Panduan Pengguna

AWS CloudTrail

Versi 1.0

AWS CloudTrail: Panduan Pengguna

Table of Contents

Apa Itu AWS CloudTrail?

AWS CloudTrailadalah AWS layanan yang membantu Anda mengaktifkan audit operasional dan risiko, tata kelola, dan kepatuhan akun AndaAWS. Tindakan yang diambil oleh pengguna, peran, atau AWS layanan dicatat sebagai peristiwa di CloudTrail. Peristiwa mencakup tindakan yang diambil dalamAWS Management Console,AWS Command Line Interface, dan AWS SDK dan API.

CloudTrail aktif di Anda Akun AWS saat Anda membuatnya dan tidak memerlukan pengaturan manual apa pun. Ketika aktivitas terjadi di AndaAkun AWS, aktivitas itu dicatat dalam suatu CloudTrail peristiwa.

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 CloudTrailDanau adalah danau data terkelola untuk menangkap, menyimpan, mengakses, dan menganalisis aktivitas pengguna dan API AWS untuk tujuan audit dan keamanan. 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 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun. Anda dapat membuat penyimpanan data acara untuk satu Akun AWS atau beberapa Akun AWS dengan menggunakanAWS 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, silakan lihat Bekerja dengan AWS CloudTrail Danau dan Buat toko data acara.

  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 CloudTrailHarga danMengelola biaya CloudTrail Danau.

- Trails — Trails menangkap catatan AWS aktivitas, mengirimkan dan menyimpan peristiwa ini dalam bucket Amazon S3, dengan pengiriman opsional ke Amazon 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 menggunakanAWS Organizations. Anda dapat mencatat peristiwa Insights untuk menganalisis peristiwa manajemen Anda untuk perilaku anomali dalam volume 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 Amazon S3 Anda tanpa biaya CloudTrail dengan membuat jejak, namun, ada biaya penyimpanan Amazon S3. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrailHarga. 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.

Topik

- Bagaimana cara CloudTrail kerja
- CloudTrail alur kerja
- CloudTrail konsep

- CloudTrail Daerah yang didukung
- CloudTrail contoh file log
- CloudTrail layanan dan integrasi yang didukung
- Kuota di AWS CloudTrail

Bagaimana cara CloudTrail kerja

CloudTrail aktif di AWS akun Anda saat Anda membuatnya. Ketika aktivitas terjadi di AWS akun Anda, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa. Anda dapat melihat 90 hari terakhir aktivitas API yang direkam (peristiwa manajemen) Wilayah AWS di CloudTrail konsol dengan membuka Riwayat peristiwa.

Untuk catatan acara yang sedang berlangsung di AndaAkun AWS, buat penyimpanan data acara atau jejak. Trails dapat mencatat peristiwa untuk peristiwa CloudTrail manajemen, data, dan Wawasan. Penyimpanan data peristiwa dapat mencatat CloudTrail manajemen dan peristiwa data, peristiwa CloudTrail Wawasan, item AWS Config konfigurasi, AWS Audit Managerbukti, dan AWS non-peristiwa dari integrasi.

Untuk memulai CloudTrail, lihatMemulai dengan AWS CloudTrail tutorial.

Untuk CloudTrail harga, lihat AWS CloudTrailHarga. Untuk harga Amazon S3 dan Amazon SNS, lihat Harga Amazon S3 dan Harga Amazon SNS.

Topik

- Riwayat acara
- CloudTrail Penyimpanan data danau dan acara
- CloudTrail jalan setapak
- CloudTrail saluran

Riwayat acara

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 Anda dapat dengan mudah melihat peristiwa 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.

CloudTrail Penyimpanan data danau dan acara

Anda dapat membuat penyimpanan data acara CloudTrail Lake untuk mengarsipkan, menganalisis, dan menanggapi perubahan AWS sumber daya 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 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun.

Anda dapat membuat penyimpanan data acara untuk mengumpulkan peristiwa CloudTrail manajemen dan data, peristiwa CloudTrail Wawasan, item AWS Config konfigurasi, AWS Audit Managerbukti, atau AWS non-peristiwa. Anda dapat membuat penyimpanan data acara menggunakan konsol, theAWS CLI, atau CloudTrail API. Untuk informasi selengkapnya tentang membuat penyimpanan data acara menggunakan konsol, lihatBuat toko data acara. Untuk informasi selengkapnya tentang membuat penyimpanan data acara menggunakanAWS CLI, lihatMengelola CloudTrail Danau dengan menggunakan AWS CLI.

CloudTrail Lake memungkinkan Anda mencatat peristiwa dari aplikasi di luarAWS, termasuk dari sumber apa pun di lingkungan hibrida Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau wadah dengan membuat integrasi. Anda dapat membuat integrasi dengan lebih dari 12 mitra untuk mencatat peristiwa yang terjadi di luar AWS penyimpanan data acara Anda. Untuk membuat integrasi, pertama-tama Anda mengonfigurasi saluran tempat acara dikirimkan. Anda dapat menggunakan CloudTrail Lake untuk menyimpan, mengakses, menganalisis, memecahkan masalah, dan mengambil tindakan pada data ini tanpa mempertahankan beberapa agregator log dan alat pelaporan.

Penyimpanan data acara dapat mencatat peristiwa dari saat iniWilayah 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.

Untuk mengubah penyimpanan data peristiwa setelah Anda membuatnya, Anda dapat menjalankan update-event-data-storeperintah, atau menggunakan konsol CloudTrail Lake.

Jika Anda telah membuat organisasiAWS 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. Secara default, akun anggota tidak memiliki akses ke file log untuk penyimpanan data acara organisasi, juga tidak dapat menjalankan kueri pada penyimpanan data acara organisasi. Penyimpanan data acara organisasi tidak dapat digunakan untuk mengumpulkan acara dari luarAWS. Untuk informasi selengkapnya, lihat Menyimpan data acara organisasi.

Untuk informasi lebih lanjut tentang cara memulai dengan CloudTrail Lake, lihat Bekerja dengan AWS CloudTrail Danau di panduan ini.

CloudTrail jalan setapak

Anda juga dapat membuat CloudTrail jejak untuk mengarsipkan, menganalisis, dan menanggapi perubahan AWS sumber daya Anda. Trails dapat mencatat peristiwa CloudTrail manajemen, peristiwa data, dan peristiwa Wawasan.

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. Anda dapat membuat jejak dengan CloudTrail konsol, theAWS CLI, atau CloudTrail API.

Anda dapat membuat dua jenis jejak untuk AWS akun:

Jejak yang berlaku untuk semua Wilayah

> Saat Anda membuat jejak yang berlaku untuk semua Wilayah, CloudTrail merekam peristiwa di setiap Wilayah dan mengirimkan file log CloudTrail peristiwa ke bucket S3 yang Anda tentukan. Jika Wilayah ditambahkan setelah Anda membuat jejak yang berlaku untuk semua Wilayah,

Wilayah baru tersebut secara otomatis disertakan, dan peristiwa di Wilayah tersebut dicatat. Membuat jejak Multi-wilayah adalah praktik terbaik yang disarankan karena Anda menangkap aktivitas di semua Wilayah di akun Anda. Semua jalur yang Anda buat menggunakan CloudTrail konsol adalah Multi-wilayah. Anda dapat memperbarui jejak wilayah Tunggal untuk mencatat semua Wilayah dengan menggunakan. AWS CLI Lihat informasi yang lebih lengkap di Membuat jejak di konsol dan Mengonversi jejak yang berlaku untuk satu Wilayah untuk diterapkan ke semua Wilayah.

Jejak yang berlaku untuk satu Wilayah

Saat Anda membuat jejak yang berlaku untuk satu Wilayah, 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 Amazon 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 Command Line Interface.

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

Mulai 12 April 2019, jalur hanya dapat dilihat di AWS Wilayah tempat mereka mencatat peristiwa. Jika Anda membuat jejak yang mencatat peristiwa di semua AWS Wilayah, itu akan muncul di konsol di semua AWS Wilayah. Jika Anda membuat jejak yang hanya mencatat peristiwa di satu AWS Wilayah, Anda dapat melihat dan mengelolanya hanya di AWS Wilayah tersebut.

Jika Anda telah membuat organisasiAWS 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.

Anda dapat mengubah konfigurasi jejak setelah Anda membuatnya, termasuk apakah itu mencatat peristiwa di satu Wilayah atau semua Wilayah. Untuk mengubah jejak wilayah Tunggal menjadi jejak All-region, atau sebaliknya, Anda harus menjalankan perintah. AWS CLI update-trail Anda juga dapat mengubah apakah itu mencatat data atau peristiwa CloudTrail Wawasan. Mengubah apakah jejak mencatat peristiwa di satu Wilayah atau di semua Wilayah memengaruhi peristiwa mana yang dicatat. Untuk informasi lebih lanjut, lihat Mengelola jalur dengan AWS CLI (AWS CLI), danBekerja dengan file CloudTrail log.

Secara default, file log CloudTrail peristiwa dari jejak dienkripsi menggunakan enkripsi sisi server Amazon S3 (SSE). Anda juga dapat memilih untuk mengenkripsi file log Anda 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.

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 attempted-to-deliver peristiwa 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, AWS CloudFormation `CreateStack` panggilan dapat menghasilkan panggilan API tambahan ke Amazon EC2, Amazon RDS, Amazon EBS, atau layanan lain seperti yang dipersyaratkan oleh template. AWS CloudFormation Perilaku ini normal dan diharapkan. Anda dapat mengidentifikasi apakah tindakan itu diambil oleh AWS layanan dengan `invokedby` bidang dalam CloudTrail acara tersebut.

CloudTrail saluran

CloudTrail mendukung dua jenis saluran:

Saluran untuk integrasi CloudTrail Danau dengan sumber acara di luar AWS

CloudTrail Lake menggunakan saluran untuk membawa AWS non-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 diatur untuk mencatat peristiwa aktivitas. 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.

Saluran terkait layanan

AWSlayanan dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWSLayanan yang membuat saluran terkait layanan mengonfigurasi pemilih peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semua Wilayah, atau satu Wilayah.

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

CloudTrail alur kerja

Bagian ini memberikan informasi tentang CloudTrail fitur dan tugas yang dapat Anda lakukan untuk fitur-fitur ini.

Riwayat acara

Lihat riwayat acara untuk AWS akun Anda

Anda dapat melihat dan mencari 90 hari terakhir peristiwa yang direkam oleh CloudTrail di CloudTrail konsol atau dengan menggunakanAWS CLI. Untuk informasi selengkapnya, lihat Bekerja dengan Riwayat CloudTrail Acara.

Unduh acara

Anda dapat mengunduh file CSV atau JSON yang berisi CloudTrail acara hingga 90 hari terakhir untuk akun AndaAWS. Untuk informasi selengkapnya, lihat Mengunduh acara.

CloudTrail Danau

Aktifkan CloudTrail Danau

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL berbutir halus pada peristiwa dari kedua AWS sumber, dan sumber di luar. AWS 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun. 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.

Buat toko data acara

Saat Anda membuat penyimpanan data acara di CloudTrail Lake, Anda memilih jenis acara yang akan disertakan dalam penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat Buat toko data acara.

Lihat dasbor Danau

Anda dapat menggunakan dasbor CloudTrail Danau untuk memvisualisasikan peristiwa di penyimpanan data acara. Anda dapat memilih dari beberapa jenis dasbor yang berbeda. Untuk informasi selengkapnya, lihat Lihat dasbor Danau.

Manajemen log dan peristiwa data

Konfigurasikan penyimpanan data acara Anda untuk mencatat read-only, write-only, atau semua peristiwa manajemen dan data. Secara default, data peristiwa menyimpan peristiwa manajemen log log. Untuk informasi selengkapnya, lihat Buat penyimpanan data acara untuk CloudTrail acara, Acara manajemen logging, dan Pencatatan peristiwa data.

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, silakan lihat Membuat penyimpanan data acara untuk acara CloudTrail Insights dan Acara Logging Insights.

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 Harga AWS CloudTrail.

Salin acara jejak ke CloudTrail Danau

Anda dapat menyalin peristiwa jejak yang ada ke penyimpanan data acara CloudTrail Lake untuk membuat point-in-time snapshot peristiwa yang dicatat ke jejak. Untuk informasi selengkapnya, lihat Salin peristiwa jejak ke penyimpanan data acara.

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. Untuk informasi selengkapnya, lihat Federasi toko data acara.

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. Untuk informasi selengkapnya tentang cara menghentikan konsumsi acara di CloudTrail konsol, lihat. Hentikan dan mulai konsumsi acara Untuk informasi selengkapnya tentang cara menghentikan konsumsi acara dengan menggunakanAWS CLI, lihat. Hentikan konsumsi pada penyimpanan data acara dengan AWS CLI

Buat integrasi dengan sumber acara di luar AWS

Anda dapat menggunakan integrasi CloudTrail Lake untuk mencatat dan menyimpan data aktivitas pengguna dari luarAWS; 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 membuat integrasi di CloudTrail konsol, lihatBuat integrasi dengan sumber acara di luar AWS. Untuk informasi tentang membuat integrasi dengan menggunakanAWS CLI, lihatBuat integrasi untuk mencatat peristiwa dari luar AWS dengan AWS CLI.

Lihat contoh kueri Lake di konsol CloudTrail

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri. Untuk informasi selengkapnya, lihat Melihat contoh kueri di konsol CloudTrail .

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. Untuk informasi selengkapnya, silakan lihat Membuat atau mengedit kueri dan CloudTrail Kendala Lake SQL.

Simpan hasil kueri CloudTrail Lake ke bucket Amazon S3

Saat menjalankan kueri, Anda dapat menyimpan hasil kueri ke bucket S3. Untuk informasi selengkapnya, lihat Jalankan kueri dan simpan hasil kueri.

Unduh hasil kueri yang disimpan

Anda dapat mengunduh file CSV yang berisi hasil kueri CloudTrail Lake yang disimpan. Untuk informasi selengkapnya, lihat Unduh Anda CloudTrail Lake menyimpan hasil kueri.

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 selengkapnya, lihat Memvalidasikan hasil kueri yang disimpan.

Mengelola izin pengguna

Gunakan AWS Identity and Access Management (IAM) untuk mengelola pengguna mana yang memiliki izin untuk membuat, mengonfigurasi, atau menghapus penyimpanan dan saluran data peristiwa; memulai dan menghentikan konsumsi acara; dan menyalin peristiwa jejak ke penyimpanan data acara. Untuk informasi selengkapnya, lihat Pemberian izin untuk administrasi CloudTrail .

Daftarkan administrator yang didelegasikan untuk mengelola sumber daya organisasi CloudTrail Anda

Anda dapat mendaftarkan administrator yang didelegasikan untuk mengelola penyimpanan data CloudTrail acara organisasi Anda. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan organisasi.

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. Untuk informasi selengkapnya, lihat halaman AWS CloudTrailmitra.

Jalan setapak

Buat jejak

Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3 Anda. Secara default, ketika Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah . Jejak mencatat peristiwa dari semua Wilayah di AWSpartisi dan mengirimkan file log ke bucket S3 yang Anda tentukan. Untuk informasi selengkapnya, lihat Membuat jejak untuk Anda Akun AWS.

Manajemen log dan peristiwa data

Konfigurasikan jejak Anda untuk mencatat read-only, write-only, atau semua peristiwa manajemen dan data. Secara default, melacak peristiwa manajemen log. Untuk informasi selengkapnya, silakan lihat Acara manajemen logging dan Pencatatan peristiwa data.

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. Untuk informasi selengkapnya, lihat Acara Logging Insights.

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 Harga AWS CloudTrail.

Lihat acara Wawasan

Setelah mengaktifkan CloudTrail Insights on a trail, Anda dapat melihat hingga 90 hari peristiwa Insights menggunakan CloudTrail konsol atau. AWS CLI Untuk informasi selengkapnya, lihat Melihat acara CloudTrail Wawasan untuk jalur.

Unduh acara Insights

Setelah mengaktifkan CloudTrail Insights on a trail, Anda dapat mengunduh file CSV atau JSON yang berisi hingga 90 hari terakhir acara Insights untuk jejak Anda. Untuk informasi selengkapnya, lihat Mengunduh acara Wawasan.

Salin acara jejak ke CloudTrail Danau

Anda dapat menyalin peristiwa jejak yang ada ke penyimpanan data acara CloudTrail Lake untuk membuat point-in-time snapshot peristiwa yang dicatat ke jejak. Untuk informasi selengkapnya, lihat Menyalin acara jejak ke Danau CloudTrail.

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. Untuk informasi, lihat Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail.

> **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 CloudTrail Perpustakaan Pengolahan

Lihat file log Anda

Gunakan Amazon S3 untuk mengambil file log. Untuk informasi, lihat Mendapatkan dan melihat file CloudTrail log Anda.

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. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

> **Note**
>
> Jika Anda mengonfigurasi jejak yang berlaku untuk semua Wilayah untuk mengirim peristiwa ke grup CloudWatch log Log, CloudTrail mengirimkan peristiwa dari semua Wilayah ke grup log tunggal.

Aktifkan enkripsi log

Enkripsi file log memberikan lapisan keamanan ekstra untuk file log Anda. Untuk informasi selengkapnya, lihat Mengenkripsi file CloudTrail log dengan AWS KMS kunci (SSE-KMS).

Aktifkan integritas file log

Validasi integritas file log membantu Anda memverifikasi bahwa file log tetap tidak berubah sejak CloudTrail dikirimkan. Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas berkas log.

Bagikan file log dengan AWS akun lain

Anda dapat berbagi file log antar akun. Untuk informasi selengkapnya, lihat Berbagi file CloudTrail log antar AWS akun.

Log agregat dari beberapa akun

Anda dapat menggabungkan file log dari beberapa akun ke satu bucket. Untuk informasi selengkapnya, lihat Menerima file CloudTrail log dari beberapa akun.

Mengelola izin pengguna

Gunakan AWS Identity and Access Management (IAM) untuk mengelola pengguna mana yang memiliki izin untuk membuat, mengonfigurasi, atau menghapus jejak; memulai dan menghentikan pencatatan; dan mengakses bucket yang memiliki file log. Untuk informasi selengkapnya, lihat Pemberian izin untuk administrasi CloudTrail .

Daftarkan administrator yang didelegasikan untuk mengelola sumber daya organisasi CloudTrail Anda

Anda dapat mendaftarkan administrator yang didelegasikan untuk mengelola CloudTrail jejak organisasi Anda. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan organisasi.

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. Untuk informasi selengkapnya, lihat halaman AWS CloudTrailmitra.

CloudTrail konsep

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

Daftar Isi

- Bagaimana CloudTrail kaitannya dengan layanan AWS pemantauan lainnya?
- Solusi mitra

Apa itu 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 AWS Management Console, AWS SDK, alat baris perintah, dan layanan lainnya AWS . Ada tiga jenis peristiwa yang dapat masuk CloudTrail: peristiwa manajemen, peristiwa data, dan peristiwa CloudTrail Wawasan. Secara default, jejak dan data peristiwa menyimpan peristiwa manajemen log, tetapi bukan data atau peristiwa Wawasan.

Semua jenis acara menggunakan format log CloudTrail JSON.

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

Apa itu acara 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 ditangkap oleh CloudTrail. Untuk daftar peristiwa manajemen yang CloudTrail mencatat AWS layanan, lihatCloudTrail layanan dan integrasi yang didukung.

Apa itu 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 seringkali merupakan aktivitas volume tinggi.

Contoh peristiwa data meliputi:

- Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject`, `DeleteObject`, dan operasi `PutObject` API) pada bucket dan objek dalam bucket.
- 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 peristiwa data yang tersedia untuk jejak dan penyimpanan data peristiwa. Kolom tipe peristiwa data (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 bucket Amazon S3 dan objek bucket, fungsi Lambda, dan tabel DynamoDB (ditampilkan dalam tiga baris pertama tabel). Anda hanya dapat menggunakan pemilih acara lanjutan untuk mencatat jenis peristiwa data yang ditampilkan di baris yang tersisa.

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

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon DynamoDB	Aktivitas API tingkat objek Amazon DynamoDB pada tabel (misalnya	DynamoDB	`AWS::DynamoDB::Table`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	PutItem,,DeleteItem , dan operasi API). UpdateItem **Note** Untuk tabel dengan aliran diaktifkan, resources bidang dalam peristiwa data berisi keduanya AWS::DynamoDB::Stream danAWS::DynamoDB::Table . Jika Anda menentukan AWS::DynamoDB::Table untukresources.type , itu akan mencatat kedua tabel DynamoDB dan DynamoDB		

