara.	Juni 2, 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di ruang kerja log write-ahead Amazon EMR dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	31 Mei 2023
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Security Lake. Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung serta Pencatatan panggilan Amazon Security Lake API menggunakan AWS CloudTrail.	30 Mei 2023
Diperbarui versi acara	Sekarang 1,09. `eventVersion`	23 Mei 2023

Dokumentasi diperbarui	Topik elemen CloudTrail UserIdentity yang diperbaru i untuk menyertakan contoh dan deskripsi bidang untuk permintaan yang dibuat atas nama pengguna Pusat Identitas IAM. Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.	23 Mei 2023
Dokumentasi diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Processing Library: CloudTrai l aws-cloudtrail-processing-library-1.6.1.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	23 Mei 2023
Ditambahkan fungsionalitas	CloudTrail Lake sekarang mendukung semua fungsi dan operator Presto. Untuk informasi selengkapnya, lihat kendala CloudTrail Lake SQL.	9 Mei 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada GuardDuty detektor Amazon dengan menggunak an pemilih peristiwa lanjutan. Untuk informasi selengkap nya, lihat Mencatat peristiwa data dan Mencatat panggilan Amazon GuardDuty API dengan AWS CloudTrail.	30 Maret 2023

Dokumentasi diperbarui	Menambahkan bagian baru tentang membuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara. Untuk informasi selengkapnya, lihat Membuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake.	24 Maret 2023
Menambahkan dukungan layanan	Rilis ini mendukung AWS Telco Network Builder (AWS TNB). Untuk informasi selengkapnya, lihat layanan dan integrasi yang CloudTrail didukung dan Pencatatan panggilan API Pembuat Jaringan AWS Telco menggunakan. AWS CloudTrail	21 Februari 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di kumpulan identitas Amazon Cognito dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	15 Februari 2023
Dokumentasi diperbarui	Menambahkan bagian baru tentang sumber belajar yang tersedia untuk CloudTrail Lake. Untuk informasi selengkapnya, lihat Sumber belajar.	9 Februari 2023

Ditambahkan fungsionalitas	Anda sekarang dapat membuat integrasi CloudTrail Danau dengan sumber acara di luar. AWS Anda dapat mencatat dan menyimpan data aktivitas pengguna dari sumber apa pun di lingkungan hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau wadah. Untuk informasi selengkapnya, lihat Membuat integrasi dengan sumber acara di luar AWS.	31 Januari 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada CloudTrail `PutAuditEvents` aktivitas di saluran CloudTrail Lake dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	31 Januari 2023
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Asia Pasifik (Melbourne). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	Januari 24, 2023

Dokumentasi diperbarui	Menambahkan bagian baru tentang mengelola konsisten si data di CloudTrail, lihat Mengelola konsistensi data di CloudTrail.	18 Januari 2023
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data di toko fitur Amazon SageMaker AI dengan menggunakan pemilih acara tingkat lanjut. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	Desember 27, 2022
Menambahkan dukungan layanan	Rilis ini mendukung AWS Marketplace Discovery. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	15 Desember 2022
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrai l data di komponen uji coba eksperimen metrik Amazon SageMaker AI dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	15 Desember 2022

Ditambahkan fungsionalitas	Anda sekarang dapat membuat penyimpanan data peristiwa untuk menyertakan item AWS Config konfigurasi, dan menggunakan penyimpanan data peristiwa untuk menyelidiki perubahan yang tidak sesuai pada lingkungan produksi Anda. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk item AWS Config konfigurasi.	28 November 2022
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Asia Pasifik (Hyderabad). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	22 November 2022
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data di Amazon FinSpace lingkungan dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	18 November 2022
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Eropa (Spanyol). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	16 November 2022

Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Eropa (Zurich). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	9 November 2022
Ditambahkan fungsionalitas	Akun manajemen untuk AWS Organizations organisasi sekarang dapat menambahkan administrator yang didelegasikan untuk mengelola CloudTrail jejak organisasi dan penyimpanan data acara. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan organisasi.	7 November 2022
Ditambahkan fungsionalitas	Anda sekarang dapat mengaktifkan AWS Key Management Service enkripsi untuk penyimpanan data acara CloudTrail Lake. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara.	7 November 2022

Ditambahkan fungsionalitas	Anda sekarang dapat menyimpan hasil kueri CloudTrail Lake ke bucket Amazon S3 saat menjalank an kueri. Untuk informasi selengkapnya tentang menjalankan kueri, lihat Menjalankan kueri dan menyimpan hasil kueri. Untuk informasi selengkapnya tentang mengunduh hasil kueri, lihat Mendapatkan dan mengunduh hasil kueri yang disimpan.	21 Oktober 2022
Ditambahkan fungsionalitas	Anda sekarang dapat menyalin peristiwa CloudTrai l jejak ke penyimpanan data acara CloudTrail Lake. Untuk informasi lebih lanjut, lihat Menyalin acara jejak ke CloudTrail Danau.	19 September 2022
Dokumentasi diperbarui	Menambahkan daftar CloudWatch metrik Amazon yang didukung untuk CloudTrail Lake. Untuk informasi selengkapnya, lihat CloudWatch Metrik yang didukung.	September 16, 2022

Ditambahkan fungsionalitas	Anda sekarang dapat melihat saluran CloudTrail terkait layanan menggunakan. AWS CLI Untuk informasi selengkapnya, lihat Melihat saluran terkait layanan untuk CloudTrail menggunakan. AWS CLI	9 September 2022
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Timur Tengah (UEA). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	30 Agustus 2022
Fungsionalitas berubah	CloudTrail telah mengubah nama kebijakan yang dikelola `AWSCloudTrailReadOnlyAccess` menjadi `AWSCloudTrail_ReadOnlyAccess` . Izin dalam kebijakan ini telah dicakup. Secara default, kebijakan tidak lagi memberikan izin untuk mencantumkan semua bucket, fungsi AWS Lambda , atau alias Amazon S3. AWS KMS Untuk informasi selengkapnya, lihat Read-only akses.	6 Juni 2022