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	stream peristiwa secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.		
AWS Lambda	AWS Lambda aktivitas eksekusi fungsi (`Invoke`API).	Lambda	`AWS::Lambda::Function`
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject` `DeleteObject` , dan operasi `PutObject` API) pada bucket dan objek dalam bucket.	S3	`AWS::S3::Object`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS AppConfig	AWS AppConfig Aktivitas API untuk operasi konfigurasi seperti panggilan ke `StartConfiguration Session` dan`GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Pertukaran Data B2B	Aktivitas B2B Data Interchange API untuk operasi Transformer seperti panggilan ke dan. `GetTransformerJob` `StartTransformerJob`	Pertukaran Data B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias agen.	Alias agen batuan dasar	`AWS::Bedrock::AgentAlias`
	Aktivitas Amazon Bedrock API pada basis pengetahuan.	Basis pengetahuan batuan dasar	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Aktivitas API pada a KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Aktivitas API pada namespace.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	AWS Cloud Map Aktivitas API pada layanan.	AWS Cloud Map layanan	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS.	CloudTrail	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API pada kustomisasi.	CodeWhisperer kustomisasi	`AWS::CodeWhisperer::Customization`
	Aktivitas Amazon CodeWhisperer API di profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Aktivitas API Amazon Cognito di kumpulan identitas Amazon Cognito.	Kolam Identitas Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Aktivitas Amazon DynamoDB API di stream.	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon Elastic Block Store	API langsung Amazon Elastic Block Store (EBS), seperti,`PutSnapshotBlock` , `GetSnapshotBlock` dan snapshot `ListChangedBlocks` Amazon EBS.	API langsung Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Aktivitas Amazon EMR API di ruang kerja log tulis di depan.	Ruang kerja log tulis ke depan EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Amazon FinSpaceAktivitas API di lingkungan.	FinSpace	`AWS::FinSpace::Environment`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS Glue	AWS Glue Aktivitas API pada tabel yang dibuat oleh Lake Formation. **Note** AWS Glue peristiwa data untuk tabel saat ini hanya didukung di wilayah berikut: • AS Timur (N. Virginia) • AS Timur (Ohio) • AS Barat (Oregon) • Eropa (Irlandia) • Wilayah Asia Pasifik (Tokyo)	Formasi Danau	`AWS::Glue::Table`
Amazon GuardDuty	Aktivitas Amazon GuardDuty API untuk detektor.	GuardDuty detektor	`AWS::GuardDuty::Detector`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS HealthImaging	AWS HealthImaging Aktivitas API pada penyimpanan data.	Toko data Pencitraan Medis	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Aktivitas API pada sertifikat.	Sertifikat IoT	`AWS::IoT::Certificate`
	AWS IoT Aktivitas API pada berbagai hal.	Hal IoT	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	Aktivitas API Greengrass dari perangkat inti Greengrass pada versi komponen. **Note** Greengrass tidak mencatat peristiwa yang ditolak akses.	Versi komponen Greengrass IoT	`AWS::GreengrassV2::ComponentVersion`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Greengrass aktivitas API dari perangkat inti Greengrass pada penerapan. **Note** Greengrass tidak mencatat peristiwa yang ditolak akses.	Penyebaran Greengrass IoT	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada aset.	Aset IoT SiteWise	`AWS::IoTSiteWise::Asset`
	Aktivitas SiteWise API IoT pada deret waktu.	Deret waktu IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT pada entitas.	Entitas IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
	Aktivitas TwinMaker API IoT di ruang kerja.	Ruang kerja IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Peringkat Cerdas Amazon Kendra	Aktivitas API Peringkat Cerdas Amazon Kendra pada rencana eksekusi skor ulang.	Peringkat Kendra	`AWS::KendraRanking::ExecutionPlan`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces di atas meja.	Meja Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis	Aktivitas API Amazon Kinesis pada aliran video, seperti panggilan ke dan. `GetMedia` `PutMedia`	Aliran video Kinesis	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Aktivitas API Amazon Managed Blockchain di jaringan.	Jaringan Blockchain yang dikelola	`AWS::ManagedBlockchain::Network`
	Amazon Managed Blockchain JSON-RPC memanggil node Ethereum, seperti atau. `eth_getBalance` `eth_getBlockByNumber`	Blockchain yang Dikelola	`AWS::ManagedBlockchain::Node`
Grafik Amazon Neptunus	Aktivitas API data, misalnya kueri, algoritme , atau pencarian vektor, pada Grafik Neptunus.	Grafik Neptunus	`AWS::NeptuneGraph::Graph`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS Private CA	AWS Private CA Konektor untuk aktivitas Active Directory API.	AWS Private CA Konektor untuk Active Directory	`AWS::PCAConnectorAD::Connector`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada aplikasi.	Aplikasi Amazon Q Business	`AWS::QBusiness::Application`
	Aktivitas Amazon Q Business API pada sumber data.	Sumber data Amazon Q Business	`AWS::QBusiness::DataSource`
	Aktivitas API Amazon Q Business pada indeks.	Amazon Q Indeks Bisnis	`AWS::QBusiness::Index`
	Aktivitas Amazon Q Business API pada pengalaman web.	Pengalaman web Amazon Q Bisnis	`AWS::QBusiness::WebExperience`
Amazon RDS	Aktivitas Amazon RDS API di Cluster DB.	API Data RDS - Kluster DB	`AWS::RDS::DBCluster`
Amazon S3	Aktivitas API Amazon S3 pada titik akses.	Titik Akses S3	`AWS::S3::AccessPoint`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Aktivitas API titik akses Objek Lambda Amazon S3, seperti panggilan ke dan. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 pada aktivitas API tingkat objek Outposts.	Outposts S3	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Aktivitas Amazon di titik akhir.	SageMaker titik akhir	`AWS::SageMaker::Endpoint`
	Aktivitas SageMaker API Amazon di toko fitur.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`
	Aktivitas Amazon SageMaker API pada komponen percobaan percobaan.	SageMaker komponen uji coba eksperimen metrik	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Operasi `Publish`API Amazon SNS pada titik akhir platform.	Titik akhir platform SNS	`AWS::SNS::PlatformEndpoint`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Operasi Amazon SNS `Publish`dan `PublishBatch` API pada topik.	Topik SNS	`AWS::SNS::Topic`
Amazon SQS	Aktivitas Amazon SQS API pada pesan.	SQS	`AWS::SQS::Queue`
Rantai Pasokan AWS	Rantai Pasokan AWS Aktivitas API pada sebuah instance.	Rantai Pasokan	`AWS::SCN::Instance`
Amazon SWF	Aktivitas API Amazon SWF di domain.	Domain SWF	`AWS::SWF::Domain`
AWS Systems Manager	Aktivitas API Systems Manager pada saluran kontrol.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Aktivitas API Systems Manager pada node terkelola.	Node terkelola Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Aktivitas `Query`API Amazon Timestream pada database.	Database Timestream	`AWS::Timestream::Database`
	Aktivitas `Query`API Amazon Timestream pada tabel.	Tabel Timestream	`AWS::Timestream::Table`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Izin Terverifikasi Amazon	Aktivitas API Izin Terverifikasi Amazon di toko kebijakan.	Izin Terverifikasi Amazon	`AWS::VerifiedPermissions::PolicyStore`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Perangkat.	Perangkat Klien Tipis	`AWS::ThinClient::Device`
	WorkSpaces Aktivitas API Klien Tipis di Lingkungan.	Lingkungan Klien Tipis	`AWS::ThinClient::Environment`
AWS X-Ray	Aktivitas X-Ray API pada jejak.	Jejak X-Ray	`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. Lihat informasi yang lebih lengkap di Membuat jejak dan Buat penyimpanan data acara untuk CloudTrail acara.

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

Apa itu acara Insights?

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.

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. Untuk informasi selengkapnya tentang membuat penyimpanan data acara, lihatMembuat penyimpanan data acara untuk acara CloudTrail Insights.

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 Harga AWS CloudTrail.

Bagaimana cara melihat peristiwa Insights untuk jejak dan penyimpanan data acara?

CloudTrail mendukung peristiwa Wawasan untuk penyimpanan data jejak dan acara, 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 CloudTrail Wawasan untuk jejak di konsol CloudTrail .

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 CloudTrail Insights.

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 Amazon S3. Lihat informasi yang lebih lengkap di Membuat atau mengedit kueri dan Melihat contoh kueri di konsol CloudTrail .

Anda dapat melihat dasbor CloudTrail Danau untuk memvisualisasikan peristiwa Wawasan di penyimpanan data acara tujuan Anda. Untuk informasi lebih lanjut tentang dasbor Danau, lihatLihat dasbor Danau.

Apa itu sejarah CloudTrail peristiwa?

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 AWS Management Console, 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.

Apa itu jalan setapak?

Trail adalah konfigurasi yang memungkinkan pengiriman CloudTrail peristiwa ke bucket Amazon S3, CloudWatch Log, dan Amazon. EventBridge Anda dapat menggunakan jejak untuk memfilter CloudTrail peristiwa yang ingin dikirim, 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.

Apa itu jalur 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 OPT, 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 OPT, salinan jejak 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 AWS 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 organisasi.

Bagaimana Anda mengelola CloudTrail?

CloudTrail konsol

Anda dapat menggunakan dan mengelola layanan dengan AWS CloudTrail konsol. 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.
- 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
  - Menggunakan AWS KMS kunci untuk enkripsi data penyimpanan data acara.
  - Menambahkan dan mengelola tag untuk penyimpanan data acara Anda.

Mulai 12 April 2019, jalur hanya dapat dilihat di AWS Wilayah tempat mereka mencatat peristiwa. Jika Anda membuat jejak yang mencatat peristiwa di semua AWS Wilayah, itu akan muncul di konsol di semua AWS Wilayah. Jika Anda membuat jejak yang hanya mencatat peristiwa di satu AWS Wilayah, Anda dapat melihat dan mengelolanya hanya di AWS Wilayah tersebut.

Untuk informasi lebih lanjut tentang AWS Management Console, lihat AWS Management Console.

CloudTrail 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 Perintah yang Tersedia.

CloudTrail API

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

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 halaman Alat untuk Amazon Web Services.

Mengapa menggunakan tag untuk CloudTrail sumber daya?

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 Amazon 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 Amazon 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 mengetahui informasi lebih lanjut, lihat AWS Strategi Penandaan.

Bagaimana Anda mengontrol akses ke CloudTrail?

AWS Identity and Access Management adalah layanan web yang memungkinkan pelanggan Amazon Web Services (AWS) untuk mengontrol akses ke AWS sumber daya dengan aman. Menggunakan IAM, Anda dapat mengelola izin secara terpusat yang mengontrol CloudTrail sumber daya mana yang dapat diakses pengguna. Untuk informasi selengkapnya tentang mengontrol izin pengguna, lihatMengontrol izin pengguna untuk CloudTrail jalan setapak.

Bagaimana Anda mencatat manajemen dan peristiwa data?

Secara default, melacak peristiwa manajemen log untuk AWS akun Anda dan tidak menyertakan peristiwa data. Anda dapat memilih untuk membuat atau memperbarui jejak untuk mencatat peristiwa data. Hanya peristiwa yang cocok dengan setelan jejak yang dikirimkan ke bucket Amazon S3, dan secara opsional ke grup CloudWatch log Amazon Log. Jika acara tidak cocok dengan pengaturan untuk jejak, jejak tidak mencatat peristiwa. Untuk informasi selengkapnya, lihat Bekerja dengan file CloudTrail log.

Bagaimana Anda mencatat peristiwa CloudTrail Wawasan?

AWS 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. Untuk informasi selengkapnya, lihat Acara Logging Insights dan Harga AWS CloudTrail.

Bagaimana Anda menjalankan kueri kompleks pada peristiwa yang dicatat oleh? CloudTrail

CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL halus pada acara Anda, dan mencatat peristiwa dari sumber di luar, termasuk dari aplikasi Anda sendiri AWS, dan dari mitra yang terintegrasi dengannya. CloudTrail Anda tidak perlu memiliki jejak yang dikonfigurasi di akun Anda untuk menggunakan CloudTrail Lake. Penyimpanan data acara adalah 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun. 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 Amazon Simple Storage Service. 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.

Bagaimana Anda melakukan pemantauan dengan CloudTrail?

CloudWatch Log, EventBridge, dan CloudTrail

Amazon CloudWatch adalah layanan web yang mengumpulkan dan melacak metrik untuk memantau sumber daya Amazon Web Services (AWS) dan aplikasi yang Anda jalankan. AWS Amazon CloudWatch Logs adalah fitur CloudWatch yang dapat Anda gunakan secara khusus untuk memantau data log. Integrasi dengan CloudWatch Log memungkinkan CloudTrail untuk mengirim peristiwa yang berisi aktivitas API di AWS akun Anda ke grup CloudWatch log Log. CloudTrail peristiwa yang dikirim ke CloudWatch Log dapat memicu alarm sesuai dengan filter metrik yang Anda tentukan. Anda dapat mengonfigurasi CloudWatch alarm secara opsional untuk mengirim

pemberitahuan atau membuat perubahan pada sumber daya yang Anda pantau berdasarkan peristiwa aliran log yang diekstrak oleh filter metrik Anda. Menggunakan CloudWatch Log, Anda juga dapat melacak CloudTrail peristiwa bersama peristiwa dari sistem operasi, aplikasi, atau AWS layanan lain yang dikirim ke CloudWatch Log. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

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 Saat Anda membuat aturan dengan EventBridge konsol, pilih tipe `AWS API Call via CloudTrail` detail untuk mengirimkan CloudTrail data dan peristiwa manajemen, atau tipe `AWS Insight via CloudTrail` detail untuk mengirimkan peristiwa Insights.

Untuk merekam peristiwa dengan nilai tipe detail`AWS API Call via CloudTrail`, Anda harus memiliki jejak aktif yang mencatat manajemen atau peristiwa data. Untuk informasi selengkapnya tentang cara membuat jejak, lihatMembuat jejak.

Untuk merekam peristiwa dengan nilai tipe detail`AWS Insight via CloudTrail`, Anda harus memiliki jejak aktif yang mencatat peristiwa Wawasan. Untuk informasi tentang mencatat peristiwa Wawasan, lihatAcara Logging Insights.

Bagaimana CloudTrail berperilaku regional dan global?

Jejak dapat diterapkan ke semua Wilayah atau satu Wilayah. Sebagai praktik terbaik, buat jejak yang berlaku untuk semua Wilayah di AWS partisi tempat Anda bekerja. Ini adalah pengaturan default saat Anda membuat jejak di CloudTrail konsol.

> **Note**
>
> Menghidupkan jejak berarti Anda membuat jejak dan memulai pengiriman file log CloudTrail peristiwa ke bucket Amazon S3. Di CloudTrail konsol, logging diaktifkan secara otomatis saat Anda membuat jejak.

Apa keuntungan menerapkan jejak ke semua Wilayah?

Jejak yang berlaku untuk semua AWS Wilayah memiliki keuntungan sebagai berikut:

- Pengaturan konfigurasi untuk jejak berlaku secara konsisten di semua AWS Wilayah.
- Anda menerima CloudTrail peristiwa dari semua AWS Wilayah dalam satu bucket Amazon S3 dan, secara opsional, dalam grup CloudWatch log Log.
- Anda mengelola konfigurasi jejak untuk semua AWS Wilayah dari satu lokasi.
- Anda segera menerima acara dari AWS Wilayah baru. Saat AWS Wilayah baru diluncurkan, CloudTrail secara otomatis membuat salinan semua jalur Wilayah Anda untuk Anda di Wilayah baru dengan pengaturan yang sama dengan jejak asli Anda.
- Anda tidak perlu membuat jalur di AWS Wilayah yang tidak sering Anda gunakan untuk memantau aktivitas yang tidak biasa. Aktivitas apa pun di AWS Wilayah mana pun dicatat dalam jejak yang berlaku untuk semua AWS Wilayah.

Apa yang terjadi ketika Anda menerapkan jejak ke semua Wilayah?

Saat Anda menerapkan jejak ke semua AWS Wilayah, CloudTrail gunakan jejak yang Anda buat di Wilayah tertentu untuk membuat jalur dengan konfigurasi identik di semua Wilayah lain di AWS partisi tempat Anda bekerja.

Ini memiliki efek sebagai berikut:

- CloudTrail mengirimkan file log untuk aktivitas akun dari semua AWS Wilayah 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 AWS Wilayah akan dikirim ke topik SNS tunggal tersebut.
- Jika Anda mengaktifkannya, validasi integritas file log diaktifkan untuk jejak di semua AWS Wilayah. Untuk informasi, lihat Memvalidasi CloudTrail integritas berkas log.

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 namun 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 yang berlaku untuk semua AWS Wilayah dianggap sebagai satu jejak di setiap Wilayah.

Contoh berikut adalah Wilayah dengan lima jalur:

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

Jalur muncul di AWS Wilayah tempat mereka ada. Jejak yang mencatat peristiwa di semua AWS Wilayah muncul di setiap Wilayah. Anda dapat melihat daftar jejak di AWS Wilayah di halaman Jalur konsol. CloudTrail Untuk informasi selengkapnya, lihat Memperbarui jejak. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

AWS Security Token Service dan CloudTrail

AWS Security Token Service (AWS STS) adalah layanan yang memiliki titik akhir global dan juga mendukung titik akhir khusus Wilayah. 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 titik akhir AWS STS khusus Wilayah, jejak di Wilayah tersebut 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 AWS STS peristiwa yang berasal dari us-barat-2. 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-timur-1. 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.
- Jika Anda mengubah konfigurasi jejak dari mencatat semua Wilayah menjadi mencatat satu Wilayah, pencatatan peristiwa layanan global akan dimatikan secara otomatis untuk jejak tersebut. Demikian pula, jika Anda mengubah konfigurasi jejak dari mencatat satu Wilayah menjadi mencatat semua Wilayah, pencatatan peristiwa layanan global diaktifkan secara otomatis untuk jejak tersebut.

  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 Command Line Interface.

> **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.

Bagaimana CloudTrail kaitannya dengan layanan AWS pemantauan lainnya?

CloudTrail menambahkan dimensi lain pada kemampuan pemantauan yang sudah ditawarkan oleh AWS. Itu tidak mengubah atau mengganti fitur logging yang mungkin sudah Anda gunakan, seperti untuk langganan Amazon S3 atau Amazon CloudFront . Amazon CloudWatch berfokus pada pemantauan kinerja dan kesehatan sistem. CloudTrail berfokus pada aktivitas API. Meskipun CloudTrail tidak melaporkan kinerja sistem atau kesehatan, Anda dapat menggunakan CloudTrail dengan CloudWatch alarm untuk memberi tahu Anda tentang aktivitas yang mungkin Anda minati.

Solusi mitra

AWS bermitra dengan spesialis pihak ketiga dalam pencatatan dan analisis untuk memberikan solusi yang menggunakan CloudTrail output. Untuk informasi lebih lanjut, kunjungi halaman CloudTrail detail di AWS CloudTrail.

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	Wilayah	Kontrol titik akhir pesawat	Protokol	Tanggal Support
US East (Northern Virginia)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	11/13/2013
Timur AS (Ohio)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	10/17/2016
US West (Northern California)	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
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
Afrika (Cape Town)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	04/22/2020

Nama wilayah	Wilayah	Kontrol titik akhir pesawat	Protokol	Tanggal Support
Asia Pasifik (Hong Kong)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	04/24/2019
Asia Pasifik (Mumbai)	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	06/27/2016
Asia Pasifik (Hyderabad)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	11/22/2022
Asia Pasifik (Tokyo)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	06/30/2014
Asia Pasifik (Seoul)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	01/06/2016
Asia Pacific (Osaka)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	02/12/2018
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 (Jakarta)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
Asia Pacific (Melbourne)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	01/23/2023
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

Nama wilayah	Wilayah	Kontrol titik akhir pesawat	Protokol	Tanggal Support
Eropa (Frankfurt)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	10/23/2014
Europe (Zurich)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
Eropa (Stockholm)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	12/11/2018
Eropa (Irlandia)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	05/13/2014
Eropa (London)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	12/13/2016
Eropa (Paris)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	12/18/2017
Eropa (Milan)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	04/27/2020
Eropa (Spanyol)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
Israel (Tel Aviv)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	07/31/2023
Timur Tengah (UAE)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	08/30/2022
Timur Tengah (Bahrain)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	07/29/2019

Nama wilayah	Wilayah	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
Amerika Selatan (Sao Paulo)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	06/30/2014

Untuk informasi selengkapnya tentang penggunaan CloudTrail di Wilayah AWS GovCloud (AS-Timur), lihat Titik Akhir AWS GovCloud (AS-Timur) di Panduan Pengguna. AWS GovCloud (US)

Untuk informasi selengkapnya tentang penggunaan CloudTrail di Wilayah AWS GovCloud (AS-Barat), lihat Titik Akhir AWS GovCloud (AS-Barat) di Panduan Pengguna. AWS GovCloud (US)

Untuk informasi lebih lanjut tentang penggunaan CloudTrail di Wilayah China (Beijing), lihat Titik Akhir Wilayah China (Beijing) di Referensi Umum Amazon Web Services.

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
```

- ItuYYYY,MM, DDHH,, dan mm merupakan digit tahun, bulan, hari, jam, dan menit ketika file log dikirimkan. 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 isi rekaman.

Daftar Isi

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 untuk Instans Linux.

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 mengontrol AWS sumber daya mana 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 `AddUserToGroup`tindakan 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": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "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, lihatAcara Logging Insights.


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


CloudTrail layanan dan integrasi yang didukung

CloudTrail mendukung peristiwa logging untuk banyak AWS layanan. Anda dapat menemukan spesifikasi untuk setiap layanan yang didukung dalam panduan layanan itu. Tautan ke topik khusus layanan tersebut disediakan di bawah ini. Selain itu, beberapa AWS layanan dapat digunakan untuk menganalisis dan menindaklanjuti data yang dikumpulkan dalam CloudTrail log. Anda dapat menelusuri ikhtisar integrasi layanan tersebut di sini.

> **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
- 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. Lihat informasi yang lebih lengkap di 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 Lake, 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 meningkatkan analisis aktivitas AWS layanan Anda. Misalnya, Anda dapat menggunakan kueri untuk mengidentifikasi tren dan mengisolasi aktivitas selengkapnya berdasarkan atribut seperti alamat IP sumber atau pengguna. Anda dapat secara otomatis membuat tabel untuk

AWS Layanan	Topik	Deskripsi
		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	Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log	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 Saat Anda membuat aturan dengan EventBridge konsol, pilih tipe `AWS API Call via CloudTrail` detail

untuk mengirimkan CloudTrail data dan peristiwa manajemen, atau tipe `AWS Insight via CloudTrail` detail untuk mengirimkan peristiwa Insights.

Untuk merekam peristiwa dengan nilai tipe detail`AWS API Call via CloudTrail`, Anda harus memiliki jejak yang saat ini mencatat manajemen atau peristiwa data. Untuk informasi selengkapnya tentang cara membuat jejak, lihatMembuat jejak.

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, lihatAcara Logging Insights.

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 membantu Anda menentukan strategi pencatatan peristiwa yang seragam untuk organisasi Anda.

Jejak organisasi diterapkan secara otomatis ke setiap AWS akun di organisasi Anda. Pengguna di akun anggota dapat melihat jejak ini tetapi tidak dapat memodifikasinya, dan secara default tidak dapat melihat file log yang dibuat untuk jejak organisasi. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi.

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. CloudTrail saat ini tidak mencatat peristiwa khusus kebijakan titik akhir Amazon VPC.

> **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
Amazon AppStream 2.0	Mencatat Panggilan API Amazon AppStream 2.0 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
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	Pencatatan Panggilan API Amazon Cloud Directory	01/26/2017

AWS Layanan	CloudTrail Topik	Support dimulai
	Menggunakan AWS CloudTrail	
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 AWS CloudTrail	04/30/2014
CloudWatch Acara Amazon	Logging Amazon CloudWatch Events API Panggilan di AWS CloudTrail	01/16/2016
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
CodeGuru Peninjau Amazon	Mencatat Panggilan API Amazon CodeGuru Reviewer dengan AWS CloudTrail	12/02/2019

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon CodeWhisperer	AWS CloudTrail dan CodeWhisperer API	04/13/2023
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
Amazon Connect	Mencatat Panggilan API Amazon Connect dengan AWS CloudTrail	12/11/2019
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
Amazon DocumentDB (dengan kompatibilitas MongoDB)	Mencatat Panggilan API Amazon DocumentDB dengan AWS CloudTrail	01/09/2019

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon DynamoDB	Logging Operasi DynamoDB Dengan Menggunakan AWS CloudTrail	05/28/2015
Amazon EC2	Pencatatan Panggilan API 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: 11/13/2013 API langsung EBS: 30/06/2020
Amazon Elastic Container Registry (Amazon ECR)	Mencatat Panggilan API ECR Amazon Dengan Menggunakan AWS CloudTrail	12/21/2015
Amazon Elastic Container Service (Amazon ECS)	Pencatatan Panggilan API Amazon ECS Dengan Menggunakan AWS CloudTrail	04/09/2015

AWS Layanan	CloudTrail Topik	Support dimulai
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 Elastic Transcoder	Mencatat Panggilan API Amazon Elastic Transcoder dengan AWS CloudTrail	10/27/2014
Amazon ElastiCache	Pencatatan Panggilan ElastiCache API Amazon Menggunakan AWS CloudTrail	09/15/2014
Amazon EMR	Mencatat Panggilan API EMR Amazon di AWS CloudTrail	04/04/2014
Amazon EMR di EKS	Logging Amazon EMR pada panggilan EKS API menggunakan AWS CloudTrail	12/09/2020
Amazon EventBridge	EventBridge informasi di AWS CloudTrail	07/11/2019
Amazon FinSpace	Memeriksa 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
Amazon GameLift	Mencatat Panggilan GameLift API Amazon dengan AWS CloudTrail	01/27/2016
Amazon GuardDuty	Mencatat Panggilan GuardDuty API Amazon dengan AWS CloudTrail	02/12/2018
Amazon Honeycode	Mencatat Panggilan API Honeycode Amazon dengan AWS CloudTrail	06/24/2020
Amazon Inspector	Mencatat panggilan Amazon Inspector API dengan AWS CloudTrail	04/20/2016
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	Memantau Amazon Managed Service untuk Apache Flink dengan AWS CloudTrail (Aplikasi SQL) dan Memantau Amazon Managed Service untuk Apache Flink dengan AWS CloudTrail (Apache Flink Applications)	03/22/2019
Amazon Data Firehose	Memantau Panggilan API Firehose Data Amazon dengan AWS CloudTrail	03/17/2016
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

AWS Layanan	CloudTrail Topik	Support dimulai
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 panggilan Amazon Lookout for Equipment dengan AWS CloudTrail	12/01/2020
Amazon Lookout for Metrics	Melihat aktivitas Amazon Lookout for Metrics API di AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	Mencatat panggilan Amazon Lookout for Vision dengan AWS CloudTrail	12/01/2020
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

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Managed Grafana	Mencatat panggilan API Grafana yang Dikelola Amazon menggunakan AWS CloudTrail	12/15/2020
Layanan Terkelola Amazon untuk Prometheus	Logging Amazon Managed Service untuk panggilan API Prometheus menggunakan AWS CloudTrail	12/15/2020
Amazon Managed Streaming untuk Apache Kafka	Mencatat Panggilan API MSK Amazon dengan AWS CloudTrail	12/11/2018
Amazon Managed Workflows for Apache Airflow (MWAA)	Memantau aktivitas Amazon MWAA API dengan AWS CloudTrail	11/24/2020
Amazon MemoryDB for Redis	Logging Amazon MemoryDB untuk panggilan Redis API 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 CloudTrai l	05/30/2018
Amazon Nimble Studio	Logging panggilan Nimble Studio menggunakan AWS CloudTrail	06/19/2023

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon Satu Perusahaan	Mencatat panggilan API Amazon One Enterprise menggunakan AWS CloudTrail	11/27/2023
OpenSearch Layanan Amazon	Mengaudit Domain 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
Amazon Polly	Mencatat Panggilan API Amazon Polly dengan AWS CloudTrail	11/30/2016
Amazon Q (Untuk Penggunaan Bisnis)	Mencatat panggilan Amazon Q API menggunakan AWS CloudTrail	11/28/2023
Amazon Q (Untuk Penggunaan AWS Builder)	Mencatat panggilan Amazon Q API menggunakan AWS CloudTrail	11/28/2023
Amazon Quantum Ledger Database (Amazon QLDB)	Mencatat Panggilan API QLDB Amazon dengan AWS CloudTrail	09/10/2019

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon QuickSight	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
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
Pengendali Pemulihan Aplikasi Amazon Route 53	Logging Amazon Route 53 Application Recovery Controller API menggunakan AWS CloudTrail	07/27/2021

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon S3	Mencatat Panggilan API Amazon S3 Dengan Menggunakan AWS CloudTrail	Acara manajemen: 09/01/2015 Data peristiwa: 11/21/2016
Amazon S3 Glacier	Logging S3 Glacier API Panggilan Dengan Menggunakan AWS CloudTrail	12/11/2014
Amazon SageMaker	Mencatat Panggilan SageMaker API Amazon dengan AWS CloudTrail	01/11/2018
Amazon Security Lake	Mencatat panggilan Amazon Security Lake API menggunakan CloudTrail	05/30/2023
Amazon Simple Email Service (Amazon SES)	Pencatatan Panggilan API Amazon SES Dengan Menggunakan AWS CloudTrail	05/07/2015
Amazon Simple Notification Service (Amazon SNS)	Logging Amazon Simple Notification Service API Panggilan Dengan 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: 13/05/2014 Data peristiwa: 02/14/2024

AWS Layanan	CloudTrail Topik	Support dimulai
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
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

AWS Layanan	CloudTrail Topik	Support dimulai
Amazon WorkDocs	Pencatatan 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
WorkSpaces Web Amazon	Pencatatan panggilan Amazon WorkSpaces Web API menggunakan AWS CloudTrail	11/30/2021
Application Auto Scaling	Logging Application Auto Scaling API panggilan dengan AWS CloudTrail	10/31/2016
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 03/18/2022

AWS Layanan	CloudTrail Topik	Support dimulai
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 Profiler Biaya Aplikasi	AWS Referensi API Profiler Biaya Aplikasi	05/13/2021
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	Logging panggilan AWS Audit Manager API dengan AWS CloudTrail	12/07/2020

AWS Layanan	CloudTrail Topik	Support dimulai
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 Billing and Cost Management	Pencatatan Panggilan AWS Billing and Cost Management API dengan AWS CloudTrail	06/07/2018
AWS Billing Conductor	Pencatatan panggilan AWS Billing Conductor API menggunakan AWS CloudTrail	03/12/2024
AWS BugBust	Pencatatan panggilan BugBust API menggunakan CloudTrail	06/24/2021
AWS Certificate Manager	Menggunakan AWS CloudTrail	03/25/2016
AWS Clean Rooms	Pencatatan panggilan AWS Clean Rooms API menggunakan AWS CloudTrail	03/21/2023

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Cloud Map	Logging AWS Cloud Map API Calls 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 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 Layanan	CloudTrail Topik	Support dimulai
AWS CodeDeploy	Memantau Deployment dengan AWS CloudTrail	12/16/2014
AWS CodePipeline	Pencatatan Panggilan CodePipeline API Dengan Menggunakan AWS CloudTrai l	07/09/2015
AWS CodeStar	Pencatatan Panggilan AWS CodeStar API dengan AWS CloudTrail	06/14/2017
AWS CodeStar Pemberita huan	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 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 CloudTrai l	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 Layanan	CloudTrail Topik	Support dimulai
AWS Batas Waktu Cloud	Pencatatan panggilan dengan CloudTrail	04/02/2024
AWS Device Farm	Pencatatan Panggilan AWS Device Farm API Dengan Menggunakan AWS CloudTrail	07/13/2015
AWS Direct Connect	Pencatatan Panggilan AWS Direct Connect API di AWS CloudTrail	03/08/2014
AWS Directory Service	Pencatatan Panggilan AWS Directory Service API dengan Menggunakan CloudTrail	05/14/2015
AWS Elastic Beanstalk (Elastic Beanstalk)	Menggunakan Panggilan API Elastic Beanstalk dengan AWS CloudTrail	03/31/2014
AWS Elastic Disaster Recovery	Pencatatan 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 Layanan	CloudTrail Topik	Support dimulai
AWS Elemental MediaPackage	Pencatatan Panggilan AWS Elemental MediaPackage API dengan AWS CloudTrail	12/21/2018
AWS Elemental MediaStore	Pencatatan Panggilan AWS Elemental MediaStore API dengan CloudTrail	11/27/2017
AWS Elemental MediaTailor	Pencatatan Panggilan AWS Elemental MediaTailor API dengan AWS CloudTrail	02/11/2019
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 Layanan	CloudTrail Topik	Support dimulai
AWS Health	Pencatatan Panggilan AWS Health API dengan AWS CloudTrail	11/21/2016
AWS Health Dashboard	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 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 1-Click	Pencatatan Panggilan AWS IoT 1-Click API dengan AWS CloudTrail	05/14/2018

AWS Layanan	CloudTrail Topik	Support dimulai
AWS IoT Analitik	Logging panggilan API AWS IoT Analytics dengan AWS CloudTrail	04/23/2018
AWS IoT Event	Logging AWS IoT Events API Panggilan dengan AWS CloudTrail	06/11/2019
AWS IoT Greengrass	Pencatatan Panggilan AWS IoT Greengrass API dengan AWS CloudTrail	10/29/2018
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 Menggunakan Lambda dengan AWS CloudTrail	Acara manajemen: 04/09/2015 Data peristiwa: 11/30/2017

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Launch Wizard	Pencatatan 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	Pencatatan panggilan AWS Mainframe Modernization API menggunakan AWS CloudTrail	06/08/2022
AWS Managed Services	Manajemen log di AMS Accelerate	12/21/2016
AWS Marketplace	Pencatatan Panggilan AWS Marketplace API dengan AWS CloudTrail	05/02/2017
AWS Marketplace Perjanjian	Perjanjian Pencatatan Panggilan API menggunakan AWS CloudTrail	09/01/2023
AWS Marketplace Layanan Deployment	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 Layanan	CloudTrail Topik	Support dimulai
AWS Migration Hub	Mencatat Panggilan API AWS Migration Hub dengan AWS CloudTrail	08/14/2017
AWS Mobile Hub	Mencatat AWS Panggilan API CLI Seluler dengan AWS CloudTrail	06/29/2018
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 Perusahaan Boneka dengan AWS CloudTrail	07/16/2018
AWS OpsWorks Stacks	Pencatatan Panggilan AWS OpsWorks Stacks API dengan AWS CloudTrail	06/04/2014
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 Panorama	Referensi AWS Panorama API	10/20/2021

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Payment Cryptography	Pencatatan panggilan AWS Payment Cryptography API menggunakan AWS CloudTrail	06/08/2023
AWS 5G pribadi	Mencatat panggilan API 5G AWS Pribadi menggunakan AWS CloudTrail	08/11/2022
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	Pencatatan panggilan Penjelajah Sumber Daya AWS API menggunakan AWS CloudTrail	11/07/2022
AWS Resource Groups	Pencatatan Panggilan AWS Resource Groups API dengan AWS CloudTrail	06/29/2018

AWS Layanan	CloudTrail Topik	Support dimulai
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	Pencatatan Panggilan AWS Security Hub API dengan AWS CloudTrail	11/27/2018
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	Pencatatan Panggilan AWS Snowball API dengan AWS CloudTrail	01/25/2019
AWS Snowball Tepi	Logging AWS Snowball Edge API Panggilan dengan AWS CloudTrail	01/25/2019

AWS Layanan	CloudTrail Topik	Support dimulai
AWS Step Functions	Pencatatan Panggilan AWS Step Functions API dengan AWS CloudTrail	12/01/2016
Storage Gateway	Mencatat Panggilan API Storage Gateway dengan Menggunakan AWS CloudTrail	12/16/2014
AWS Support	Pencatatan Panggilan AWS Support API dengan AWS CloudTrail	04/21/2016
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 Layanan	CloudTrail Topik	Support dimulai
AWS Trusted Advisor	Mencatat tindakan AWS Trusted Advisor konsol dengan AWS CloudTrail	10/22/2020
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
Penyeimbang Beban Elastis	AWS CloudTrail Logging untuk Classic Load Balancer dan AWS CloudTrail Logging untuk Application Load Balancer Anda	04/04/2014
Pembaruan FreeRTOS Over-the-Air (OTA)	Mencatat Panggilan API AWS IoT OTA dengan AWS CloudTrail	05/22/2019
Kuota Layanan	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, berikutAWSlayanan dan acara tidak didukung:

- AWS Import/Export
- Acara VPC endpoint endpoint Amazon

Untuk daftar yang didukungAWSlayanan, lihatAWS topik layanan untuk CloudTrail.

Kuota di AWS CloudTrail