Fungsionalitas berubah	Sebagai praktik terbaik keamanan, Anda sekarang dapat menambahkan kunci `aws:SourceArn` atau `aws:SourceAccount` kondisi ke blok pemeriksaan `s3:GetBucketAcl` ACL di kebijakan bucket Amazon S3. Untuk selengkapnya, lihat Mengonfigurasi kebijakan bucket Amazon S3 untuk informasi selengkapnya. CloudTrail	Mei 11, 2022
Fungsionalitas berubah	Mulai 24 Februari 2022, AWS CloudTrail mulai mengubah nilai `sourceIPAddress` bidang `userAgent` dan dalam hal apa pun yang berasal dari Konsol Manajemen AWS sesi di mana klien proxy digunakan. Untuk acara ini, CloudTrail ganti nilai `userAgent` dan `sourceIPAddress` bidang dengan`AWS Internal`. CloudTrai lmembuat perubahan ini untuk menstandarisasi cara log informasi untuk tindakan layanan di semua AWS layanan. Untuk informasi selengkapnya, lihat CloudTrail merekam konten.	12 April 2022

Menambahkan dukungan layanan	Rilis ini mendukung Amazon GameSparks. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	24 Maret 2022
Menambahkan dukungan layanan	Rilis ini mendukung AWS App Mesh Layanan Manajemen Utusan. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	18 Maret 2022
Dokumentasi diperbarui	Contoh kueri baru telah ditambahkan untuk CloudTrail Lake, fitur baru yang memungkinkan Anda menjalankan kueri SQL multi-bidang berbutir halus pada acara Anda. Juga, bidang baru,`BytesScanned` , telah ditambahkan ke hasil metadata kueri `DescribeQuery` dan `GetQueryResults` operasi. Untuk informasi lebih lanjut, lihat Bekerja dengan CloudTrail Danau.	4 Maret 2022

Fungsionalitas berubah	CloudTrail sekarang menghapus ID akun pemilik bucket Amazon S3 di `resources` blok peristiwa data jika kedua kondisi berikut terpenuhi: panggilan API peristiwa data berasal dari AWS akun yang berbeda dari pemilik bucket Amazon S3, dan pemanggil API menerima kesalahan yang hanya untuk `AccessDenied` akun pemanggil. Untuk informasi selengkapnya, lihat Menyuntin g ID akun pemilik bucket untuk peristiwa data yang dipanggil oleh akun lain.	3 Maret 2022

Dokumentasi diperbarui	Pembaruan ini mendukung rilis berikut untuk Pustaka CloudTrail Pemrosesan: Menambahkan dukungan untuk mengimplementasikan pengelola S3 kustom, pencatatan peristiwa untuk mencatat pengecualian terkait penguraian file, dukungan untuk mengurai `errorCode` bidang opsional di`insightDetails` , dan memperbarui regex penguraian ID akun untuk menerima nilai non-numerik. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	28 Januari 2022

Ditambahkan fungsionalitas	CloudTrail memperkenalkan CloudTrail Lake, fitur baru yang memungkinkan Anda menjalankan kueri SQL multi-bidang berbutir halus pada acara Anda. Peristiwa digabungkan ke dalam penyimpanan data peristiwa, yang merupakan kumpulan peristiwa yang tidak dapat diubah berdasarkan kriteria yang Anda pilih dengan menerapkan pemilih acara tingkat lanjut. Untuk informasi lebih lanjut, lihat Bekerja dengan CloudTrail Danau.	5 Januari 2022
Dukungan Wilayah Baru	CloudTrail memperluas dukungan ke Wilayah baru, Wilayah Asia Pasifik (Jakarta). Untuk informasi selengkapnya, lihat Wilayah yang CloudTrail didukung.	13 Desember 2021
Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkSpaces Web. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	Desember 3, 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada AWS Glue tabel yang dibuat oleh Lake Formation dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	30 November 2021

Fungsionalitas berubah	Sebagai praktik terbaik keamanan, kini Anda dapat menambahkan kunci `aws:SourceArn` atau `aws:SourceAccount` kondisi ke kebijakan AWS KMS utama dan kebijakan bucket Amazon S3. Untuk informasi selengkapnya, lihat Mengonfigurasi kebijakan AWS KMS utama untuk CloudTrail dan Mengonfigurasi kebijakan bucket Amazon S3 untuk. CloudTrail	15 November 2021
Menambahkan dukungan layanan	Rilis ini mendukung AWS Resilience Hub. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	November 10, 2021
Ditambahkan fungsionalitas	Jenis peristiwa CloudTrai l Insights baru tersedia: peristiwa Insights tingkat kesalahan. Peristiwa Insights tingkat kesalahan menangkap aktivitas yang tidak biasa pada kesalahan yang terjadi pada API yang dipanggil di akun Anda. Untuk informasi selengkapnya, lihat peristiwa Logging Insights untuk jejak.	November 10, 2021

Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa CloudTrail data pada aliran DynamoDB dengan menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	22 September 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data di jalur akses Amazon S3. Anda dapat mencatat peristiwa data titik akses Amazon S3 dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	Agustus 24, 2021
Fungsionalitas berubah	Saat Anda mengonfigurasi jejak untuk mengirim notifikasi ke Amazon SNS, CloudTrail tambahkan pernyataan kebijakan ke kebijakan akses topik SNS Anda yang memungkinkan CloudTrail untuk mengirim konten ke topik SNS. Sebagai praktik keamanan terbaik, kami sarankan untuk menambahkan kunci `aws:SourceArn` atau `aws:SourceAccount` kondisi ke pernyataan CloudTrail kebijakan. Untuk informasi selengkapnya, lihat kebijakan topik Amazon SNS untuk. CloudTrail	16 Agustus 2021

Menambahkan dukungan layanan	Rilis ini mendukung Amazon Route 53 Application Recovery Controller. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	27 Juli 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data di Amazon EBS direct API yang dijalankan pada snapshot EBS. Anda dapat mencatat peristiwa data API langsung Amazon EBS dengan menggunakan pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	27 Juli 2021
Fungsionalitas berubah	Saat CloudTrail memproses peristiwa data, ia mempertahankan angka dalam format aslinya, apakah itu integer (`int`) atau a. `float` Dalam peristiwa yang memiliki bilangan bulat di bidang peristiwa data, CloudTrail secara historis memproses angka-angka ini sebagai pelampung. Sekarang, CloudTrail simpan format asli bilangan bulat dalam peristiwa data. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan.	13 Juli 2021

Ditambahkan fungsionalitas	Anda sekarang dapat mengecualikan peristiwa manajemen Amazon RDS Data API dari jejak Anda. Untuk informasi selengkapnya, lihat Peristiwa pengelolaan log untuk jejak.	1 Juli 2021
Menambahkan dukungan layanan	Rilis ini mendukung AWS BugBust. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	24 Juni 2021
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Managed Grafana dan Amazon Managed Service untuk Prometheus. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	2 Juni 2021
Menambahkan dukungan layanan	Rilis ini mendukung AWS App Runner. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	18 Mei 2021
Menambahkan dukungan layanan	Rilis ini mendukung Manajer AWS Systems Manager Insiden. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	10 Mei 2021