Tabel berikut menjelaskan kuota (sebelumnya disebut sebagai batas) di dalamnya. CloudTrail CloudTrail tidak memiliki kuota yang dapat disesuaikan. Untuk informasi tentang kuota lain diAWS, lihat kuota AWS layanan.

Sumber daya	Kuota bawaan	Komentar
Jalur per Wilayah	5	Kuota ini tidak dapat dinaikkan jumlahnya.
Dapatkan, jelaskan, dan daftar API	10 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling. `StartQuery` API `CancelQuery` `LookupEvents` ,`ListInsightsMetricData` ,`PutAuditEvents` , dan tidak termasuk dalam kategori ini.
CancelQuery, StartQuery API	3 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda

Sumber daya	Kuota bawaan	Komentar
		lakukan per detik tanpa mengalami throttling. Kuota ini tidak dapat dinaikkan jumlahnya.
LookupEvents API	2 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling. Kuota ini tidak dapat dinaikkan jumlahnya.
ListInsightsMetricData API	1 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling. Kuota ini tidak dapat dinaikkan jumlahnya.
PutAuditEvents API	100 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling. Kuota ini tidak dapat dinaikkan jumlahnya.
Semua API lainnya	1 transaksi per detik (TPS)	Jumlah maksimal permintaan operasi yang dapat Anda lakukan per detik tanpa mengalami throttling. Kuota ini tidak dapat dinaikkan jumlahnya.

Sumber daya	Kuota bawaan	Komentar
Menyimpan data acara	10	Jumlah maksimum penyimpanan data acara yang dapat Anda miliki di salah satuWilayah AWS. Ini termasuk penyimpanan data acara Single-region untuk Wilayah serta penyimpanan data acara Multi-wilayah di semua. Wilayah AWS Ini termasuk penyimpanan data acara di setiap tahap siklus hidup. Kuota ini tidak dapat dinaikkan jumlahnya.
Saluran	25	Kuota ini berlaku untuk saluran yang digunakan untuk integrasi CloudTrail Lake dengan sumber acara di luarAWS, dan tidak berlaku untuk saluran terkait layanan. 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.

Sumber daya	Kuota bawaan	Komentar
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.
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. Kecuali penyimpanan data jejak atau peristiwa mencatat peristiwa data pada semua sumber daya, seperti semua bucket S3 atau semua fungsi Lambda, Anda dibatasi hingga 250 sumber daya data. Sumber daya data dapat didistribusikan di seluruh pemilih acara, tetapi total keseluruhan tidak dapat melebihi 250. 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 atau pemilih acara lanjutan, 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	File ZIP 50 MB, setelah kompresi	Untuk peristiwa manajemen dan data, CloudTrail kirimkan peristiwa ke S3 dalam file ZIP maksimum 50 MB (terkompr esi). Jika diaktifkan di jalur, pemberitahuan pengiriman log dikirim oleh Amazon SNS setelah CloudTrail mengirim file ZIP ke S3.

Memulai dengan AWS CloudTrail tutorial

Jika Anda baru mengenal AWS CloudTrail, tutorial ini membantu Anda mempelajari cara menggunakan fitur-fiturnya.

Topik

Prasyarat

Bagian ini memberikan informasi umum tentang cara mengatur Akun AWS dan menjelaskan kebijakan terkelola tersedia untuk CloudTrail.

Topik

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai

praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

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

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan Pengguna AWS Sign-In .
2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke sebuah pengguna administratif.

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

Masuk sebagai pengguna administratif

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

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

Berikan izin untuk digunakan CloudTrail

Untuk membuat, memperbarui, dan mengelola CloudTrail sumber daya seperti jejak, penyimpanan data acara, dan saluran, Anda harus memberikan izin untuk digunakan. CloudTrail

> **Note**
>
> Izin yang Anda berikan kepada pengguna untuk melakukan tugas CloudTrail administrasi tidak sama dengan izin yang CloudTrail diperlukan 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, Anda CloudTrail juga memerlukan peran yang dapat diasumsikan untuk mengirimkan peristiwa ke grup CloudWatch log Amazon Logs. Anda harus membuat peran yang CloudTrail menggunakan. Lihat informasi yang lebih lengkap di Memberikan izin untuk melihat dan mengonfigurasi informasi CloudWatch Log Amazon di konsol CloudTrail dan Mengirim acara ke CloudWatch Log.

Kebijakan AWS terkelola berikut tersedia untuk CloudTrail:

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

  Kebijakan ini juga menyediakan izin untuk mengelola bucket Amazon S3, grup log CloudWatch untuk Log, dan topik Amazon SNS untuk jejak. Namun, kebijakan `AWSCloudTrail_FullAccess` terkelola tidak memberikan izin untuk menghapus bucket Amazon S3, grup log CloudWatch untuk

Log, atau topik Amazon SNS. Untuk informasi tentang kebijakan terkelola untuk AWS layanan lain, lihat Panduan Referensi Kebijakan AWS 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 ke administrator akun. Anda harus mengontrol dan memantau penggunaan kebijakan ini dengan cermat.

- AWSCloudTrail_ReadOnlyAccess— Kebijakan ini memberikan izin untuk melihat CloudTrail konsol, termasuk peristiwa terbaru dan riwayat acara. Kebijakan ini juga memungkinkan Anda untuk melihat jejak 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, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti petunjuk dalam Buat set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

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

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

Tutorial: Tinjau aktivitas AWS akun dalam riwayat acara

CloudTrail aktif di AWS akun Anda saat Anda membuat akun. Ketika aktivitas API yang didukung (peristiwa manajemen) terjadi di AWS layanan apa pun yang mendukung CloudTrail, aktivitas tersebut direkam dalam peristiwa CloudTrail manajemen bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Dengan kata lain, Anda dapat melihat, mencari, dan mengunduh peristiwa manajemen terbaru di AWS akun Anda sebelum membuat penyimpanan atau jejak data acara, meskipun membuat penyimpanan atau jejak data acara penting untuk catatan jangka panjang dan audit aktivitas AWS akun Anda.

Note

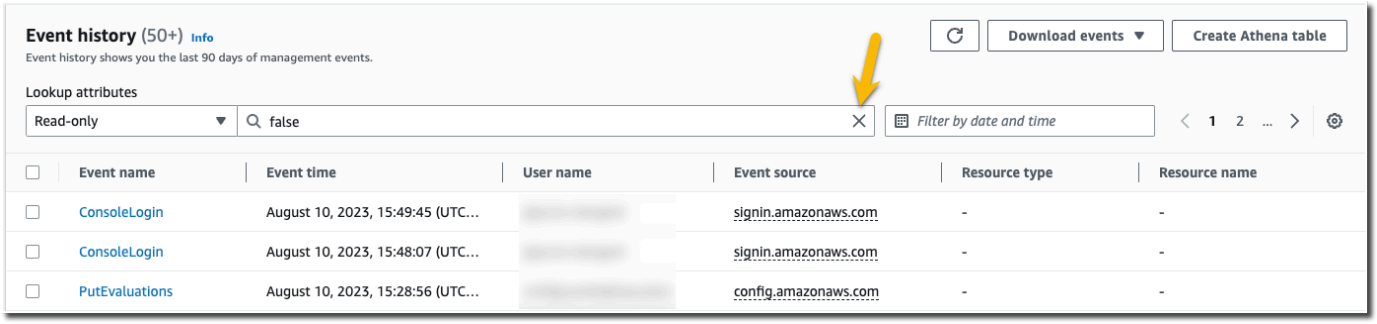
Batasan berikut berlaku untuk riwayat Acara.

- Halaman riwayat peristiwa di CloudTrail konsol hanya menampilkan peristiwa manajemen. Itu tidak menampilkan peristiwa data atau peristiwa Wawasan.
- Riwayat acara terbatas pada 90 hari terakhir peristiwa. Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, buat penyimpanan data acara atau jejak.
- 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.

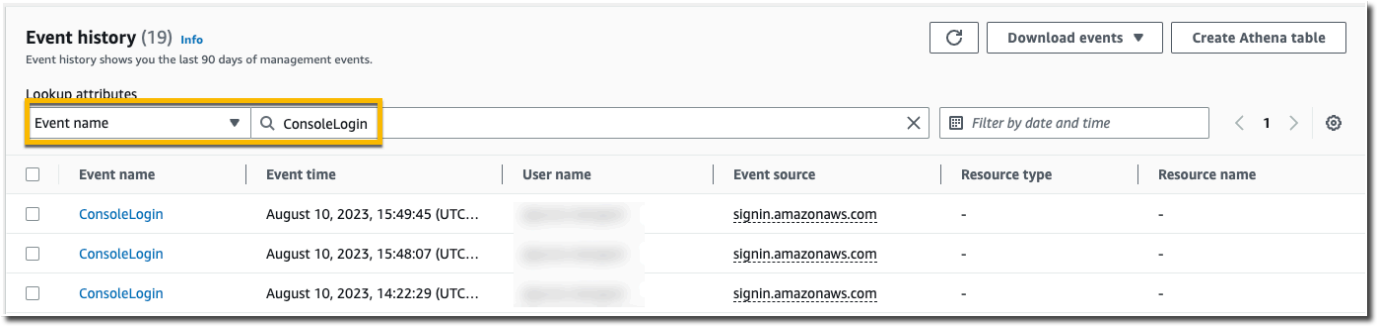
  Anda dapat membuat penyimpanan data acara CloudTrail Lake untuk kueri di beberapa atribut dan Wilayah AWS. Anda juga dapat melakukan kueri di beberapa Akun AWS dalam suatu AWS Organizations organisasi. Di CloudTrail Lake, Anda dapat menanyakan beberapa jenis peristiwa, termasuk peristiwa manajemen, peristiwa data, 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 dalam riwayat Acara, atau berjalan. `LookupEvents` Lihat informasi yang lebih lengkap di Bekerja dengan AWS CloudTrail Danau dan Buat penyimpanan data acara untuk CloudTrail acara.
- 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 melihat riwayat Acara

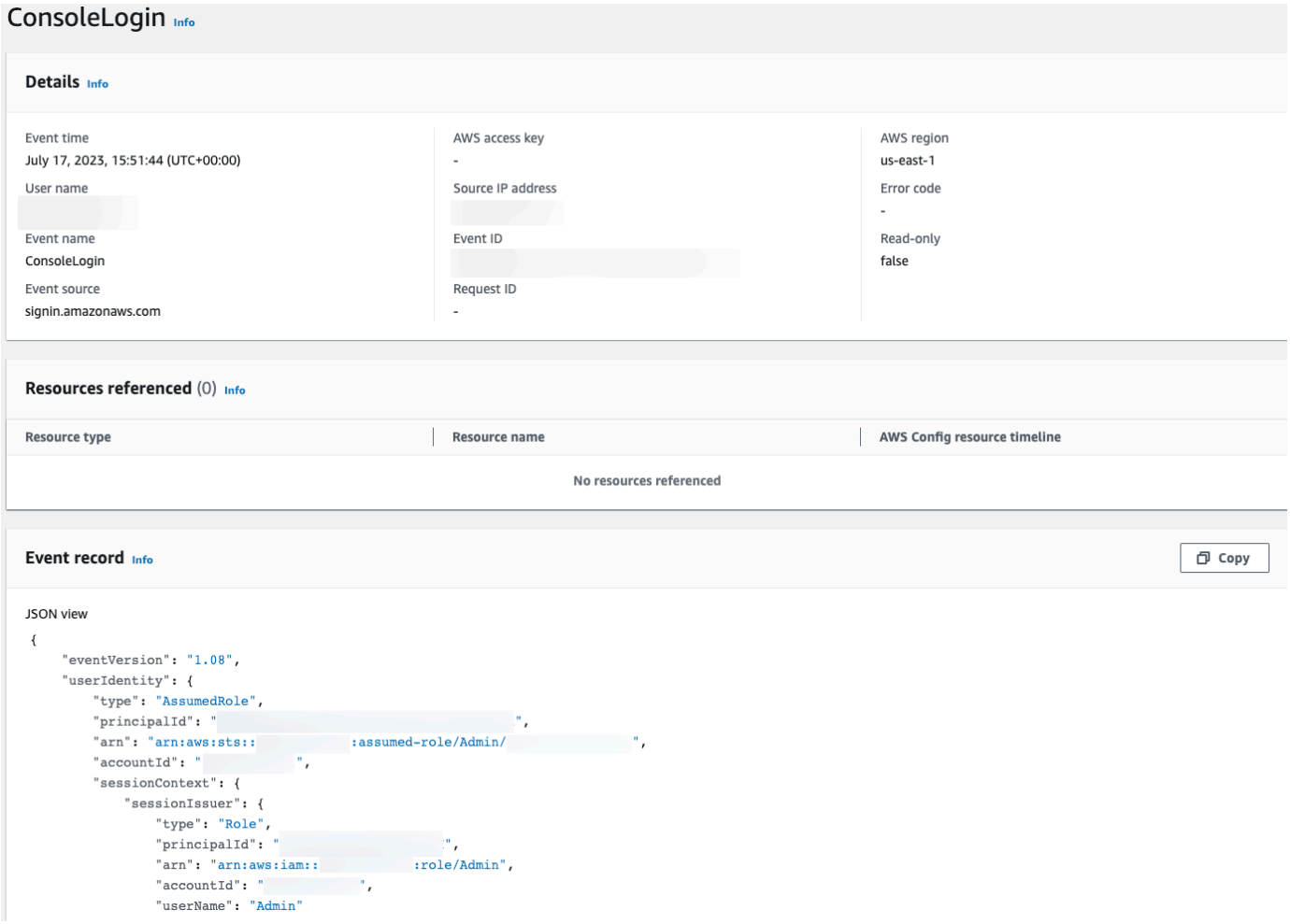
1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Pada panel navigasi, pilih Riwayat peristiwa. Anda melihat daftar acara yang difilter, dengan acara terbaru ditampilkan terlebih dahulu. Filter default untuk acara adalah Read only, disetel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



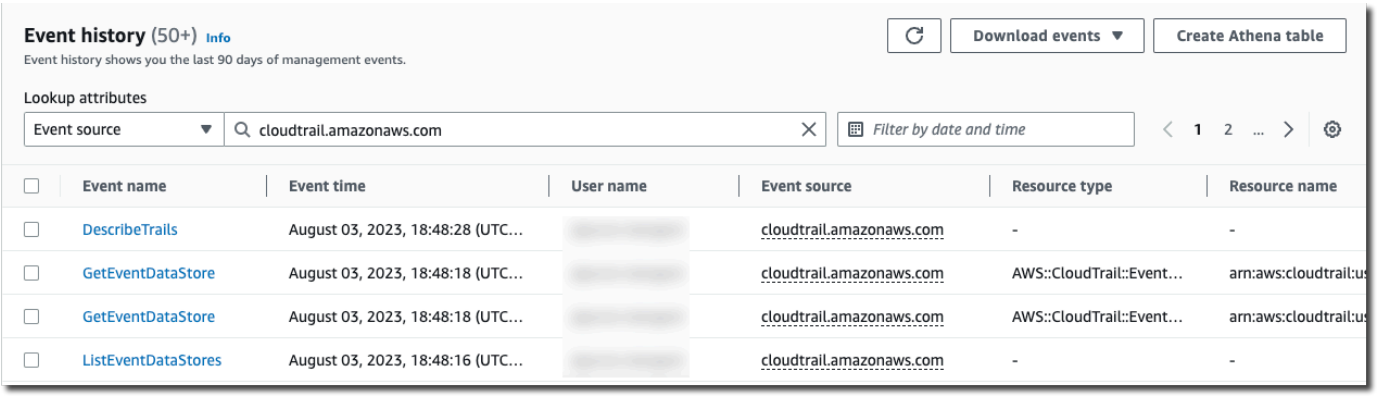
3. Banyak lagi acara ditampilkan tanpa filter default. Anda dapat memfilter acara dengan banyak cara. Misalnya, untuk melihat semua peristiwa login konsol, Anda dapat memilih filter nama acara, dan menentukan ConsoleLogin. Pilihan filter terserah Anda.



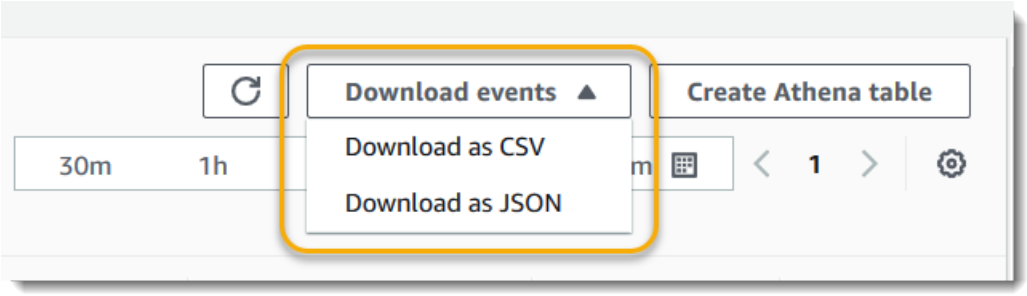
4. Untuk melihat acara manajemen tertentu, pilih nama acara. Pada halaman detail acara, Anda dapat melihat detail tentang acara, melihat sumber daya yang direferensikan, dan melihat catatan acara.



5. Untuk melihat peristiwa manajemen terbaru untuk layanan, filter pada sumber 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.

Tutorial: Buat jejak

Meskipun peristiwa yang disediakan dalam riwayat Acara di CloudTrail konsol berguna untuk meninjau aktivitas acara manajemen terbaru, mereka terbatas pada aktivitas terbaru, dan tidak mencakup semua kemungkinan peristiwa yang dapat direkam oleh CloudTrail, seperti data dan peristiwa Wawasan. Selain itu, tampilan acara Anda di konsol terbatas pada AWS Wilayah tempat Anda masuk. Untuk membuat catatan aktivitas yang sedang berlangsung di AWS akun Anda yang menangkap informasi untuk semua AWS Wilayah, Anda dapat membuat jejak. Secara default, saat Anda membuat jejak di CloudTrail konsol, jejak mencatat peristiwa Wilayah AWS di semua AWS partisi tempat Anda bekerja. Mencatat peristiwa di semua Wilayah di akun Anda adalah praktik terbaik yang disarankan.

Untuk jejak pertama Anda, sebaiknya buat jejak yang mencatat semua peristiwa manajemen di semua AWS Wilayah, dan tidak mencatat peristiwa data apa pun. Contoh peristiwa manajemen termasuk peristiwa keamanan seperti IAM `CreateUser` dan `AttachRolePolicy` acara, acara 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**
>
> Tutorial ini mengasumsikan Anda membuat jejak pertama Anda. Bergantung pada jumlah jejak yang Anda miliki di AWS akun Anda, dan bagaimana jejak tersebut dikonfigurasi, prosedur berikut mungkin atau mungkin tidak menimbulkan biaya. CloudTrail menyimpan file log di bucket Amazon S3, yang menimbulkan biaya. Untuk informasi selengkapnya tentang harga, lihat AWS CloudTrail Harga dan Harga Amazon S3.

Untuk membuat jejak

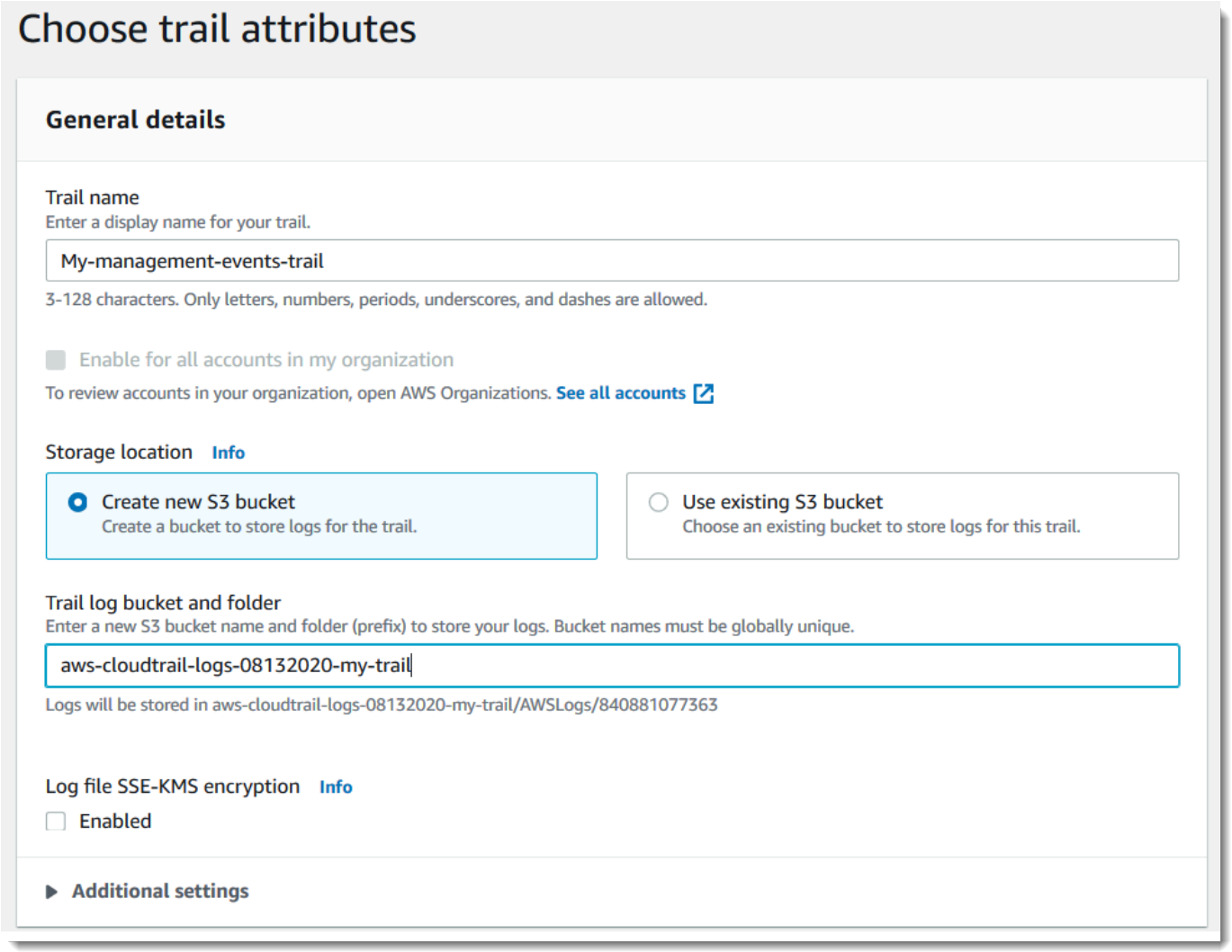
1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di pemilih Region, pilih AWS Wilayah tempat Anda ingin jejak Anda dibuat. Ini adalah daerah asal untuk jalan setapak.

   > **Note**
   >
   > Wilayah asal adalah satu-satunya AWS Wilayah di mana Anda dapat melihat dan memperbarui jejak setelah dibuat, bahkan jika jejak mencatat peristiwa di semua AWS Wilayah.

3. Pada halaman beranda CloudTrail layanan, halaman Trails, atau bagian Trails pada halaman Dasbor, pilih Buat jejak.
4. Dalam nama Trail, beri nama jejak Anda, seperti *My-Management-Events-Trail*. Sebagai praktik terbaik, gunakan nama yang dengan cepat mengidentifikasi tujuan jejak. Dalam hal ini, Anda membuat jejak yang mencatat peristiwa manajemen.
5. Tinggalkan pengaturan default untuk Aktifkan untuk semua akun di organisasi saya. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi di Organizations.
6. Untuk lokasi Storage, pilih Create new S3 bucket untuk membuat bucket. Saat Anda membuat bucket, CloudTrail membuat dan menerapkan kebijakan bucket yang diperlukan. Beri nama bucket Anda, seperti *my-bucket-for-storing-cloudtrail-logs*.

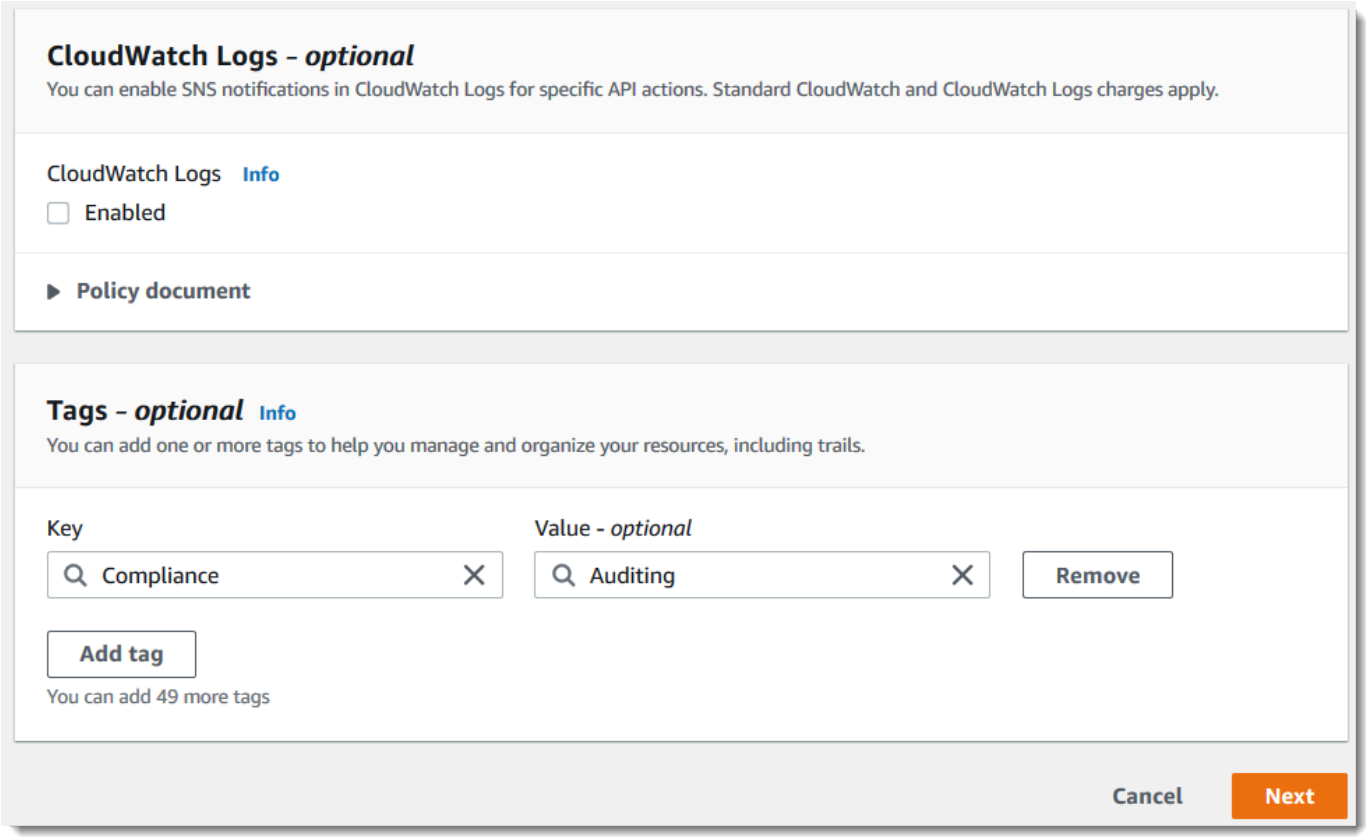
   Untuk mempermudah menemukan log Anda, buat folder baru (juga dikenal sebagai awalan) di bucket yang ada untuk menyimpan CloudTrail log Anda.

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



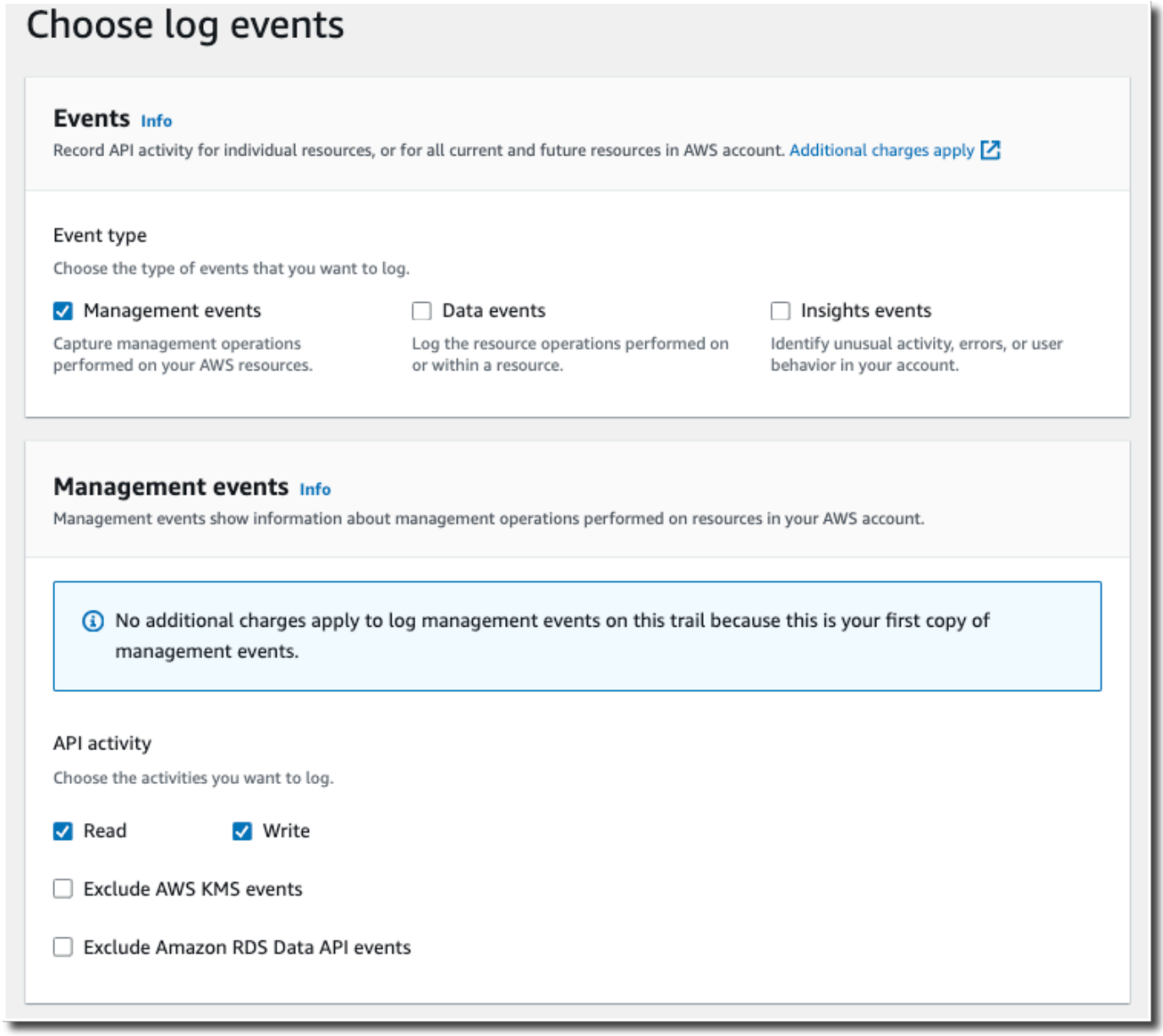
7. Kosongkan kotak centang untuk menonaktifkan Enkripsi file Log SSE-KMS. Secara default, file log Anda dienkripsi dengan enkripsi SSE-S3. Untuk informasi selengkapnya tentang setelan ini, lihat Melindungi Data Menggunakan Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3).
8. Tinggalkan 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, tambahkan satu atau beberapa tag khusus (pasangan nilai kunci) ke jejak Anda. Tag dapat membantu Anda mengidentifikasi CloudTrail jejak dan sumber daya lainnya, seperti bucket Amazon S3 yang CloudTrail berisi file log. Misalnya, Anda bisa melampirkan tag dengan nama **`Compliance`** dan nilainya**`Auditing`**.

> **Note**
>
> Meskipun Anda dapat menambahkan tag ke jejak saat 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 konsol. CloudTrail Untuk informasi selengkapnya tentang melihat dan mengubah properti bucket Amazon S3, termasuk menambahkan tag ke bucket, lihat Panduan Pengguna Amazon S3.

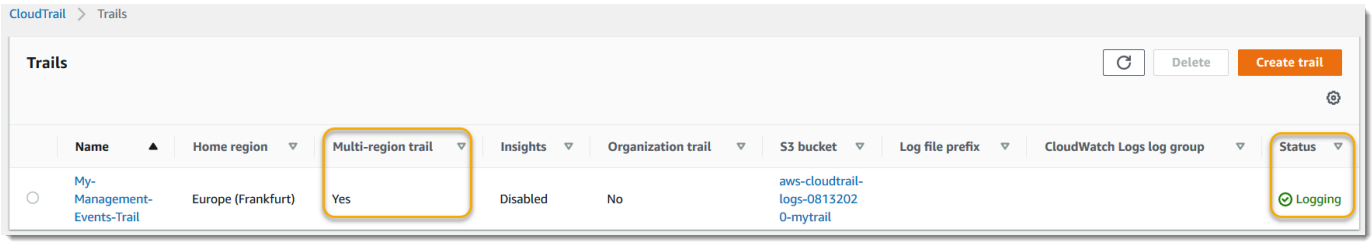


Setelah selesai membuat tag, pilih Berikutnya.

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



12. Tinggalkan setelan default untuk peristiwa Data dan peristiwa Wawasan. Jejak ini tidak akan mencatat data atau peristiwa CloudTrail Wawasan apa pun. Pilih Berikutnya.
13. Pada halaman Tinjau 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 Trails menunjukkan jejak baru Anda di tabel. Perhatikan bahwa jejak diatur ke jejak Multi-wilayah secara default, dan pencatatan diaktifkan untuk jejak secara default.



Tutorial: Lihat file log Anda

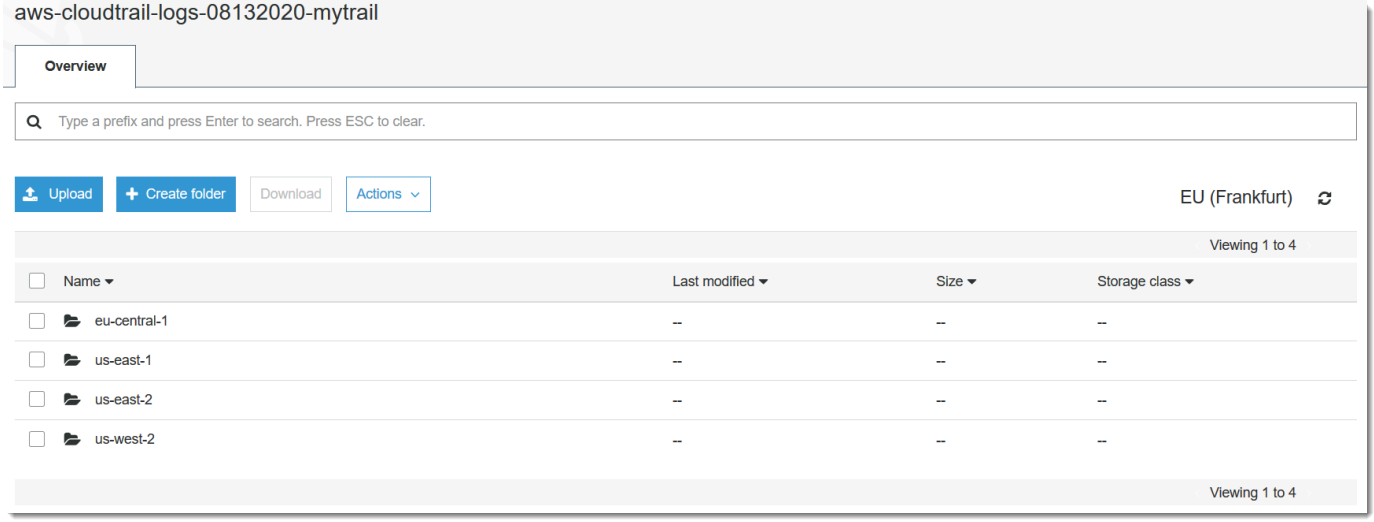
Dalam waktu rata-rata sekitar 5 menit setelah membuat jejak pertama Anda, CloudTrail kirimkan kumpulan file log pertama ke bucket Amazon S3 untuk jejak Anda. Anda dapat melihat file-file ini dan mempelajari tentang informasi yang dikandungnya.

> **Note**
>
> CloudTrail biasanya mengirimkan log dalam waktu rata-rata sekitar 5 menit dari panggilan API. Kali ini tidak dijamin. Tinjau Perjanjian 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.

Untuk melihat file log Anda

1. Masuk ke AWS Management Console 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, *My-Management-Events-Trail*).
3. Di baris untuk jejak, pilih nilai untuk bucket S3 (dalam contoh, *aws-cloudtrail-logs-08132020-mytrail*).
4. Konsol Amazon S3 terbuka dan menunjukkan bucket itu, di tingkat atas untuk file log. Karena Anda membuat jejak yang mencatat peristiwa di semua AWS Wilayah, tampilan akan terbuka pada tingkat yang menampilkan setiap folder Wilayah. *Hirarki navigasi bucket Amazon S3 pada level ini adalahAWS bucket-name/Logs/ account-id/.* CloudTrail

Pilih folder untuk AWS Wilayah tempat Anda ingin meninjau file log. Misalnya, jika Anda ingin meninjau file log untuk Wilayah AS Timur (Ohio), pilih us-east-2.



5. 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 ID AWS akun Anda, dan diakhiri dengan ekstensi `.gz`. *Misalnya, jika ID akun Anda adalah 123456789012, Anda akan melihat file dengan nama yang mirip dengan ini: 123456789012 _ _ us-east-2 _ 20190610T1255abcdeExample .json.gz. CloudTrail*

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

   Saat Anda menelusuri konten file, Anda mungkin mulai bertanya-tanya tentang apa yang Anda lihat. CloudTrail mencatat peristiwa untuk setiap AWS layanan yang mengalami aktivitas di AWS Wilayah tersebut pada saat peristiwa itu terjadi. Dengan kata lain, acara untuk AWS layanan yang berbeda dicampur bersama, hanya berdasarkan waktu. Untuk mempelajari lebih lanjut tentang AWS layanan tertentu yang digunakan untuk log CloudTrail, termasuk contoh entri file log untuk panggilan API untuk layanan tersebut, lihat daftar layanan yang didukung untuk CloudTrail, dan baca topik CloudTrail integrasi untuk layanan tersebut. Anda juga dapat mempelajari lebih lanjut tentang konten dan struktur file CloudTrail log dengan meninjau file. CloudTrail referensi acara log

   Anda mungkin juga memperhatikan apa yang tidak Anda lihat di file log di US East (Ohio). Secara khusus, Anda tidak akan melihat peristiwa masuk konsol apa pun, meskipun Anda tahu

Anda masuk ke konsol. Itu karena login konsol dan peristiwa IAM adalah peristiwa layanan global, yang biasanya dicatat di Wilayah tertentu AWS . Dalam hal ini, mereka masuk ke US East (Virginia N.), dan ditemukan di folder us-east-1. Buka folder itu, dan buka tahun, bulan, dan hari yang Anda minati. Jelajahi file log, dan Anda menemukan `ConsoleLogin` peristiwa yang terlihat mirip dengan yang berikut ini:


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "userName": "Mary_Major"
    },
    "eventTime": "2019-06-10T17:14:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.67",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101
 Firefox/60.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs
%23&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "2681fc29-EXAMPLE",
    "eventType": "AwsConsoleSignIn",
    "recipientAccountId": "123456789012"
}
```