Dokumentasi diperbarui	Pembaruan ini menjelaskan persyaratan pencatatan peristiwa data untuk paket AWS Config kesesuaian, terutama untuk kerangka kerja kepatuhan seperti HIPAA atau FedRAMP. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	7 Mei 2021
Menambahkan dukungan layanan	Rilis ini mendukung Service Quotas dan Amazon EBS direct API. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	13 April, 2021
Ditambahkan fungsionalitas	Setelah administrator IAM mengonfigurasi AWS STS, CloudTrail mencatat `sourceIdentity` informasi dalam peristiwa saat pengguna mengambil peran IAM, atau melakukan tindakan apa pun dengan peran yang diasumsikan. Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.	13 April, 2021
Dokumentasi diperbarui	Pemutakhiran dokumen ini membatasi, dalam kilobyte (KB), untuk konten di beberapa bidang catatan CloudTrail peristiwa. Untuk informasi selengkapnya, lihat CloudTrail merekam konten.	8 April 2021

Ditambahkan fungsionalitas	Setelah administrator IAM mengonfigurasi AWS STS, CloudTrail mencatat `sourceIdentity` informasi dalam peristiwa saat pengguna mengambil peran IAM, atau melakukan tindakan apa pun dengan peran yang diasumsikan. Untuk informasi selengkapnya, lihat Elemen CloudTrail UserIdentity.	6 April 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data di tabel Amazon DynamoDB. Anda dapat mencatat peristiwa data DynamoDB dengan menggunakan penyeleksi acara atau pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	23 Maret 2021
Menambahkan dukungan layanan	Rilis ini mendukung Alur Kerja Terkelola Amazon untuk Apache Airflow. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	22 Maret 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data pada titik akses Objek Lambda S3 jika Anda telah memilih untuk menggunakan pemilih acara lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	18 Maret 2021

Menambahkan dukungan layanan	Rilis ini mendukung AWS Fault Injection Simulator. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	15 Maret 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data pada node Ethereum di Amazon Managed Blockchain jika Anda telah memilih untuk menggunakan pemilih acara tingkat lanjut. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	1 Maret 2021
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Managed Blockchain dan pratinjau Ethereum untuk Managed Blockchain. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	4 Februari 2021
Menambahkan dukungan layanan	Rilis ini mendukung AWS Amplify. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	3 Februari 2021
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Lookout for Metrics. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	1 Februari 2021

Dokumentasi diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: Perbarui referensi file.jar dalam panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.4.0.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	12 Januari 2021
Ditambahkan fungsionalitas	Anda sekarang dapat mencatat peristiwa data di Amazon S3 aktif. AWS Outposts Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	21 Desember 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Lookout for Equipment AWS Well-Architected Tool,, dan Amazon Location Service. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	16 Desember 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT Greengrass V2. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	15 Desember 2020

Menambahkan dukungan layanan	Rilis ini mendukung Amazon EMR di EKS. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	10 Desember 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS Audit Manager dan Amazon HealthLake. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	8 Desember 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Lookout for Vision. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	1 Desember 2020
Diperbarui versi acara	Versi AWS CloudTrail acara sekarang 1.08. Versi 1.08 memperkenalkan bidang baru untuk. CloudTrail Untuk informasi selengkapnya, lihat CloudTrail merekam konten.	24 November 2020

Ditambahkan fungsionalitas	AWS CloudTrail memperkenalkan pemilih acara lanjutan untuk peristiwa data. Penyeleksi acara tingkat lanjut memungkinkan kontrol yang lebih halus atas peristiwa data yang Anda log ke jejak Anda. Anda dapat menyertakan atau mengecualikan peristiwa data untuk AWS sumber daya tertentu, dan memilih API tertentu pada sumber daya tersebut untuk masuk ke jejak Anda. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	24 November 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS Network Firewall. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	17 November 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS Trusted Advisor. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	22 Oktober 2020
Dokumentasi diperbarui	Menambahkan dua contoh baru catatan peristiwa untuk peristiwa login pengguna root. Untuk informasi selengkapnya, lihat Acara login AWS konsol.	13 Oktober 2020

Fungsionalitas berubah	Izin dalam `AWSCloudTrail_FullAccess` kebijakan telah dipersempit. Kebijakan ini tidak lagi memungkinkan Anda untuk menghapus topik Amazon SNS atau bucket Amazon S3, dan `getObject` tindakan telah dihapus. Untuk informasi selengkapnya, lihat Memberikan izin khusus untuk CloudTrail pengguna.	29 September 2020
Dokumentasi diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: Perbarui referensi file.jar dalam panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.3.0.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	28 Agustus 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS Outposts. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	28 Agustus 2020

Ditambahkan fungsionalitas	AWS CloudTrail Wawasan memperkenalkan bidang atribusi untuk CloudTrai l acara Wawasan. Kolom atribusi menampilkan identitas pengguna teratas, agen pengguna, dan kode kesalahan yang terkait dengan aktivitas anomali yang memicu peristiwa Wawasan. Sebagai perbandingan, bidang atribusi juga menampilkan identitas pengguna teratas, agen pengguna, dan kode kesalahan yang terkait dengan aktivitas normal atau dasar. Untuk informasi selengkap nya, lihat peristiwa Logging Insights.	13 Agustus 2020
Ditambahkan fungsionalitas	AWS CloudTrail Konsol memiliki tampilan baru yang dirancang untuk membuatny a lebih mudah digunakan . Panduan AWS CloudTrai l Pengguna telah diperbarui dengan perubahan prosedur untuk cara melakukan tugas di konsol, seperti membuat jejak, memperbarui jejak, dan mengunduh riwayat acara.	13 Agustus 2020

Menambahkan dukungan layanan	Rilis ini mendukung Amazon Interactive Video Service. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	15 Juli 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Honeycode. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	24 Juni 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Macie. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	19 Mei 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Kendra. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	13 Mei 2020
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT SiteWise. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	29 April 2020
Ditambahkan dukungan Wilayah	Rilis ini mendukung Wilayah tambahan: Eropa (Milan). Lihat Wilayah AWS CloudTrail yang Didukung.	28 April 2020