Entri file log ini memberi tahu Anda lebih dari sekedar identitas pengguna IAM yang login (`Mary_Major`), tanggal dan waktu dia masuk, dan bahwa login berhasil. Anda juga dapat mempelajari alamat IP tempat dia masuk, sistem operasi dan perangkat lunak browser komputer yang dia gunakan, dan bahwa dia tidak menggunakan otentikasi multi-faktor.

Rencanakan langkah selanjutnya

Sekarang setelah Anda memiliki jejak, Anda memiliki akses ke catatan acara dan aktivitas yang sedang berlangsung di AWS akun Anda. Catatan yang sedang berlangsung ini membantu Anda memenuhi kebutuhan akuntansi dan audit untuk AWS akun Anda. Namun, ada banyak lagi yang dapat Anda lakukan dengan CloudTrail dan CloudTrail data.

- Tambahkan keamanan tambahan untuk data jejak Anda. CloudTrailsecara otomatis menerapkan tingkat keamanan tertentu saat Anda membuat jejak. Namun, ada langkah-langkah tambahan yang dapat Anda ambil untuk membantu menjaga keamanan data Anda.
  - Secara default, bucket Amazon S3 yang Anda buat sebagai bagian dari pembuatan jejak memiliki kebijakan yang diterapkan yang memungkinkan CloudTrail untuk menulis file log ke bucket tersebut. Bucket tidak dapat diakses publik, tetapi mungkin dapat diakses oleh pengguna lain di AWS akun Anda jika mereka memiliki izin untuk membaca dan menulis ke bucket di akun Anda. AWS Tinjau kebijakan untuk bucket Anda dan jika perlu, buat perubahan untuk membatasi akses. Untuk informasi selengkapnya, lihat dokumentasi keamanan Amazon S3 dan contoh panduan untuk mengamankan bucket.
  - File log yang dikirimkan CloudTrail ke bucket Anda dienkripsi oleh enkripsi sisi server Amazon dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). Untuk menyediakan lapisan keamanan yang dapat dikelola secara langsung, Anda dapat menggunakan enkripsi sisi server dengan AWS KMS—managed keys (SSE-KMS) untuk file log Anda. CloudTrail Untuk menggunakan SSE-KMS dengan CloudTrail, Anda membuat dan mengelola kunci KMS, juga dikenal sebagai kunci. AWS KMS key Untuk informasi selengkapnya, lihat Mengenkripsi file CloudTrail log dengan AWS KMS kunci (SSE-KMS).
  - Untuk perencanaan keamanan tambahan, tinjau praktik terbaik keamanan untuk CloudTrail.
- Buat jejak untuk mencatat peristiwa data. Jika Anda tertarik untuk mencatat saat objek ditambahkan, diambil, dan dihapus dalam satu atau beberapa bucket Amazon S3, saat item ditambahkan, diubah, atau dihapus di tabel DynamoDB, atau ketika satu atau AWS Lambda beberapa fungsi dipanggil, ini adalah peristiwa data. Jejak acara manajemen yang Anda buat sebelumnya dalam tutorial ini tidak mencatat jenis peristiwa ini. Anda dapat membuat jejak terpisah khusus untuk mencatat peristiwa data untuk beberapa atau semua jenis sumber daya yang didukung. Untuk informasi selengkapnya, lihat Peristiwa data.

> **Note**
>
> Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, silakan lihat Harga AWS CloudTrail.

- Log acara CloudTrail Insights di jejak Anda. AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen. CloudTrail Insights menggunakan model matematika untuk menentukan tingkat normal aktivitas API dan peristiwa layanan untuk akun. Ini mengidentifikasi perilaku yang berada di luar pola normal, menghasilkan peristiwa Insights, dan mengirimkan peristiwa tersebut ke `/CloudTrail-Insight` folder di bucket S3 tujuan yang dipilih untuk jejak Anda. Untuk informasi selengkapnya tentang CloudTrail Wawasan, lihatAcara Logging Insights.

> **Note**
>
> Biaya tambahan berlaku untuk acara logging Insights. Untuk informasi selengkapnya, silakan lihat Harga AWS CloudTrail.

- Siapkan alarm CloudWatch Log untuk mengingatkan Anda ketika peristiwa tertentu terjadi. CloudWatch Log memungkinkan Anda memantau dan menerima peringatan untuk peristiwa tertentu yang ditangkap oleh CloudTrail. Misalnya, Anda dapat memantau keamanan kunci dan peristiwa manajemen terkait jaringan, seperti perubahan grup keamanan, peristiwa AWS Management Console login gagal, atau perubahan kebijakan IAM. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.
- Gunakan alat analisis untuk mengidentifikasi tren di CloudTrail log Anda. Meskipun filter dalam riwayat Acara dapat membantu Anda menemukan peristiwa atau jenis acara tertentu dalam aktivitas terbaru Anda, filter tersebut tidak memberikan kemampuan untuk menelusuri aktivitas dalam jangka waktu yang lebih lama. Untuk analisis yang lebih dalam dan lebih canggih, Anda dapat menggunakan Amazon Athena. Untuk informasi selengkapnya, lihat Meminta AWS CloudTrail Log di Panduan Pengguna Amazon Athena.

Tutorial untuk CloudTrail Danau

Meskipun Anda dapat mencari peristiwa dalam riwayat Acara, Anda terbatas pada satu peristiwa Akun AWS, hanya dapat mengembalikan peristiwa dari satu Wilayah AWS, dan tidak dapat

menanyakan beberapa atribut. Sebaliknya, dengan membuat penyimpanan data acara CloudTrail Lake, Anda dapat menjalankan kueri SQL yang kompleks di beberapa bidang acara dan Anda juga dapat menanyakan peristiwa di beberapa Wilayah AWS dan. Akun AWSAnda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika Anda memilih opsi harga retensi yang dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun. Anda dapat membuat penyimpanan data acara untuk mengumpulkan peristiwa CloudTrail manajemen dan data, item AWS Config konfigurasi, AWS Audit Manager bukti, atau AWS non-peristiwa. Anda dapat membuat penyimpanan data acara menggunakan konsol, the AWS CLI, atau CloudTrail API.

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.

Tutorial berikut menunjukkan cara melakukan tugas-tugas CloudTrail Lake umum di konsol. Untuk informasi lebih lanjut tentang CloudTrail Danau, lihatBekerja dengan AWS CloudTrail Danau.

Topik

- Tutorial: Membuat penyimpanan data acara untuk acara manajemen
- Tutorial: Membuat penyimpanan data acara untuk acara data S3
- Tutorial: Salin acara jejak ke CloudTrail Danau
- Tutorial: Lihat dasbor Danau
- Tutorial: Lihat dan jalankan contoh kueri
- Tutorial: Simpan hasil kueri ke bucket Amazon S3

Tutorial: Membuat penyimpanan data acara untuk acara manajemen

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 AWS non-peristiwa.

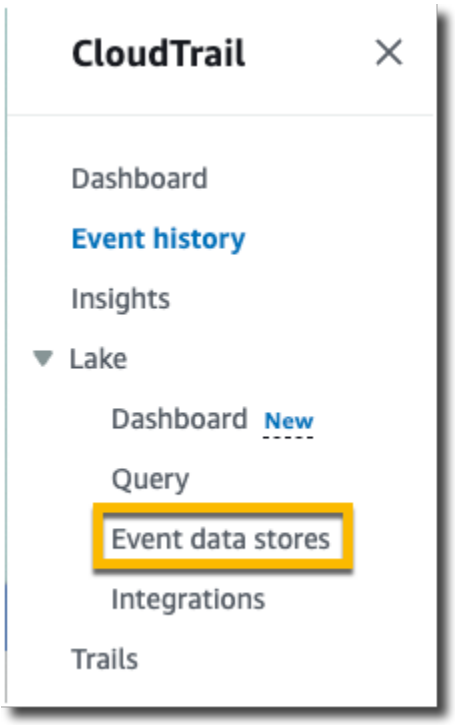
Tutorial ini menunjukkan cara membuat penyimpanan data acara yang mencatat semua peristiwa manajemen di semua AWS Wilayah, dan tidak mencatat peristiwa data apa pun. Contoh peristiwa

manajemen termasuk peristiwa keamanan seperti IAM `CreateUser` dan `AttachRolePolicy` acara, acara sumber daya seperti `RunInstances` dan`CreateBucket`, dan banyak lagi.

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.

Untuk membuat penyimpanan data acara untuk acara manajemen

1. Masuk ke AWS Management Console 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.

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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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
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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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.
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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko data acara.

Untuk mengaktifkan federasi kueri Lake, pilih Aktifkan dan lakukan hal berikut:

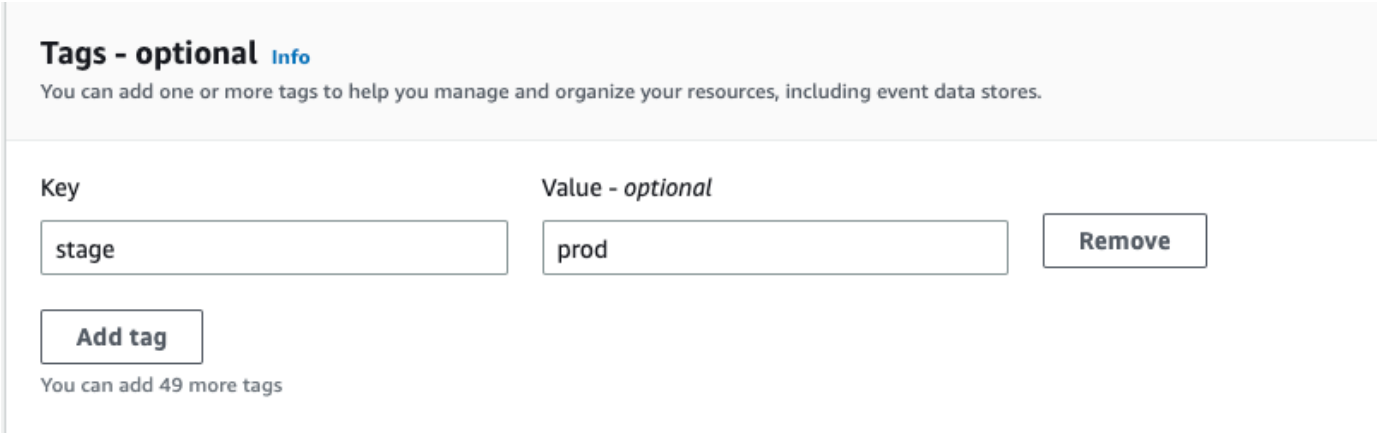
a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data acara federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin 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.

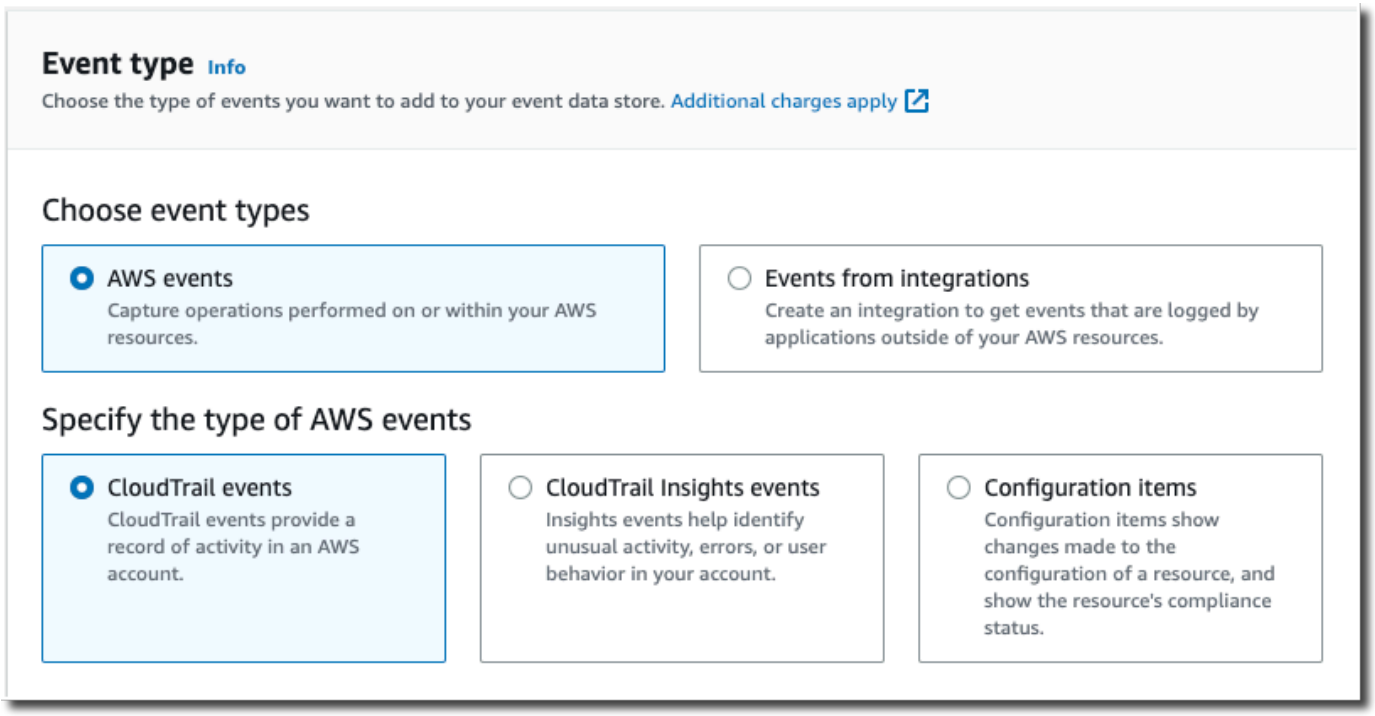
c. Jika Anda menggunakan peran yang ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) 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.

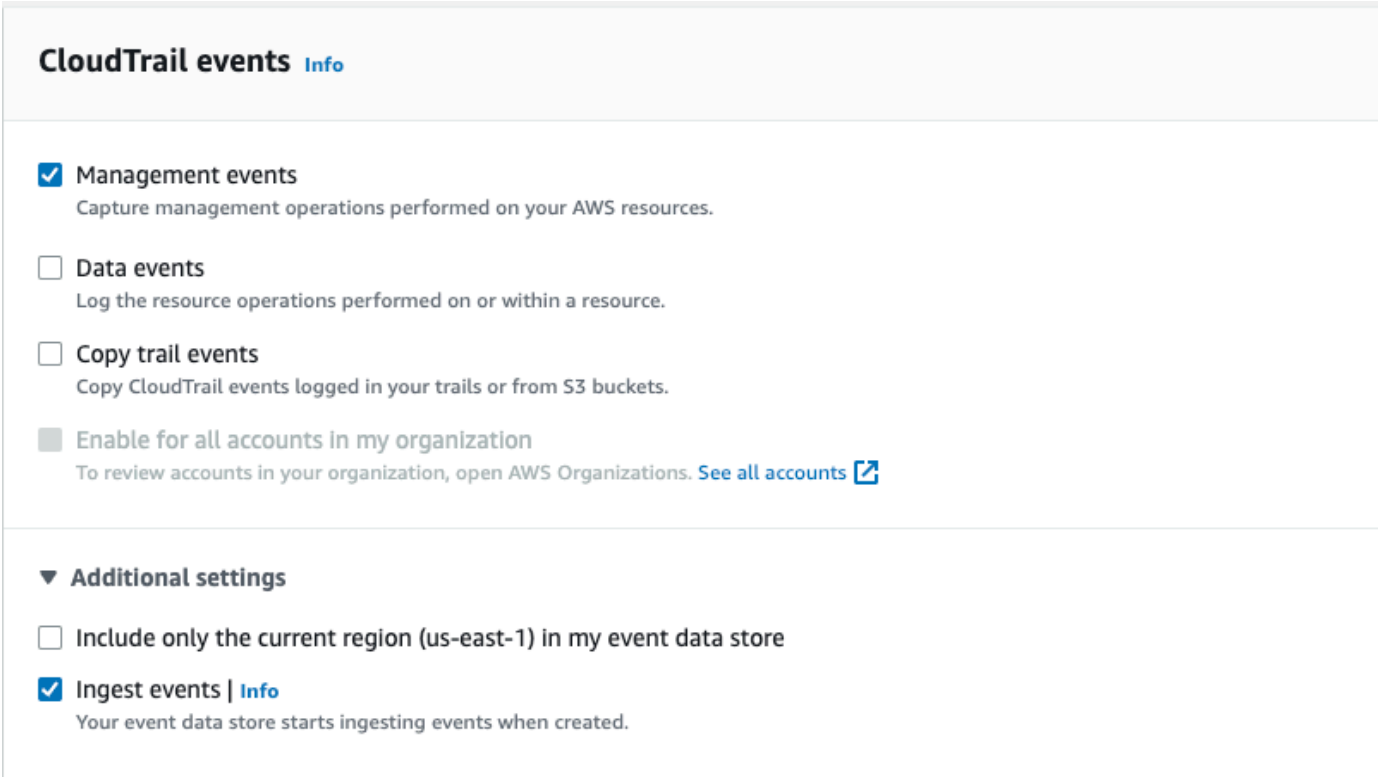
   Untuk informasi tentang cara menggunakan tag untuk melacak biaya, lihatMembuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake. Untuk informasi tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat.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



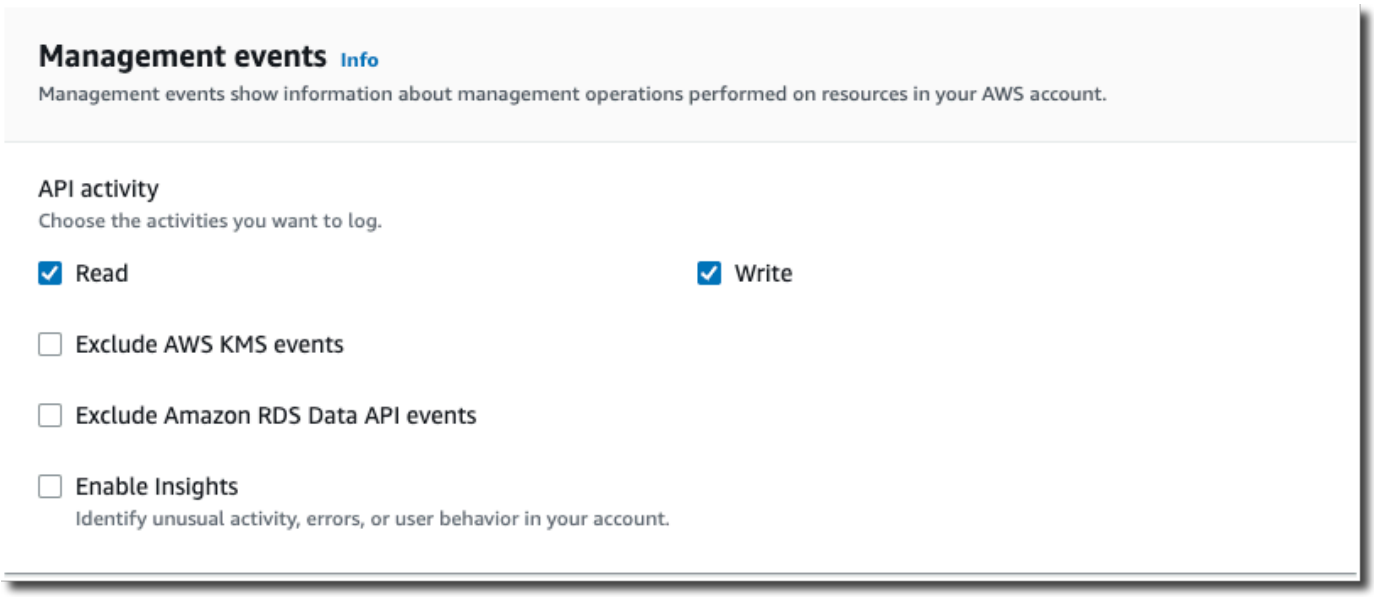
10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
11. Pada halaman Pilih acara, tinggalkan pilihan default untuk jenis Acara.



12. Untuk CloudTrail acara, tinggalkan pilihan default. Secara default, penyimpanan data CloudTrail acara mengumpulkan peristiwa manajemen dan tidak mengumpulkan peristiwa data. Untuk informasi selengkapnya tentang acara manajemen, lihatAcara manajemen logging. Untuk informasi selengkapnya tentang peristiwa data, lihatPencatatan peristiwa data.

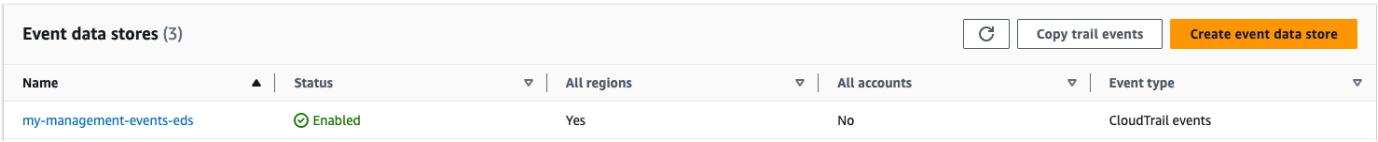


13. Tinggalkan pengaturan default untuk acara Copy trail. Anda akan menggunakan opsi ini untuk menyalin peristiwa jejak yang ada ke penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat Salin peristiwa jejak ke penyimpanan data acara.
14. Tinggalkan pengaturan default untuk Aktifkan untuk semua akun di organisasi saya. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi AWS Organizations.
15. Untuk Pengaturan tambahan tinggalkan pilihan default. Secara default, penyimpanan data acara mengumpulkan peristiwa untuk semua Wilayah AWS dan mulai menelan peristiwa saat dibuat.
16. Untuk acara Manajemen, pilih untuk mengumpulkan acara Baca dan Tulis. Biarkan kotak centang untuk Kecualikan AWS KMS peristiwa dan Kecualikan peristiwa Amazon RDS Data API kosong, untuk mengumpulkan semua peristiwa manajemen. Biarkan kotak centang untuk Aktifkan peristiwa Insights kosong.