Menambahkan layanan dan dukungan Wilayah	Rilis ini mendukung Amazon AppFlow. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung. Support juga telah ditambahkan untuk Wilayah Afrika (Cape Town). Lihat Wilayah AWS CloudTrail yang Didukung.	22 April 2020
Ditambahkan fungsionalitas	High-volume AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` sekarang dicatat sebagai peristiwa Baca. Jika Anda memilih untuk mencatat semua AWS KMS peristiwa di jejak Anda, dan juga memilih untuk mencatat peristiwa manajemen Tulis, jejak Anda mencatat AWS KMS tindakan yang relevan seperti`Disable`, `Delete` dan`ScheduleKey` .	7 April 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon CodeGuru Reviewer. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	7 Februari 2020
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Managed Apache Cassandra Service. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	17 Januari 2020

Menambahkan dukungan layanan	Rilis ini mendukung Pelanggan Amazon Connect. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	13 Desember 2019
Dokumentasi diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: Perbarui referensi file.jar di panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.2.0.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	21 November 2019
Ditambahkan fungsionalitas	Rilis ini mendukung AWS CloudTrail Insights untuk membantu Anda mendeteksi aktivitas yang tidak biasa di akun Anda. Lihat peristiwa Logging Insights untuk Trails.	20 November 2019
Ditambahkan fungsionalitas	Rilis ini menambahkan opsi untuk memfilter AWS Key Management Service acara di luar jejak. Lihat Membuat Jejak.	20 November 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS CodeStar Pemberitahuan. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	7 November 2019

Ditambahkan fungsionalitas	Rilis ini mendukung penambahan tag saat Anda membuat jejak CloudTrail, baik Anda menggunakan CloudTrai l konsol atau API. Rilis ini menambahkan dua API baru, `GetTrail` dan`ListTrails` .	1 November 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS App Mesh. Lihat Layanan dan Integrasi yang AWS CloudTrai l Didukung.	17 Oktober 2019
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Translate. Lihat Layanan dan Integrasi yang AWS CloudTrai l Didukung.	17 Oktober 2019
Pembaruan dokumentasi	Topik Layanan Tidak Didukung telah dipulihkan dan diperbarui untuk menyertakan hanya AWS layanan yang saat ini tidak mencatat peristiwa . CloudTrail Lihat Layanan CloudTrail Tidak Didukung.	7 Oktober 2019

Pembaruan dokumentasi	Dokumentasi telah diperbarui dengan perubahan `AWSCloudTrailFullAccess` kebijakan. Contoh kebijakan yang menunjukkan izin yang setara `AWSCloudTrailFullAccess` telah diperbarui untuk membatasi sumber daya tempat `iam:PassRole` tindakan dapat bertindak terhadap yang cocok dengan pernyataan kondisi berikut:. `"iam:PassedToService": "cloudtrail.amazonaws.com"` Lihat Contoh AWS CloudTrail Identity-Based Kebijakan.	24 September 2019
Pembaruan dokumentasi	Dokumentasi telah diperbarui dengan topik baru, Mengelola CloudTrail Biaya, untuk membantu Anda mendapatkan data log yang Anda butuhkan CloudTrail saat tetap dalam anggaran.	3 September 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Control Tower. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	13 Agustus 2019
Ditambahkan dukungan Wilayah	Rilis ini mendukung Wilayah tambahan: Timur Tengah (Bahrain). Lihat Wilayah AWS CloudTrail yang Didukung.	29 Juli 2019

Pembaruan dokumentasi	Dokumentasi telah diperbaru i dengan informasi tentang keamanan untuk CloudTrai l. Lihat Keamanan di AWS CloudTrail.	3 Juli 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Ground Station. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	6 Juni 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT Things Graph. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	4 Juni 2019
Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkSpaces Applications. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukun g.	25 April 2019
Ditambahkan dukungan Wilayah	Rilis ini mendukung Wilayah tambahan: Asia Pasifik (Hong Kong). Lihat Wilayah AWS CloudTrail yang Didukung.	24 April 2019
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Managed Service untuk Apache Flink. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	22 Maret 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Backup. Lihat Layanan dan Integrasi yang AWS CloudTrai l Didukung.	4 Februari 2019

Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkLink. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	23 Januari 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Cloud9. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	21 Januari 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Elemental MediaLive. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	Januari 19, 2019
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Comprehend. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	18 Januari 2019
Menambahkan dukungan layanan	Rilis ini mendukung AWS Elemental MediaPackage. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	21 Desember 2018
Ditambahkan dukungan Wilayah	Rilis ini mendukung Wilayah tambahan: UE (Stockholm). Lihat Wilayah AWS CloudTrail yang Didukung.	11 Desember 2018
Pembaruan dokumentasi	Dokumentasi telah diperbarui dengan informasi tentang layanan yang didukung dan tidak didukung. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	Selasa, 03 Desember 2018

Menambahkan dukungan layanan	Rilis ini mendukung AWS Resource Access Manager (AWS RAM). Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	20 November 2018
Fungsionalitas diperbarui	Rilis ini mendukung pembuatan jejak di CloudTrai l log peristiwa untuk semua AWS akun di organisasi AWS Organizations. Lihat Membuat Jejak untuk Organisasi.	19 November 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Pinpoint SMS dan Voice API. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukun g.	16 Novbucket 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT Greengrass. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	29 Oktober 2018
Dokumentasi diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: Perbarui referensi file.jar di panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.1.3.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan pada GitHub.	18 Oktober 2018

Ditambahkan fungsionalitas	Rilis ini mendukung penggunaan filter tambahan dalam riwayat Acara. Lihat Melihat CloudTrail Acara di CloudTrail Konsol.	18 Oktober 2018
Ditambahkan fungsionalitas	Rilis ini mendukung penggunaan Amazon Virtual Private Cloud (Amazon VPC) untuk membuat koneksi pribadi antara VPC dan VPC Anda. AWS CloudTrail Lihat Menggunakan AWS CloudTrail dengan Titik Akhir VPC Antarmuka.	9 Agustus 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Data Lifecycle Manager. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	24 Juli 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon MQ. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	19 Juli 2018
Menambahkan dukungan layanan	Rilis ini mendukung CLI AWS Seluler. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	29 Juni 2018
AWS CloudTrail pemberitahuan riwayat dokumentasi tersedia melalui umpan RSS	Anda sekarang dapat menerima pemberitahuan tentang pembaruan AWS CloudTrail dokumentasi dengan berlangganan umpan RSS.	29 Juni 2018

Pembaruan lebih awal

Tabel berikut menjelaskan riwayat rilis dokumentasi AWS CloudTrail sebelum 29 Juni 2018.

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Amazon RDS Performance Insights. Untuk informasi selengkapnya, lihat Layanan dan Integrasi yang CloudTrail Didukung.	21 Juni 2018
Menambahkan fungsionalitas	Rilis ini mendukung pencatatan semua peristiwa CloudTrail manajemen dalam riwayat Acara. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.	14 Juni 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Manajemen Penagihan dan Biaya. Lihat CloudTrail layanan dan integrasi yang didukung.	7 Juni 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic Container Service for Kubernetes (Amazon EKS). Lihat CloudTrail layanan dan integrasi yang didukung.	5 Juni 2018
Dokumentasi yang diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: • Perbarui referensi file.jar dalam panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.1.2.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan di GitHub.	16 Mei 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Manajemen Penagihan dan Biaya. Lihat CloudTrail layanan dan integrasi yang didukung.	7 Juni 2018

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic Container Service for Kubernetes (Amazon EKS). Lihat CloudTrail layanan dan integrasi yang didukung.	5 Juni 2018
Dokumentasi yang diperbarui	Pembaruan ini mendukung rilis patch berikut untuk Pustaka CloudTrail Pemrosesan: • Perbarui referensi file.jar dalam panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library-1.1.2.jar. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan di GitHub.	16 Mei 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS X-Ray. Lihat CloudTrail layanan dan integrasi yang didukung.	25 April 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT Analytics. Lihat CloudTrail layanan dan integrasi yang didukung.	23 April 2018
Menambahkan dukungan layanan	Rilis ini mendukung Secrets Manager. Lihat CloudTrail layanan dan integrasi yang didukung.	10 April 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Rekognition. Lihat CloudTrail layanan dan integrasi yang didukung.	6 April 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Private Certificate Authority (PCA). Lihat CloudTrail layanan dan integrasi yang didukung.	4 April 2018

Ubah	Deskripsi	Tanggal Rilis
Menambahkan fungsionalitas	Rilis ini mendukung membuatnya lebih mudah untuk mencari file CloudTrail log dengan Amazon Athena. Anda dapat secara otomatis membuat tabel untuk menanyakan log langsung dari CloudTrail konsol, dan menggunakan tabel tersebut untuk menjalankan kueri di Athena. Untuk informasi selengkapnya, lihat CloudTrail layanan dan integrasi yang didukung dan Membuat Tabel untuk CloudTrail Log di CloudTrail Konsol.	15 Maret 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS AppSync. Lihat CloudTrail layanan dan integrasi yang didukung.	13 Februari 2018
Dukungan Wilayah ditambahkan	Rilis ini mendukung Wilayah tambahan: Asia Pasifik (Osaka) (ap-northeast-3). Lihat CloudTrail Daerah yang didukung.	12 Februari 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Shield. Lihat CloudTrail layanan dan integrasi yang didukung.	12 Februari 2018
Menambahkan dukungan layanan	Rilis ini mendukung Amazon SageMaker AI. Lihat CloudTrail layanan dan integrasi yang didukung.	11 Januari 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Batch. Lihat CloudTrail layanan dan integrasi yang didukung.	10 Januari 2018
Menambahkan fungsionalitas	Rilis ini mendukung perpanjangan jumlah aktivitas akun yang tersedia dalam riwayat CloudTrail acara hingga 90 hari. Anda juga dapat menyesuaikan tampilan kolom untuk meningkatkan tampilan CloudTrail acara Anda. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.	12 Desember 2017

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkMail. Lihat CloudTrail layanan dan integrasi yang didukung.	12 Desember 2017
Menambahkan dukungan layanan	Rilis ini mendukung Alexa for Business AWS Elemental MediaConvert,, AWS Elemental MediaStore dan. Lihat CloudTrail layanan dan integrasi yang didukung.	1 Desember 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pencatatan peristiwa data untuk AWS Lambda fungsi. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data.	30 November 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pencatatan peristiwa data untuk AWS Lambda fungsi. Untuk informasi selengkapnya, lihat Mencatat log peristiwa data.	30 November 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pembaruan berikut ke Pustaka CloudTrail Pemrosesan: • Tambahkan dukungan untuk identifikasi Boolean dari peristiwa manajemen. • Perbarui versi CloudTrail acara ke 1.06. Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan di GitHub.	30 November 2017
Menambahkan dukungan layanan	Rilis ini mendukung AWS Glue. Lihat CloudTrail layanan dan integrasi yang didukung.	7 November 2017

Ubah	Deskripsi	Tanggal Rilis
Dokumentasi baru	Rilis ini menambahkan topik baru,Kuota di AWS CloudTrail.	19 Oktober 2017
Dokumentasi yang diperbarui	Rilis ini memperbarui dokumentasi API yang didukung dalam riwayat CloudTrail peristiwa untuk Amazon Athena, AWS CodeBuild Amazon Elastic Container Registry, dan. AWS Migration Hub	Oktober 13, 2017
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Chime. Lihat CloudTrail layanan dan integrasi yang didukung.	27 September 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung konfigurasi pencatatan peristiwa data untuk semua bucket Amazon S3 di akun Anda. AWS Lihat Mencatat log peristiwa data.	20 September 2017
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Lex. Lihat CloudTrail layanan dan integrasi yang didukung.	Agustus 15, 2017
Menambahkan dukungan layanan	Rilis ini mendukung AWS Migration Hub. Lihat CloudTrail layanan dan integrasi yang didukung.	14 Agustus 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung CloudTrail diaktifkan secara default untuk semua AWS akun. Tujuh hari terakhir aktivitas akun tersedia dalam riwayat CloudTrail acara, dan peristiwa terbaru muncul di dasbor konsol. Fitur yang sebelumnya dikenal sebagai riwayat aktivitas API telah digantikan oleh riwayat Peristiwa.	14 Agustus 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pengunduhan peristiwa dari CloudTrail konsol di halaman riwayat aktivitas API. Anda dapat mengunduh acara dalam format JSON atau CSV. Untuk informasi selengkapnya, lihat Mengunduh acara.	27 Juli 2017

Ubah	Deskripsi	Tanggal Rilis
Menambahkan fungsionalitas	Rilis ini mendukung pencatatan operasi API tingkat objek Amazon S3 di dua Wilayah tambahan, Eropa (London) dan Kanada (Tengah). Untuk informasi selengkapnya, lihat Bekerja dengan file CloudTrail log.	19 Juli 2017
Menambahkan dukungan layanan	Rilis ini mendukung pencarian API untuk Amazon CloudWatch Events di fitur riwayat aktivitas CloudTrail API.	27 Juni 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung API tambahan dalam fitur riwayat aktivitas CloudTrail API untuk layanan berikut: • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	27 Juni 2017
Menambahkan dukungan layanan	Rilis ini mendukung AWS CodeStar. Lihat CloudTrail layanan dan integrasi yang didukung.	14 Juni 2017