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

    Mulai saat ini, penyimpanan data acara menangkap peristiwa yang cocok dengan pemilih acara lanjutannya. Peristiwa yang terjadi sebelum Anda membuat penyimpanan data acara tidak ada di penyimpanan data acara, kecuali Anda memilih untuk menyalin peristiwa jejak yang ada.



Anda sekarang siap untuk menjalankan kueri di toko data acara Anda. Untuk informasi tentang cara melihat dan menjalankan contoh kueri, lihatTutorial: Lihat dan jalankan contoh kueri.

Tutorial: Membuat penyimpanan data acara untuk acara data S3

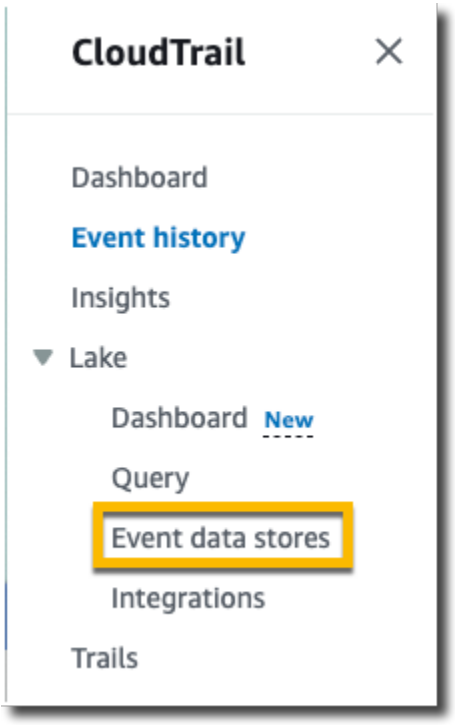
Saat Anda membuat penyimpanan data peristiwa untuk peristiwa data, Anda memilih Layanan AWS dan jenis sumber daya yang ingin Anda log peristiwa data. Untuk informasi tentang Layanan AWS peristiwa data log tersebut, lihatPeristiwa data.

Tutorial ini menunjukkan cara membuat penyimpanan data acara untuk peristiwa 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.

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.

Untuk membuat penyimpanan data acara untuk peristiwa data S3

1. Masuk ke AWS Management Console 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 *s3- data-events-eds*. Sebagai praktik terbaik, gunakan nama yang dengan cepat mengidentifikasi tujuan penyimpanan data acara. Untuk informasi tentang persyaratan CloudTrail penamaan, lihatPersyaratan penamaan.

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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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
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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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.
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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko data acara.

Untuk mengaktifkan federasi kueri Lake, pilih Aktifkan dan lakukan hal berikut:

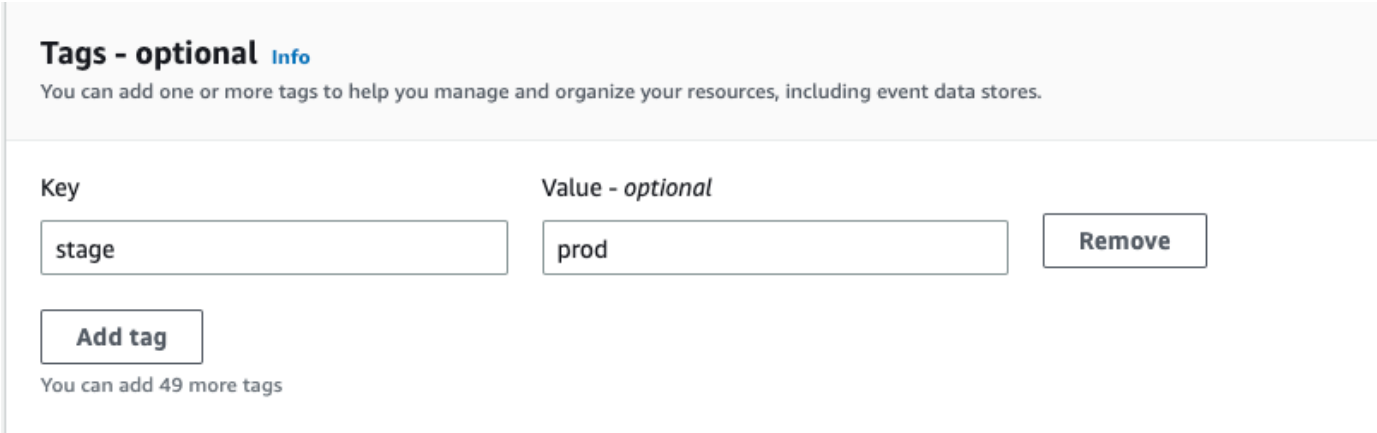
a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data acara federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin 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.

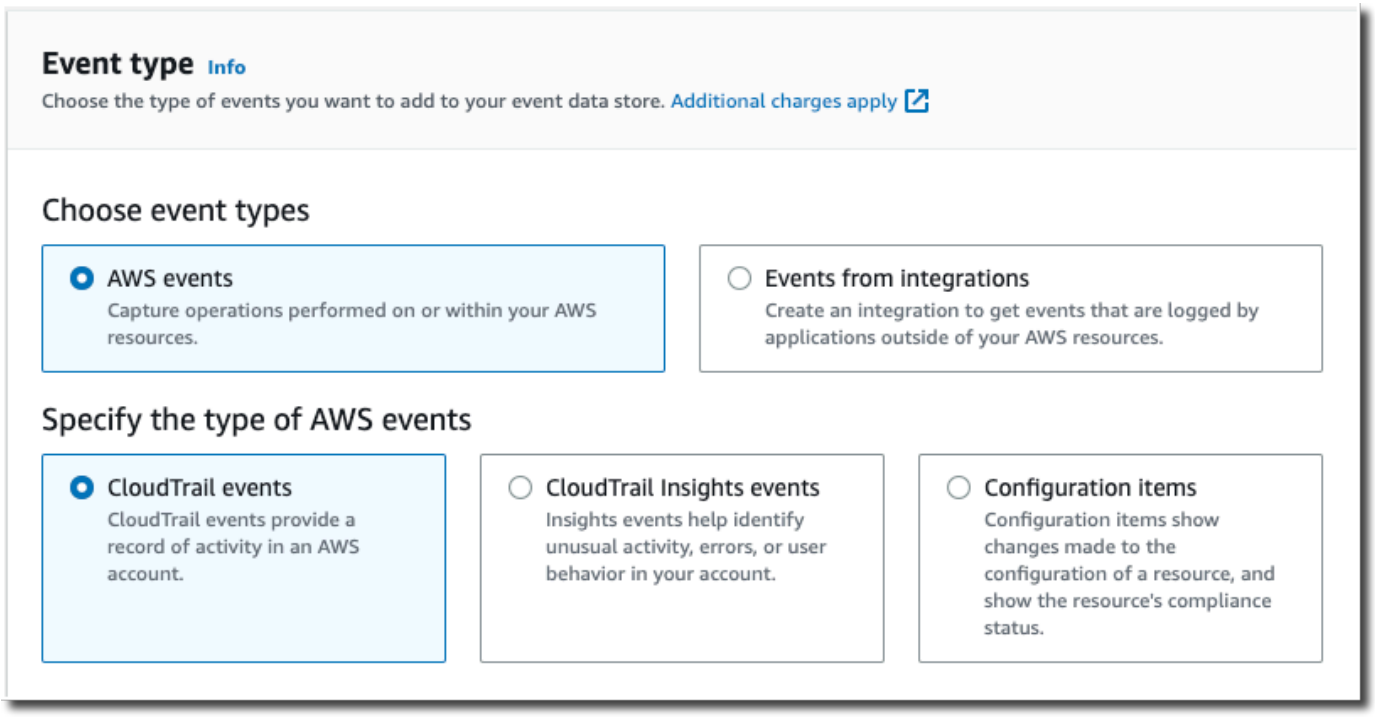
c. Jika Anda menggunakan peran yang ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) 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.

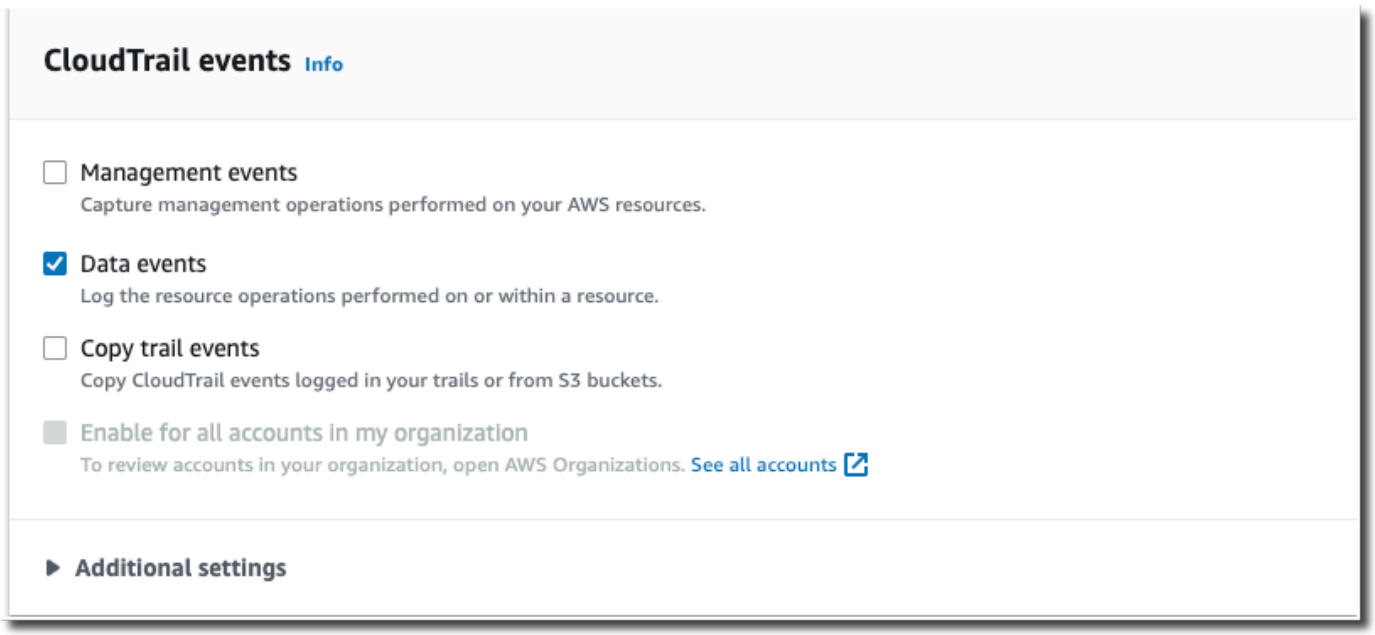
   Untuk informasi tentang cara menggunakan tag untuk melacak biaya, lihatMembuat tag alokasi biaya yang ditentukan pengguna untuk penyimpanan data acara CloudTrail Lake. Untuk informasi tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat.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



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



12. Untuk CloudTrail acara, pilih Peristiwa data dan batalkan pilihan Acara manajemen. Untuk informasi selengkapnya tentang peristiwa data, lihatPencatatan peristiwa data.



13. Tinggalkan pengaturan default untuk acara Copy trail. 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 acara.

14. Tinggalkan pengaturan default untuk Aktifkan untuk semua akun di organisasi saya. Opsi ini tidak akan tersedia untuk diubah kecuali Anda memiliki akun yang dikonfigurasi AWS Organizations.
15. Untuk Pengaturan tambahan tinggalkan pilihan default. Secara default, penyimpanan data acara mengumpulkan peristiwa untuk semua Wilayah AWS dan mulai menelan peristiwa saat dibuat.
16. Untuk peristiwa Data, buat pilihan berikut:

    a. Dalam tipe peristiwa Data, pilih S3. Jenis peristiwa data mengidentifikasi Layanan AWS dan sumber daya di mana peristiwa data dicatat.

    b. Di template pemilih Log, pilih Kustom. Memilih Kustom memungkinkan Anda menentukan pemilih acara khusus untuk memfilter pada`eventName`,`resources.ARN`, dan `readOnly` bidang. Untuk informasi tentang bidang ini, lihat AdvancedFieldSelectordi Referensi AWS CloudTrail API.

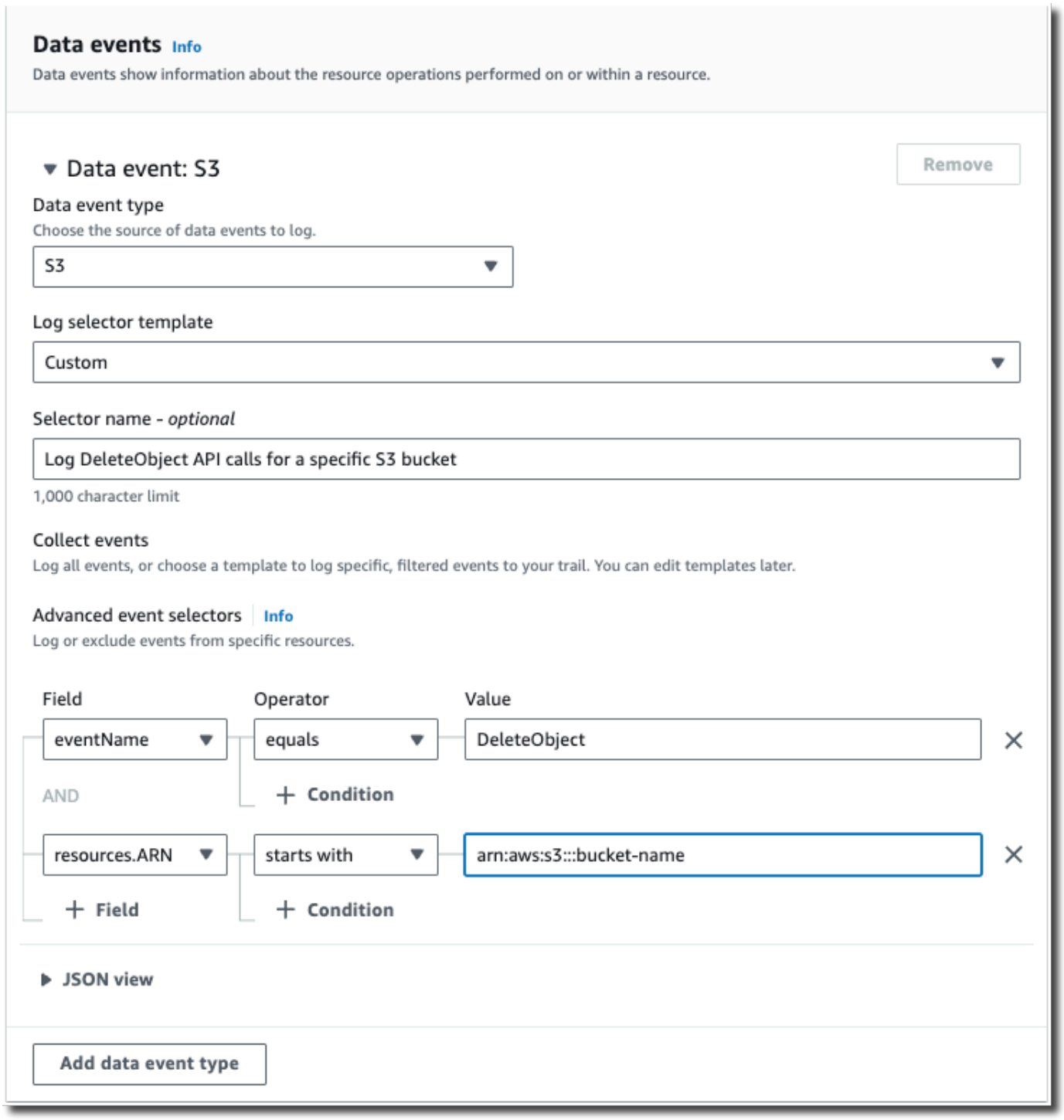
    c. (Opsional) Dalam nama Selector, masukkan nama untuk mengidentifikasi pemilih Anda. Nama pemilih adalah nama deskriptif untuk pemilih peristiwa lanjutan, seperti “Log DeleteObject API panggilan untuk bucket S3 tertentu”. Nama pemilih terdaftar seperti **`Name`** pada pemilih acara lanjutan dan dapat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

    d. Di Advanced event selectors, kami akan membangun pemilih acara khusus untuk memfilter pada `eventName` dan `resources.ARN` bidang. Penyeleksi acara lanjutan untuk penyimpanan data acara bekerja sama dengan pemilih acara tingkat lanjut yang Anda

terapkan ke jejak. Untuk informasi selengkapnya tentang cara membuat penyeleksi peristiwa tingkat lanjut, lihat Mencatat peristiwa data dengan pemilih peristiwa lanjutan.

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

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



17. Pilih Berikutnya untuk meninjau pilihan Anda.
18. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.

19. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.

    Mulai saat ini, penyimpanan data acara menangkap peristiwa yang cocok dengan pemilih acara lanjutannya. Peristiwa yang terjadi sebelum Anda membuat penyimpanan data acara tidak ada di penyimpanan data acara, kecuali Anda memilih untuk menyalin peristiwa jejak yang ada.

Anda sekarang siap untuk menjalankan kueri di toko data acara Anda. Untuk informasi tentang cara melihat dan menjalankan contoh kueri, lihatTutorial: Lihat dan jalankan contoh kueri.

Tutorial: Salin acara jejak ke CloudTrail Danau

Tutorial ini menunjukkan cara menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake baru untuk analisis historis. Untuk informasi selengkapnya tentang menyalin peristiwa jejak, lihatSalin peristiwa jejak ke penyimpanan data acara.

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.

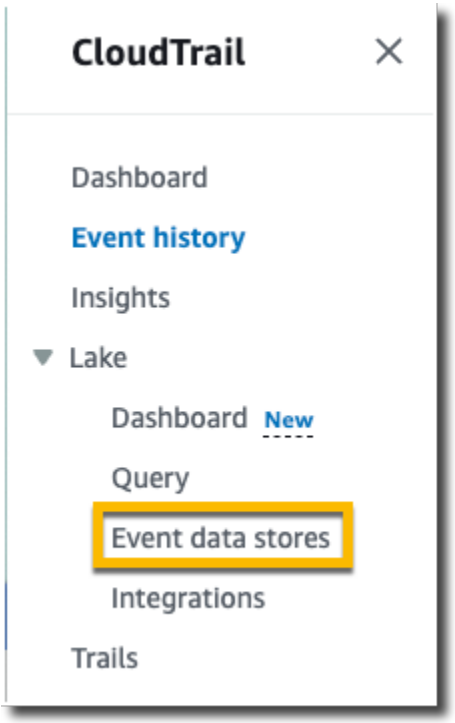
Saat Anda menyalin peristiwa jejak ke penyimpanan data acara CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data tidak terkompresi yang dikonsumsi oleh penyimpanan data acara.

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.

Untuk menyalin peristiwa jejak ke penyimpanan data acara baru

1. Masuk ke AWS Management Console 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.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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

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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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.
   > Kami menyarankan bahwa ketika Anda memilih periode retensi, Anda mempertimbangkan usia acara yang ingin Anda salin serta berapa lama Anda ingin menyimpan peristiwa yang disalin di penyimpanan data acara Anda. Misalnya, jika Anda menyalin peristiwa jejak yang berusia 5 tahun dan menentukan periode retensi 7 tahun, penyimpanan data acara akan menyimpan acara tersebut selama dua tahun.

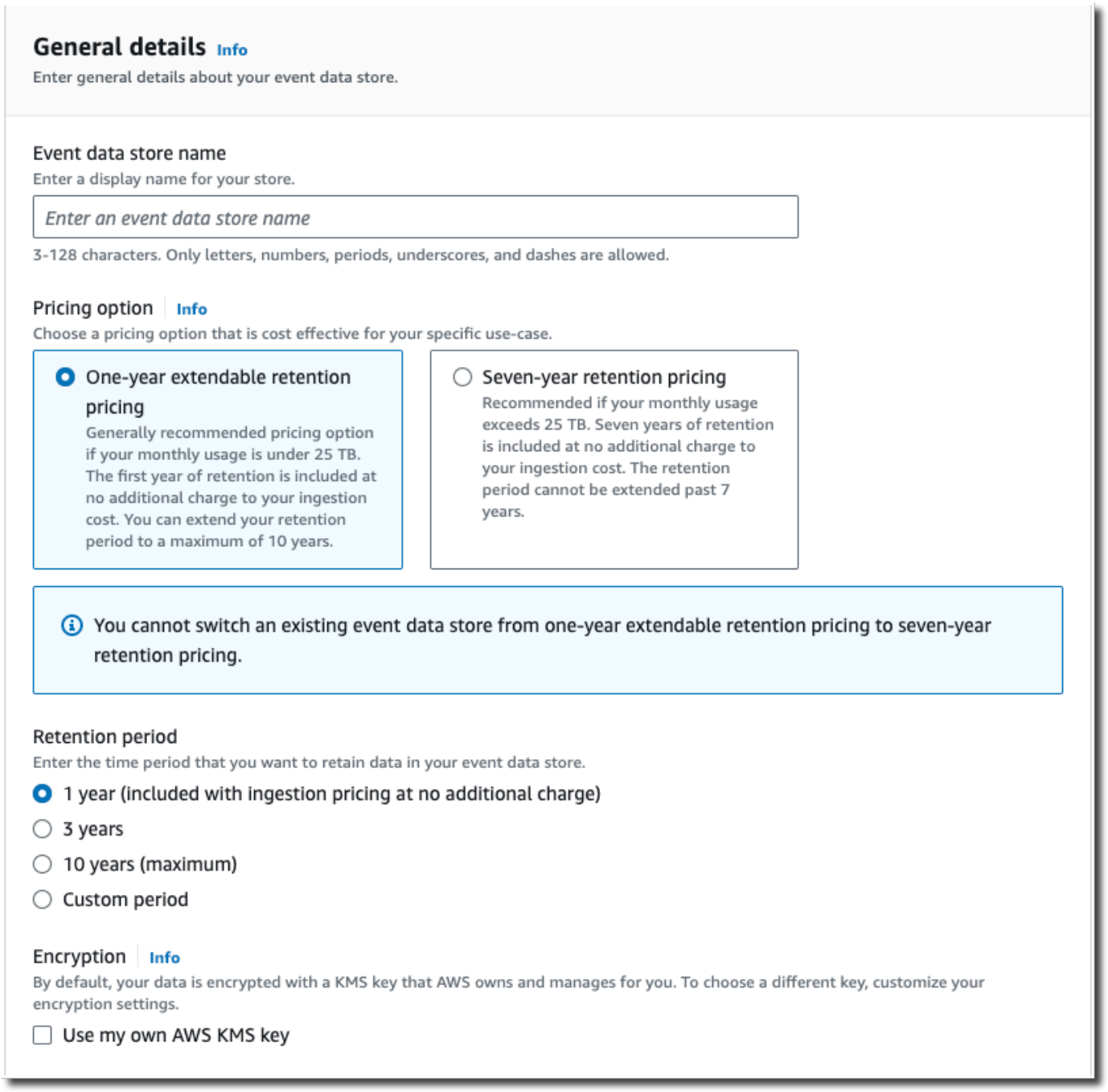
7. (Opsional) Dalam Enkripsi. pilih apakah Anda ingin mengenkripsi penyimpanan data acara menggunakan kunci KMS Anda sendiri. Secara default, semua peristiwa di penyimpanan data acara dienkripsi dengan CloudTrail menggunakan kunci KMS yang AWS memiliki dan mengelola untuk Anda.