Ubah	Deskripsi	Tanggal Rilis

Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pembaruan berikut ke Pustaka CloudTrail Pemrosesan:
	• Tambahkan dukungan untuk format yang berbeda untuk pesan SQS dari antrian SQS yang sama untuk mengidentifikasi CloudTrail file log. Format berikut ini didukung:
	  • Pemberitahuan yang CloudTrail mengirim ke topik SNS
	  • Pemberitahuan yang dikirimkan Amazon S3 ke topik SNS
	  • Pemberitahuan yang dikirimkan Amazon S3 langsung ke antrian SQS
	• Tambahkan dukungan untuk `deleteMessageUponFailure` properti, yang dapat Anda gunakan untuk menghapus pesan yang tidak dapat diproses.
	
	Untuk informasi selengkapnya, lihat Menggunakan Pustaka CloudTrail Pemrosesan dan Pustaka CloudTrail Pemrosesan di GitHub.
		1 Juni 2017

Menambahkan dukungan layanan	Rilis ini mendukung Amazon Athena. Lihat CloudTrail layanan dan integrasi yang didukung.	19 Mei 2017

Ubah	Deskripsi	Tanggal Rilis
Menambahkan fungsionalitas	Rilis ini mendukung pengiriman peristiwa data ke Amazon CloudWatch Logs. Untuk informasi selengkapnya tentang mengonfigurasi jejak Anda untuk mencatat peristiwa data, lihatPeristiwa data. Untuk informasi selengkapnya tentang mengirim peristiwa ke CloudWatch Log, lihatMemantau File CloudTrail Log dengan CloudWatch Log Amazon.	9 Mei 2017
Menambahkan dukungan layanan	Rilis ini mendukung Layanan AWS Marketplace Pengukuran. Lihat CloudTrail layanan dan integrasi yang didukung.	2 Mei 2017
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Quick. Lihat CloudTrail layanan dan integrasi yang didukung.	28 April 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pengalaman konsol yang diperbarui untuk membuat jalur baru. Anda sekarang dapat mengonfigurasi jejak baru untuk mencatat manajemen dan peristiwa data. Untuk informasi selengkapnya, lihat Membuat jejak dengan CloudTrail konsol.	11 April 2017

Ubah	Deskripsi	Tanggal Rilis
Dokumentasi ditambahkan	Jika CloudTrail tidak mengirimkan log ke bucket S3 Anda atau mengirim pemberitahuan SNS dari beberapa Wilayah di akun Anda, Anda mungkin perlu memperbarui kebijakan. Untuk mempelajari lebih lanjut tentang memperbarui kebijakan bucket S3 Anda, lihatKesalahan konfigurasi kebijakan Amazon S3 yang umum. Untuk mempelajari lebih lanjut tentang memperbarui kebijakan topik SNS Anda, lihatCloudTrail tidak mengirim notifikasi untuk Wilayah.	31 Maret 2017
Menambahkan dukungan layanan	Rilis ini mendukung AWS Organizations. Lihat CloudTrail layanan dan integrasi yang didukung.	27 Februari 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pengalaman konsol yang diperbarui untuk mengonfigurasi jejak untuk manajemen logging dan peristiwa data. Untuk informasi selengkapnya, lihat Bekerja dengan file CloudTrail log.	10 Februari 2017
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Cloud Directory. Lihat CloudTrail layanan dan integrasi yang didukung.	26 Januari 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pencarian API untuk AWS CodeCommit, Amazon GameLift Servers, dan AWS Managed Services dalam riwayat aktivitas CloudTrail API.	26 Januari 2017

Ubah	Deskripsi	Tanggal Rilis
Menambahkan fungsionalitas	Rilis ini mendukung integrasi dengan file Dasbor AWS Health. Anda dapat menggunakan file Dasbor Health untuk mengidentifikasi apakah jejak Anda tidak dapat mengirimkan log ke topik SNS atau bucket S3. Ini dapat terjadi ketika ada masalah dengan kebijakan untuk bucket S3 atau topik SNS. Dasbor Health memberi tahu Anda tentang jalur yang terkena dampak dan merekomendasikan cara untuk memperbaiki kebijakan. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Health.	24 Januari 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pemfilteran berdasarkan sumber acara di CloudTrail konsol. Sumber acara menunjukkan AWS layanan tempat permintaan dibuat. Untuk informasi selengkapnya, lihat Melihat acara manajemen terbaru dengan konsol.	Januari 12, 2017
Menambahkan dukungan layanan	Rilis ini mendukung AWS CodeCommit. Lihat CloudTrail layanan dan integrasi yang didukung.	11 Januari 2017
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Lightsail. Lihat CloudTrail layanan dan integrasi yang didukung.	Desember 23, 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Managed Services. Lihat CloudTrail layanan dan integrasi yang didukung.	Desember 21, 2016
Dukungan Wilayah ditambahkan	Rilis ini mendukung Wilayah Eropa (London). Lihat CloudTrail Daerah yang didukung.	13 Desember 2016

Ubah	Deskripsi	Tanggal Rilis
Dukungan Wilayah ditambahkan	Rilis ini mendukung Wilayah Kanada (Tengah). Lihat CloudTrail Daerah yang didukung.	8 Desember 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS CodeBuild LihatCloudTrail layanan dan integrasi yang didukung. Rilis ini mendukung AWS Health. Lihat CloudTrail layanan dan integrasi yang didukung. Rilis ini mendukung AWS Step Functions. Lihat CloudTrail layanan dan integrasi yang didukung.	1 Desember 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Polly. Lihat CloudTrail layanan dan integrasi yang didukung.	30 November 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS OpsWorks for Chef Automate. Lihat CloudTrail layanan dan integrasi yang didukung.	November 23, 2016
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung konfigurasi jejak Anda untuk mencatat read-only, write-only, atau semua peristiwa. CloudTrail mendukung pencatatan operasi API tingkat objek Amazon S3 seperti`GetObject` ,`PutObject` , dan. `DeleteObject` Anda dapat mengonfigurasi jejak Anda untuk mencatat operasi API tingkat objek. Untuk informasi selengkapnya, lihat Bekerja dengan file CloudTrail log.	21 November 2016
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung nilai tambahan untuk `type` bidang dalam `userIdentity` elemen: `AWSAccount` dan`AWSService` . Untuk informasi lebih lanjut, lihat Bidang untuk`userIdentity` .	16 Nopember 2016

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Application Auto Scaling. Lihat CloudTrail layanan dan integrasi yang didukung.	31 Oktober 2016
Dukungan Wilayah ditambahkan	Rilis ini mendukung Wilayah Timur AS (Ohio). Lihat CloudTrail Daerah yang didukung.	17 Oktober 2016
Menambahkan fungsiona litas dan dokumentasi	Rilis ini mendukung pencatatan peristiwa AWS layanan non-API. Untuk informasi selengkapnya, lihat Layanan AWS acara.	September 23, 2016
Menambahkan fungsiona litas dan dokumentasi	Rilis ini mendukung penggunaan CloudTrail konsol untuk melihat jenis sumber daya yang didukung oleh AWS Config. Untuk informasi selengkapnya, lihat Melihat sumber daya yang direferensikan dengan AWS Config.	7 Juli 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Service Catalog. Lihat CloudTrail layanan dan integrasi yang didukung.	6 Juli 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic File System (Amazon EFS). Lihat CloudTrail layanan dan integrasi yang didukung.	28 Juni 2016
Dukungan Wilayah ditambahkan	Rilis ini mendukung satu Wilayah tambahan: ap-south-1 (Asia Pasifik (Mumbai)). Lihat CloudTrail Daerah yang didukung.	27 Juni 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Application Discovery Service. Lihat CloudTrail layanan dan integrasi yang didukung.	12 Mei 2016
Menambahkan dukungan layanan	Rilis ini mendukung CloudWatch Log di Wilayah Amerika Selatan (São Paulo). Untuk informasi selengkapnya, lihat Memantau File CloudTrail Log dengan CloudWatch Log Amazon.	6 Mei 2016

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung AWS WAF. Lihat CloudTrail layanan dan integrasi yang didukung.	April 28, 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Dukungan. Lihat CloudTrail layanan dan integrasi yang didukung.	21 April 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Inspector. Lihat CloudTrail layanan dan integrasi yang didukung.	April 20, 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS IoT. Lihat CloudTrail layanan dan integrasi yang didukung.	11 April 2016
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung logging AWS Security Token Service (AWS STS) panggilan API yang dilakukan dengan Security Assertion Markup Language (SAMP) dan federasi identitas web. Untuk informasi selengkapnya, lihat Nilai untuk AWS STS API dengan SAFL dan federasi identitas web.	Maret 28, 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Certificate Manager. Lihat CloudTrail layanan dan integrasi yang didukung.	25 Maret 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Data Firehose. Lihat CloudTrail layanan dan integrasi yang didukung.	Maret 17, 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon CloudWatch Logs. Lihat CloudTrail layanan dan integrasi yang didukung.	10 Maret 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Cognito. Lihat CloudTrail layanan dan integrasi yang didukung.	18 Februari 2016
Menambahkan dukungan layanan	Rilis ini mendukung AWS Database Migration Service. Lihat CloudTrail layanan dan integrasi yang didukung.	Februari 4, 2016

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung GameLift Server Amazon (GameLift Server Amazon). Lihat CloudTrail layanan dan integrasi yang didukung.	27 Januari 2016
Menambahkan dukungan layanan	Rilis ini mendukung CloudWatch Acara Amazon. Lihat CloudTrail layanan dan integrasi yang didukung.	Januari 16, 2016
Dukungan Wilayah ditambahkan	Rilis ini mendukung satu Wilayah tambahan: ap-northeast-2 (Asia Pasifik (Seoul)). Lihat CloudTrail Daerah yang didukung.	6 Januari 2016
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic Container Registry (Amazon ECR). Lihat CloudTrail layanan dan integrasi yang didukung.	21 Desember 2015
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung CloudTrail pengaktifan di semua Wilayah dan dukungan untuk beberapa jalur per Wilayah. Untuk informasi selengkapnya, lihat Bekerja dengan jalan CloudTrail setapak.	17 Desember 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Machine Learning. Lihat CloudTrail layanan dan integrasi yang didukung.	Desember 10, 2015
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung enkripsi file log, validasi integritas file log, dan penandaan. Lihat informasi selengkapnya di Mengenkripsi file CloudTrail log, mencerna file, dan penyimpanan data peristiwa dengan AWS KMS kunci (SSE-KMS), Memvalidasi CloudTrail integritas file log, dan Memperbarui jejak dengan CloudTrail konsol.	1 Oktober 2015
Menambahkan dukungan layanan	Rilis ini mendukung OpenSearch Layanan Amazon. Lihat CloudTrail layanan dan integrasi yang didukung.	1 Oktober 2015
Menambahkan dukungan layanan	Rilis ini mendukung peristiwa tingkat bucket Amazon S3. Lihat CloudTrail layanan dan integrasi yang didukung.	1 September 2015

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung AWS Device Farm. Lihat CloudTrail layanan dan integrasi yang didukung.	Juli 13, 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon API Gateway. Lihat CloudTrail layanan dan integrasi yang didukung.	9 Juli 2015
Menambahkan dukungan layanan	Rilis ini mendukung CodePipeline. Lihat CloudTrail layanan dan integrasi yang didukung.	9 Juli 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon DynamoDB. Lihat CloudTrail layanan dan integrasi yang didukung.	28 Mei 2015
Menambahkan dukungan layanan	Rilis ini mendukung CloudWatch Log di Wilayah AS Barat (California Utara). Untuk informasi selengkap nya tentang CloudTrail dukungan untuk pemantauan CloudWatch Log, lihatMemantau File CloudTrail Log dengan CloudWatch Log Amazon.	19 Mei 2015
Menambahkan dukungan layanan	Rilis ini mendukung Directory Service. Lihat CloudTrail layanan dan integrasi yang didukung.	14 Mei 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Simple Email Service (Amazon SES). Lihat CloudTrail layanan dan integrasi yang didukung.	7 Mei 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic Container Service LihatCloudTrail layanan dan integrasi yang didukung.	9 April 2015
Menambahkan dukungan layanan	Rilis ini mendukung AWS Lambda. Lihat CloudTrail layanan dan integrasi yang didukung.	9 April 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkSpaces. Lihat CloudTrail layanan dan integrasi yang didukung.	9 April 2015