   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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko data acara.

Untuk mengaktifkan federasi kueri Lake, pilih Aktifkan dan lakukan hal berikut:

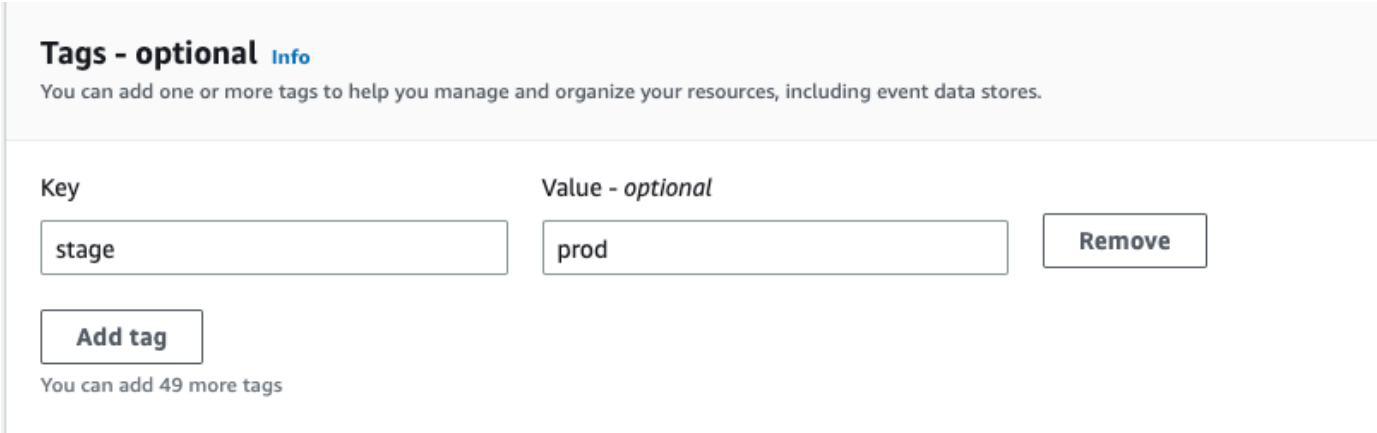
a. Pilih apakah Anda ingin membuat peran baru atau menggunakan peran IAM yang sudah ada. AWS Lake Formationmenggunakan peran ini untuk mengelola izin untuk penyimpanan data acara federasi. Saat Anda membuat peran baru menggunakan CloudTrail konsol, CloudTrail secara otomatis membuat peran dengan izin 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.

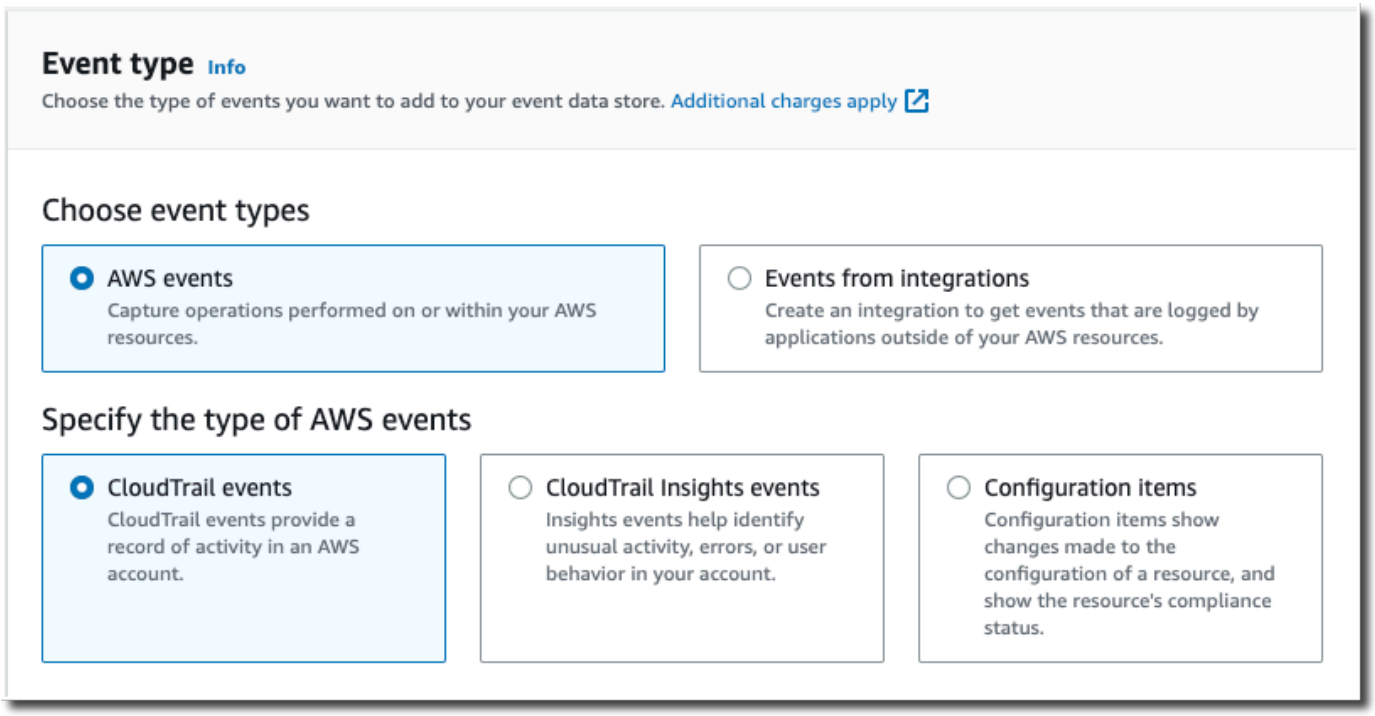
c. Jika Anda menggunakan peran yang ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

9. (Opsional) 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 di. Referensi Umum AWS

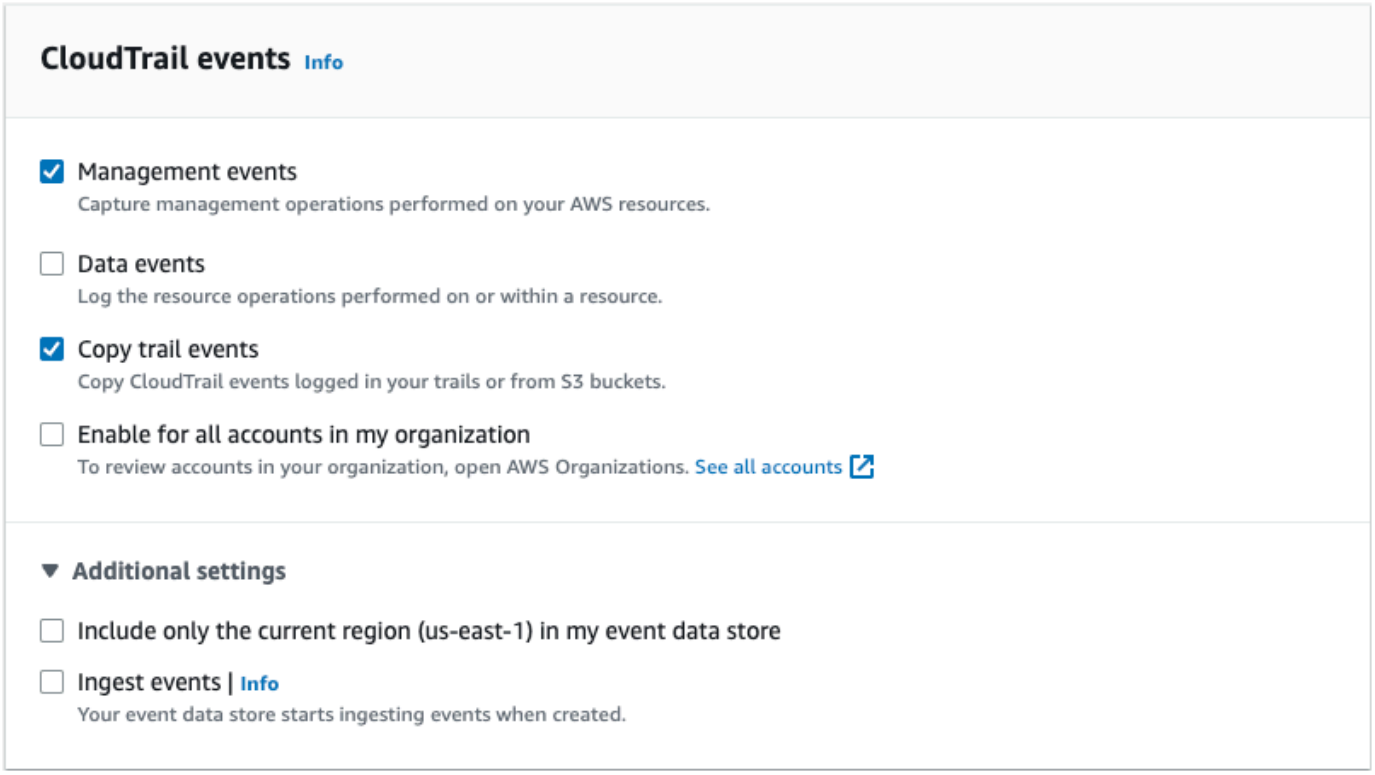


10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
11. Pada halaman Pilih acara, tinggalkan pilihan default untuk jenis Acara.



12. 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.

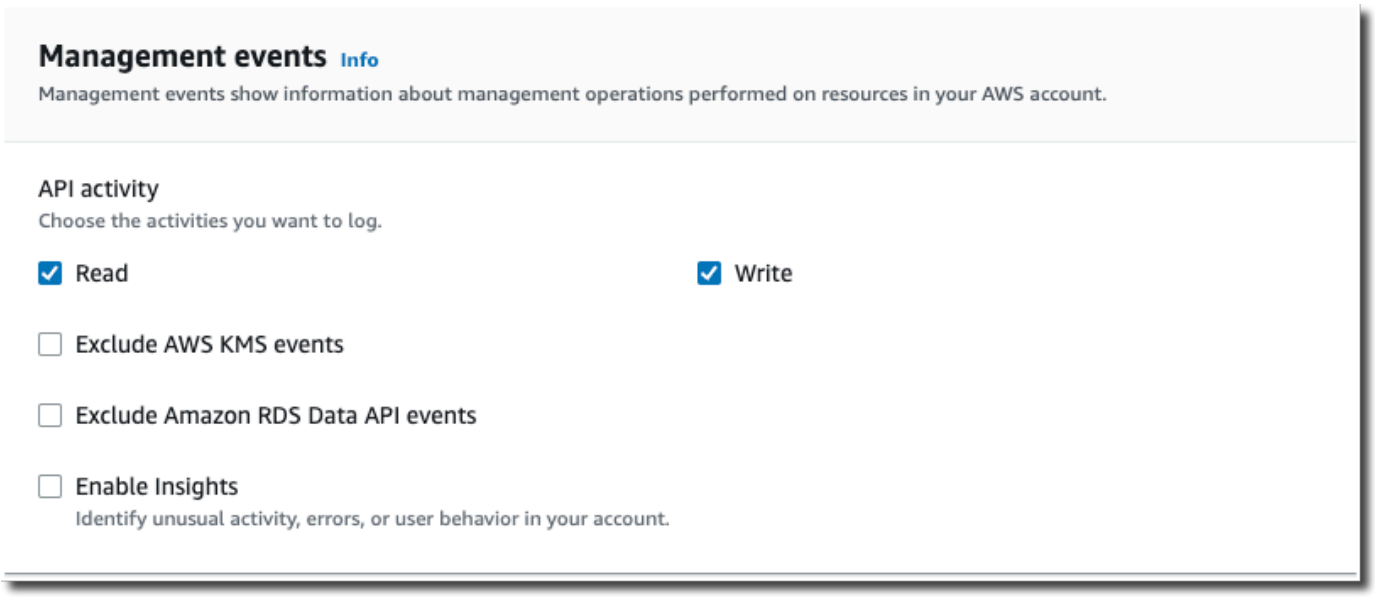
    Jika Anda membuat penyimpanan data acara untuk menggantikan jejak yang ada, pilih pemilih acara yang sama dengan jejak Anda untuk memastikan penyimpanan data acara memiliki cakupan acara yang sama.



13. 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.

14. Untuk pengaturan Tambahan, kami akan membatalkan pilihan acara Ingest, karena dalam contoh ini kami tidak ingin penyimpanan data acara menelan 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.
15. Untuk acara Manajemen, kami akan meninggalkan pengaturan default.



16. 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`*.

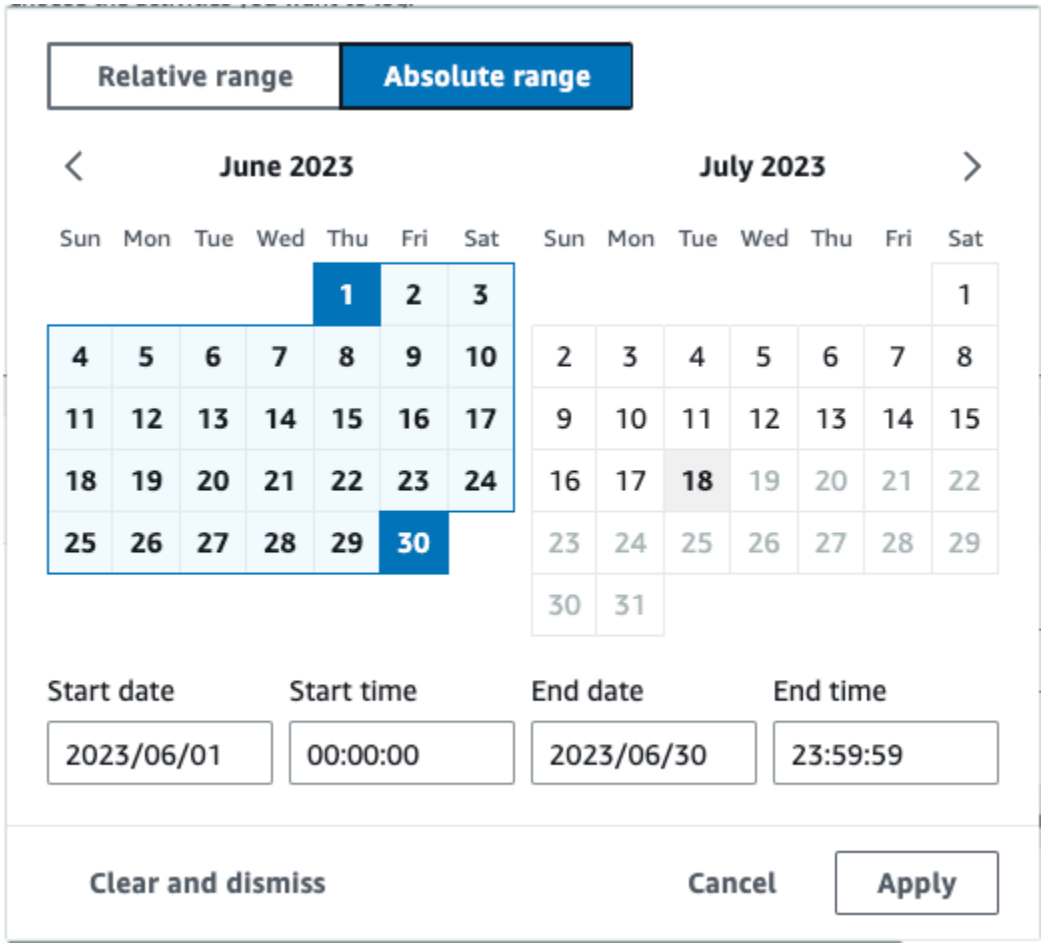
       Secara default, CloudTrail hanya menyalin CloudTrail peristiwa yang terdapat dalam awalan bucket S3 dan `CloudTrail` awalan di dalam awalan, dan tidak memeriksa `CloudTrail` awalan untuk layanan lain. AWS Jika Anda ingin menyalin CloudTrail peristiwa yang terdapat dalam awalan lain, pilih Masukkan URI 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 Juni.

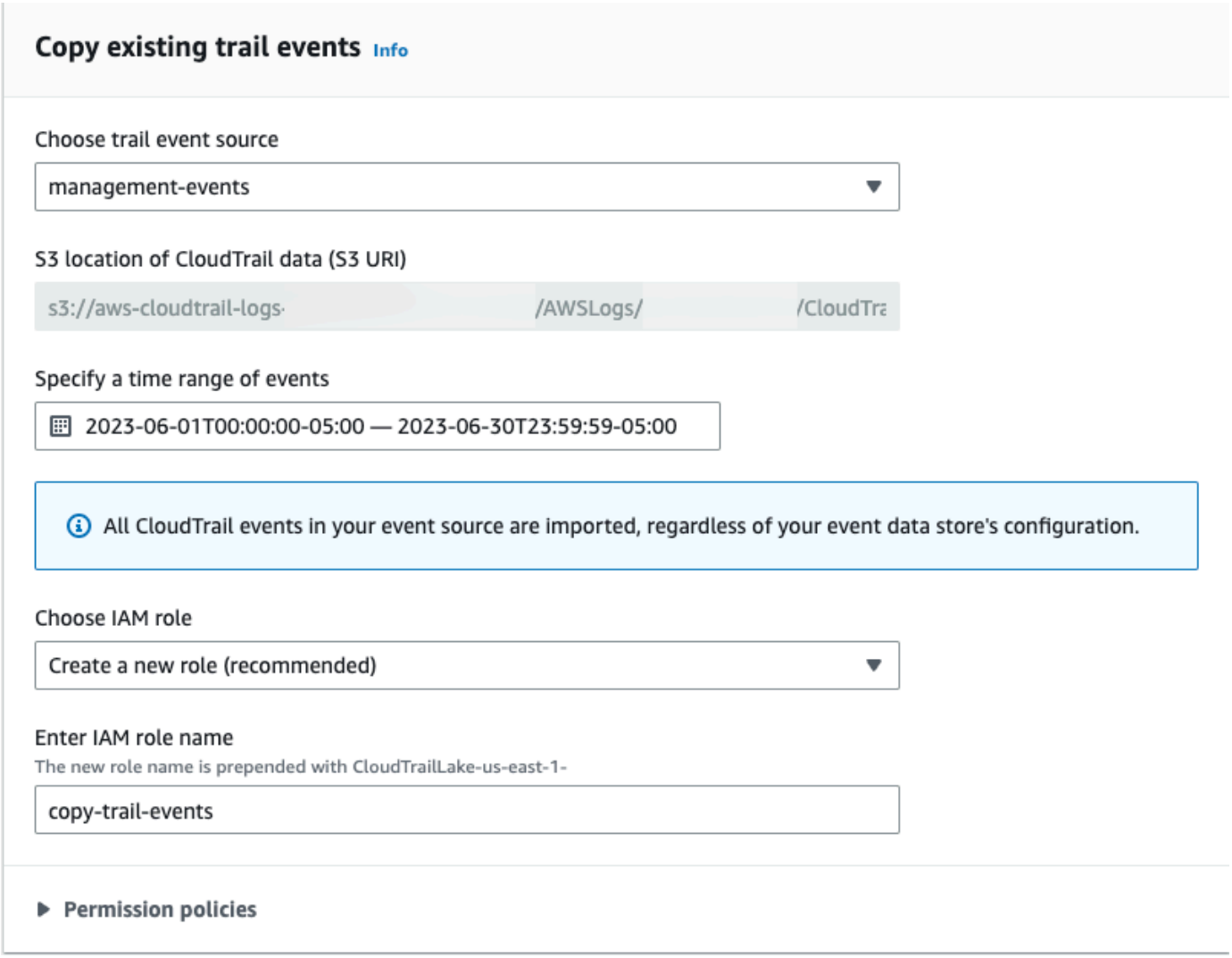


c. Untuk Izin, pilih dari opsi peran IAM berikut. Jika Anda memilih peran IAM yang ada, verifikasi bahwa kebijakan peran IAM menyediakan izin yang diperlukan. Untuk informasi selengkapnya tentang memperbarui izin peran IAM, lihat. Izin IAM untuk menyalin peristiwa jejak

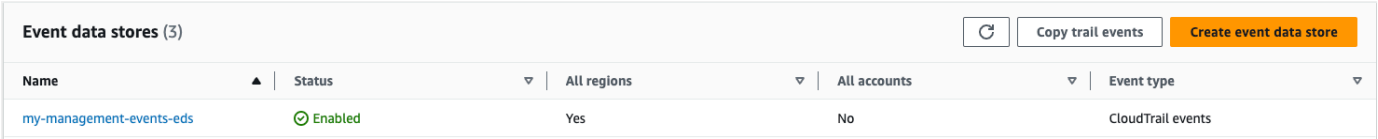
- Pilih Buat peran baru (disarankan) untuk membuat peran IAM baru. Untuk Masukkan nama peran IAM, masukkan nama untuk peran tersebut. CloudTrail secara otomatis membuat izin yang diperlukan untuk peran baru ini.
- Pilih Gunakan ARN peran IAM kustom untuk menggunakan peran IAM kustom yang tidak terdaftar. 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`**.

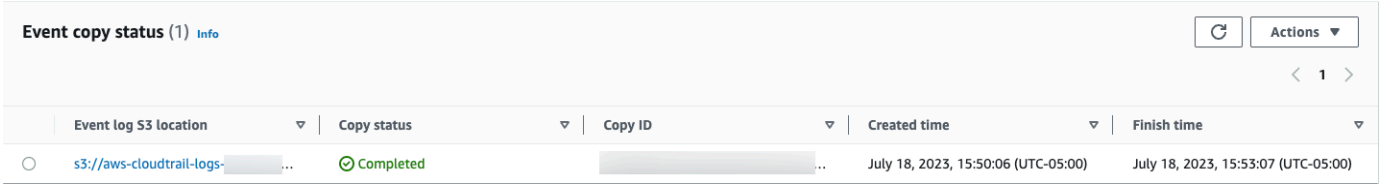


17. Pilih Berikutnya untuk meninjau pilihan Anda.
18. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
19. Penyimpanan data acara baru terlihat di tabel penyimpanan data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

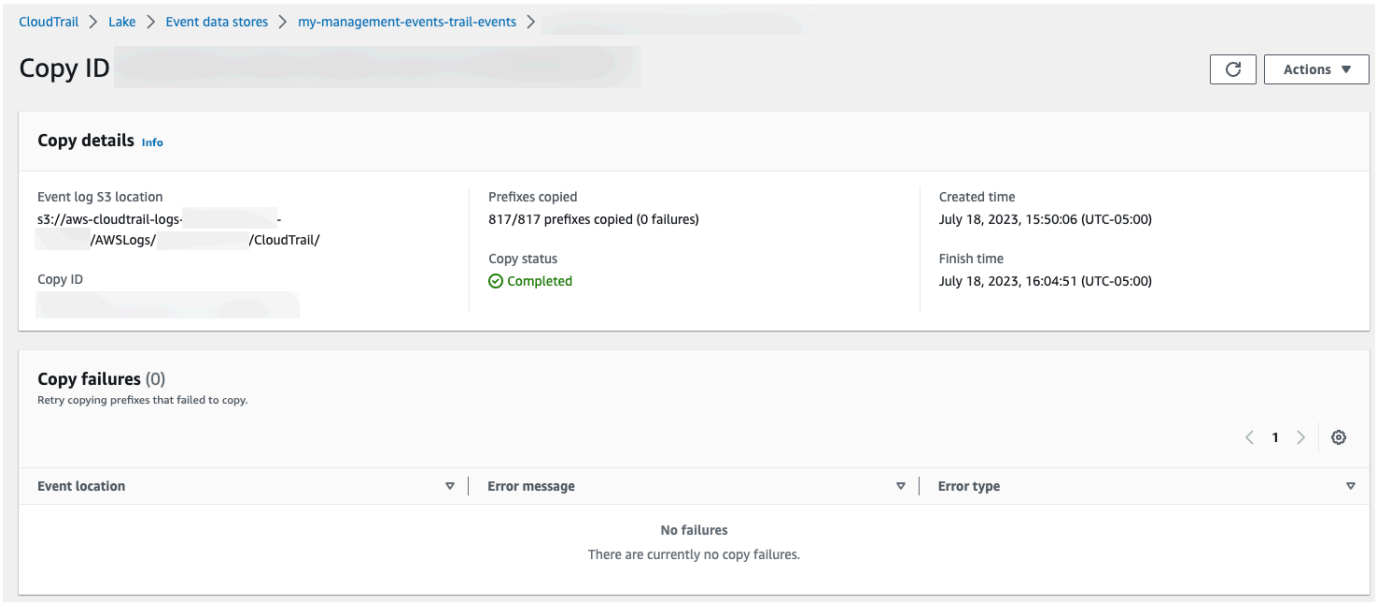


20. Pilih nama penyimpanan data acara untuk melihat halaman detailnya. Halaman detail menunjukkan detail untuk penyimpanan data acara Anda dan status salinannya. Status salinan peristiwa ditampilkan di area status salinan Acara.