Ubah	Deskripsi	Tanggal Rilis
	Rilis ini mendukung pencarian AWS aktivitas yang ditangkap oleh CloudTrail (CloudTrail peristiwa). Anda dapat mencari dan memfilter acara di akun Anda yang terkait dengan pembuatan, modifikasi, atau penghapusan. Untuk mencari peristiwa ini, Anda dapat menggunakan CloudTrail konsol, AWS Command Line Interface (AWS CLI), atau AWS SDK. Untuk informasi selengkapnya, lihat Bekerja dengan riwayat CloudTrail acara.	12 Maret 2015
Ditambahkan dukungan layanan dan dokumentasi baru	Rilis ini mendukung Amazon CloudWatch Logs di Asia Pasifik (Singapura), Asia Pasifik (Sydney), Asia Pasifik (Tokyo), dan Wilayah Eropa (Frankfurt). Untuk informasi selengkapnya, lihat Mengirim peristiwa ke CloudWatch Log.	Maret 5, 2015
Dokumentasi baru	Bagian baru yang menjelaskan CloudTrail dukungan untuk AWS Security Token Service (AWS STS) titik akhir regional telah ditambahkan ke halaman CloudTrail Konsep.	Februari 17, 2015
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Route 53. Lihat CloudTrail layanan dan integrasi yang didukung.	11 Februari 2015
Menambahkan dukungan layanan	Rilis ini mendukung AWS Config. Lihat CloudTrail layanan dan integrasi yang didukung.	10 Februari 2015
Menambahkan dukungan layanan	Rilis ini mendukung AWS CloudHSM. Lihat CloudTrail layanan dan integrasi yang didukung.	8 Januari 2015
Menambahkan dukungan layanan	Rilis ini mendukung AWS CodeDeploy. Lihat CloudTrail layanan dan integrasi yang didukung.	17 Desember 2014

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung AWS Storage Gateway. Lihat CloudTrail layanan dan integrasi yang didukung.	Desember 16, 2014
Dukungan Wilayah ditambahkan	Rilis ini mendukung satu Wilayah tambahan: us-gov-west-1 ((()).AWS GovCloud US-West Lihat CloudTrail Daerah yang didukung.	Desember 16, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Glacier. Lihat CloudTrail layanan dan integrasi yang didukung.	11 Desember 2014
Menambahkan dukungan layanan	Rilis ini mendukung AWS Data Pipeline. Lihat CloudTrail layanan dan integrasi yang didukung.	Desember 2, 2014
Menambahkan dukungan layanan	Rilis ini mendukung AWS Key Management Service. Lihat CloudTrail layanan dan integrasi yang didukung.	12 November 2014
Dokumentasi baru	Bagian baru,Memantau File CloudTrail Log dengan CloudWatch Log Amazon, telah ditambahkan ke panduan. Ini menjelaskan cara menggunakan Amazon CloudWatch Logs untuk memantau peristiwa CloudTrail log.	10 November 2014
Dokumentasi baru	Bagian baru,Menggunakan Pustaka CloudTrail Pemrosesan, telah ditambahkan ke panduan. Ini memberikan informasi tentang cara menulis prosesor CloudTrail log di Java menggunakan Perpustakaan AWS CloudTrail Pemrosesan.	5 November 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Elastic Transcoder. Lihat CloudTrail layanan dan integrasi yang didukung.	Oktober 27, 2014
Dukungan Wilayah ditambahkan	Rilis ini mendukung satu wilayah tambahan: eu-central-1 (Eropa (Frankfurt)). Lihat CloudTrail Daerah yang didukung.	23 Oktober 2014

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Amazon CloudSearch. Lihat CloudTrail layanan dan integrasi yang didukung.	16 Oktober 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Simple Notification Service. Lihat CloudTrail layanan dan integrasi yang didukung.	Oktober 09, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon ElastiCache. Lihat CloudTrail layanan dan integrasi yang didukung.	15 September 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon WorkDocs. Lihat CloudTrail layanan dan integrasi yang didukung.	Agustus 27, 2014
Penambahan konten baru	Rilis ini mencakup topik yang membahas peristiwa login logging. Lihat Konsol Manajemen AWS acara masuk.	Juli 24, 2014
Penambahan konten baru	Elemen EventVersion untuk rilis ini telah ditingkatkan ke versi 1.02 dan tiga bidang baru telah ditambahk an. Lihat CloudTrail merekam konten untuk acara manajemen, data, dan aktivitas jaringan.	Juli 18, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Auto Scaling (lihatCloudTrail layanan dan integrasi yang didukung).	Juli 17, 2014
Dukungan Wilayah ditambahkan	Rilis ini mendukung tiga Wilayah tambahan: ap-southe ast-1 (Asia Pasifik (Singapura)), ap-northeast-1 (Asia Pasifik (Tokyo)), sa-east-1 (Amerika Selatan (São Paulo)). Lihat CloudTrail Daerah yang didukung.	30 Juni 2014
Dukungan layanan tambahan	Rilis ini mendukung Amazon Redshift. Lihat CloudTrail layanan dan integrasi yang didukung.	Juni 10, 2014
Menambahkan dukungan layanan	Rilis ini mendukung OpsWorks. Lihat CloudTrail layanan dan integrasi yang didukung.	Juni 5, 2014

Ubah	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung Amazon CloudFront. Lihat CloudTrail layanan dan integrasi yang didukung.	28 Mei 2014
Dukungan Wilayah ditambahkan	Rilis ini mendukung tiga Wilayah tambahan: us-west-1 (AS Barat (California N.)), eu-west-1 (Eropa (Irlandia)), ap-southeast-2 (Asia Pasifik (Sydney)). Lihat CloudTrail Daerah yang didukung.	13 Mei 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Simple Workflow Service. Lihat CloudTrail layanan dan integrasi yang didukung.	9 Mei 2014
Penambahan konten baru	Rilis ini mencakup topik yang membahas berbagi file log antar akun. Lihat Berbagi file CloudTrail log antar AWS akun.	Mei 2, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon CloudWatch. Lihat CloudTrail layanan dan integrasi yang didukung.	28 April 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Kinesis. Lihat CloudTrail layanan dan integrasi yang didukung.	April 22, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Direct Connect. Lihat CloudTrail layanan dan integrasi yang didukung.	April 11, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon EMR. Lihat CloudTrail layanan dan integrasi yang didukung.	April 4, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Elastic Beanstalk. Lihat CloudTrail layanan dan integrasi yang didukung.	2 April 2014
Dukungan layanan tambahan	Rilis ini mendukung CloudFormation. Lihat CloudTrail layanan dan integrasi yang didukung.	Maret 7, 2014
Panduan baru	Rilis ini memperkenalkan AWS CloudTrail.	November 13, 2013

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