    Ketika salinan peristiwa jejak selesai, status Salinannya disetel ke Selesai jika tidak ada kesalahan, atau Gagal jika terjadi kesalahan.



21. 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, lihatRincian salinan acara.



22. 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.

Tutorial: Lihat dasbor Danau

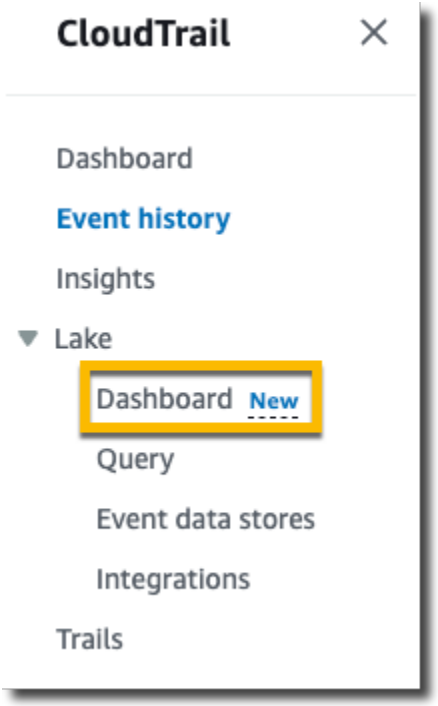
Tutorial ini menunjukkan cara melihat dasbor Danau. CloudTrail Dasbor danau memungkinkan Anda memvisualisasikan peristiwa di penyimpanan data acara Anda dan melihat tren, seperti pengguna teratas dan kesalahan teratas.

Setiap dashboard terdiri dari beberapa widget dan setiap widget mewakili query SQL. Untuk mengisi dasbor, CloudTrail jalankan kueri yang dihasilkan sistem. Kueri dikenakan biaya berdasarkan jumlah data yang dipindai.

> **Note**
>
> Saat ini, dasbor hanya tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa CloudTrail manajemen dan peristiwa data Amazon S3.

Untuk melihat dasbor Danau

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Dasbor.



3. Saat pertama kali Anda melihat halaman Dasbor, CloudTrail meminta Anda untuk mengetahui biaya yang terkait dengan menjalankan kueri. Pilih Saya setuju untuk mengakui biaya menjalankan kueri. Ini adalah konfirmasi satu kali. Untuk informasi selengkapnya tentang CloudTrail harga, lihat CloudTrailHarga.
4. Pilih penyimpanan data acara Anda dari daftar dan kemudian pilih jenis dasbor yang ingin Anda lihat.

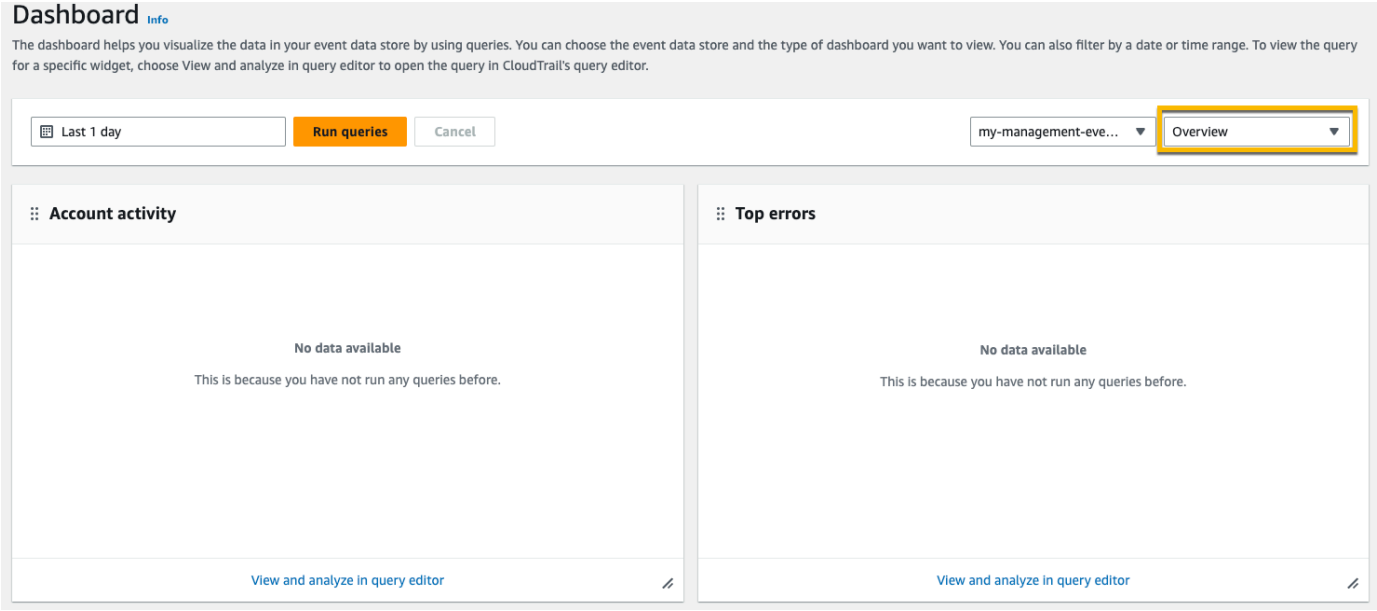
   Berikut ini adalah jenis dasbor yang mungkin.

   - Dasbor Ikhtisar - Menampilkan pengguna yang paling aktif Wilayah AWS,, dan Layanan AWS berdasarkan jumlah acara. Anda juga dapat melihat informasi tentang `read` dan `write` mengelola aktivitas acara, sebagian besar peristiwa yang dibatasi, dan kesalahan teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
   - Dasbor Acara Manajemen - Menampilkan peristiwa masuk konsol, mengakses peristiwa yang ditolak, tindakan destruktif, dan kesalahan teratas oleh pengguna. Anda juga dapat melihat informasi tentang versi TLS dan panggilan TLS yang sudah ketinggalan zaman oleh pengguna. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
   - Dasbor Acara Data S3 - Menampilkan aktivitas akun S3, objek S3 yang paling banyak diakses, pengguna S3 teratas, dan tindakan S3 teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data Amazon S3.
   - Dasbor Insights Events - Menunjukkan proporsi keseluruhan peristiwa Insights menurut jenis Insights, proporsi peristiwa Insights menurut jenis Insights untuk pengguna dan layanan teratas, dan jumlah acara Insights per hari. Dasbor juga menyertakan widget yang mencantumkan hingga 30 hari acara Insights. Dasbor ini hanya tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa 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. Untuk informasi selengkapnya, lihat Memahami penyampaian acara Wawasan.
     > - 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

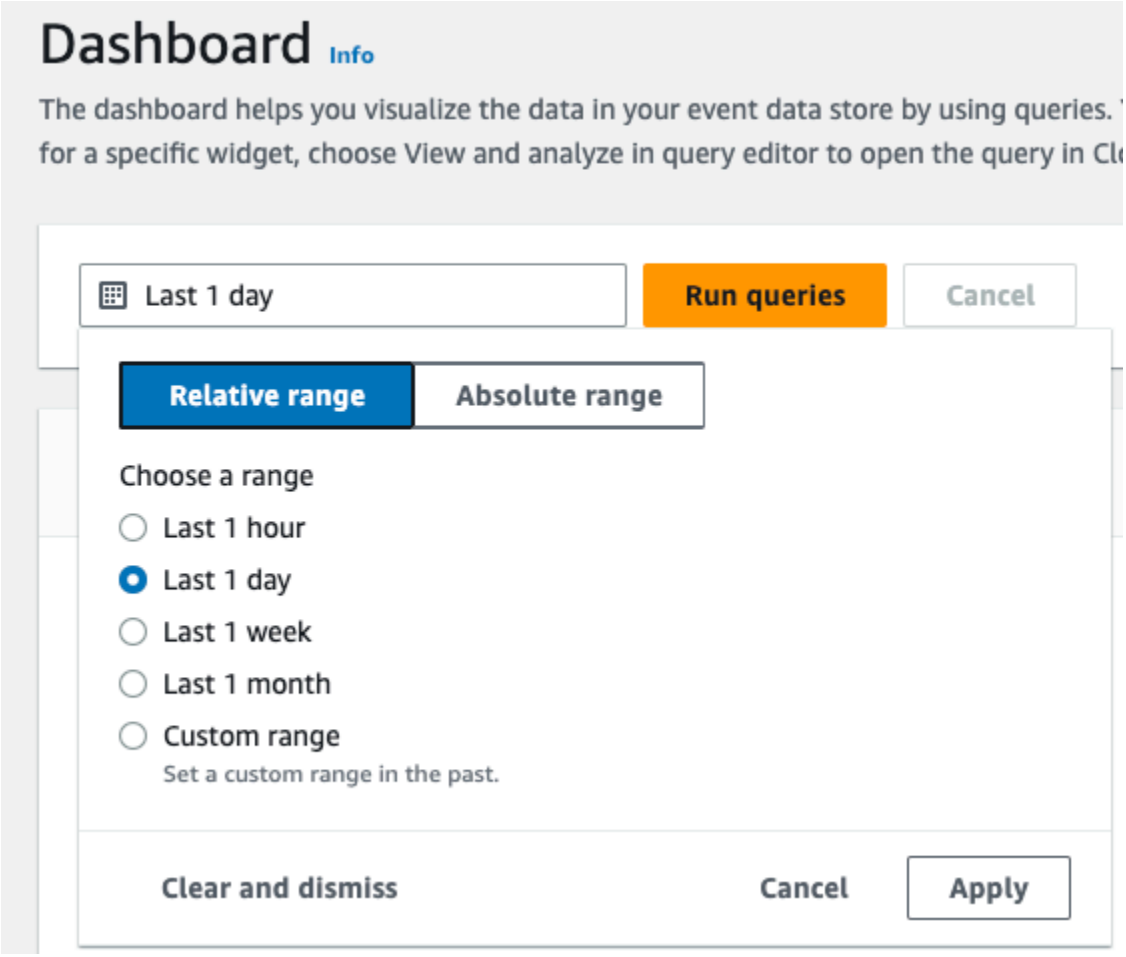
mengonfigurasi penyimpanan data peristiwa sumber untuk mengaktifkan peristiwa Wawasan `ApiCallRateInsight` tetapi tidak`ApiErrorRateInsight`, Anda tidak akan melihat informasi tentang peristiwa Wawasan. `ApiErrorRateInsight`

Dalam contoh ini, kami telah memilih dasbor Ikhtisar.



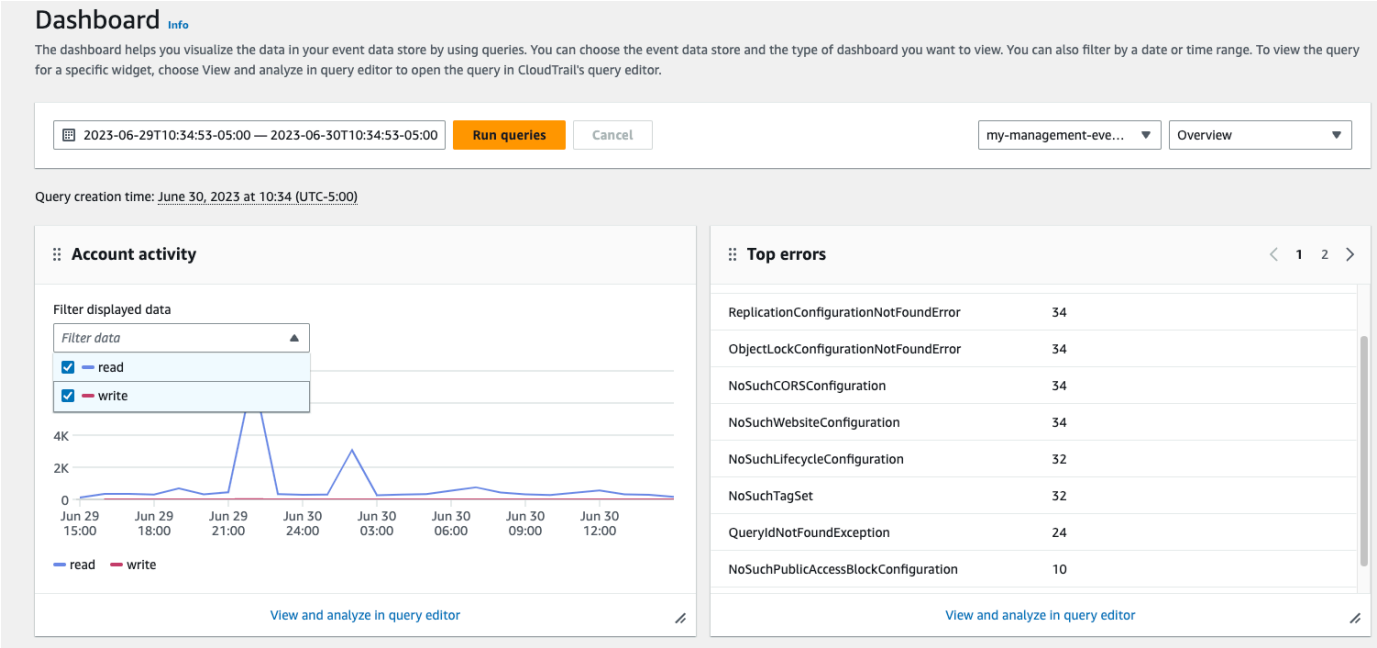
5. Pilih bidang tanggal untuk memfilter pada rentang waktu lalu pilih Terapkan. Pilih Rentang absolut untuk memilih tanggal dan rentang waktu tertentu. Pilih Rentang relatif untuk memilih rentang waktu yang telah ditentukan atau rentang khusus. Secara default, dasbor menampilkan data acara selama 24 jam terakhir.

> **Note**
>
> Karena CloudTrail kueri dibebankan berdasarkan jumlah data yang dipindai, Anda dapat mengurangi biaya dengan memfilter pada rentang waktu yang lebih sempit.

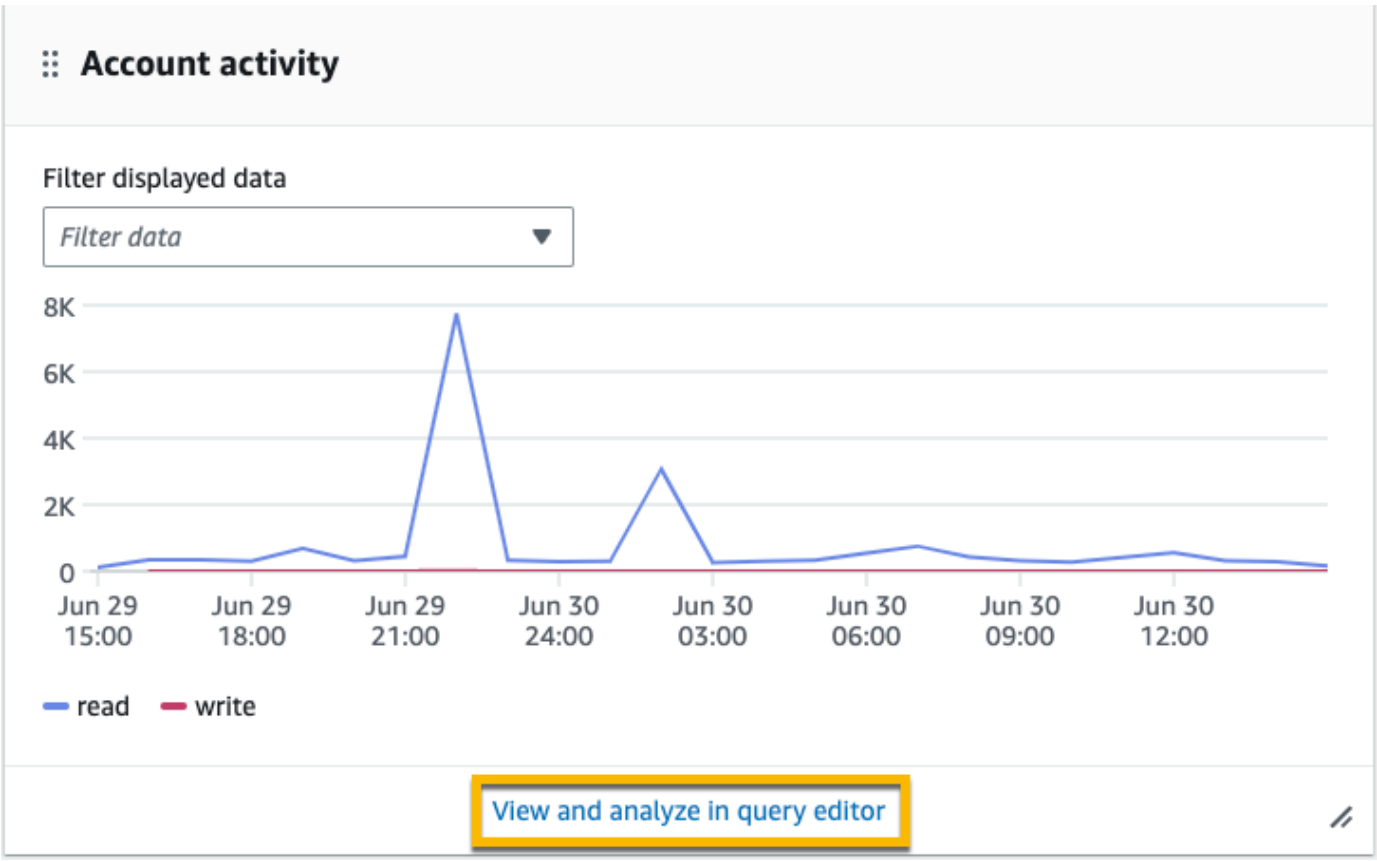


6. Pilih Jalankan kueri untuk mengisi dasbor. Setiap widget secara individual menampilkan status kueri terkait dan menyajikan data saat kueri selesai.

   Anda dapat melakukan pemfilteran tambahan pada beberapa widget, seperti Aktivitas akun, yang memungkinkan Anda memfilter aktivitas `read` dan `write` acara.

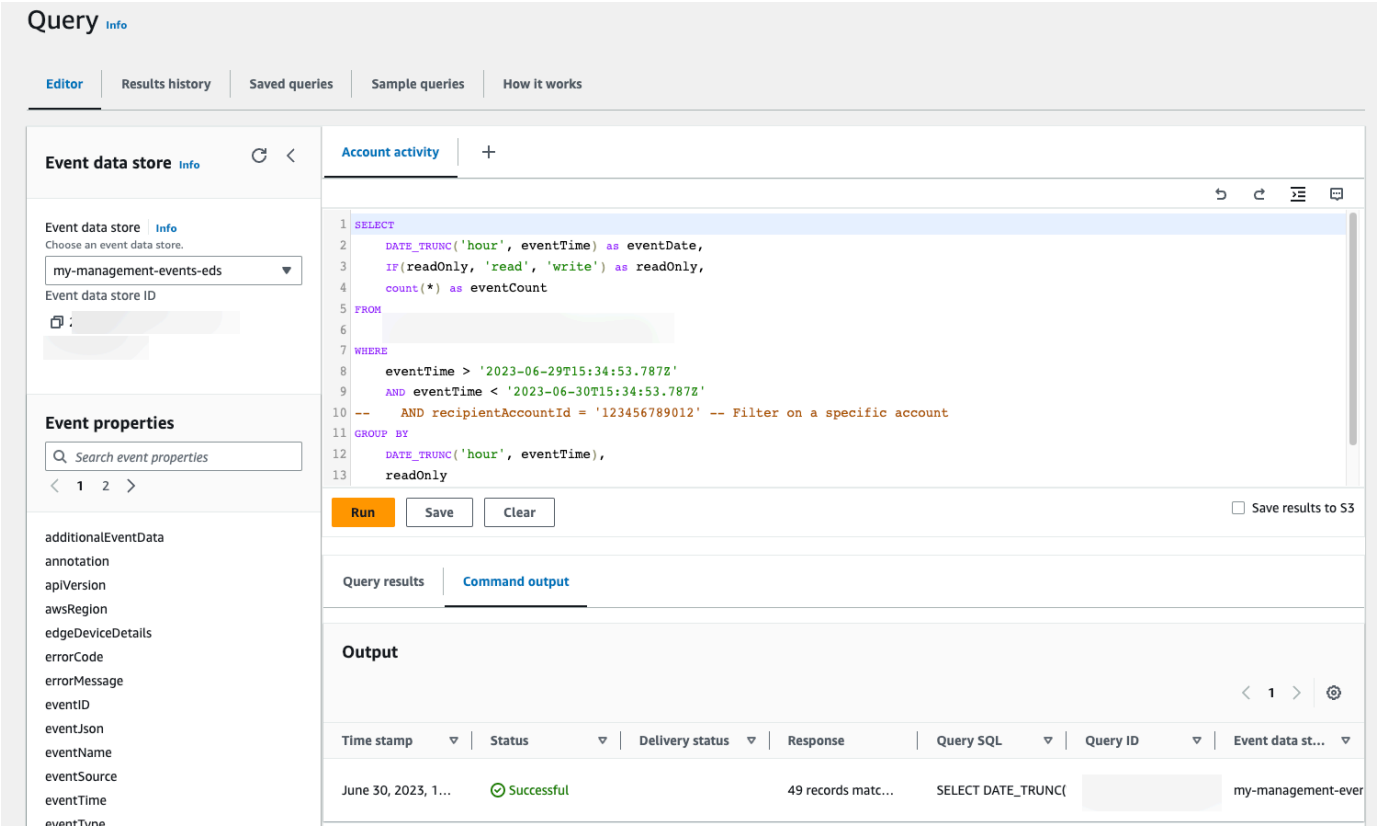


7. Untuk melihat kueri widget, pilih Lihat dan analisis di editor kueri.



Memilih Lihat dan menganalisis di editor kueri membuka kueri di editor kueri CloudTrail Lake, yang memungkinkan Anda menganalisis lebih lanjut hasil kueri di luar dasbor. Untuk informasi

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



Untuk informasi selengkapnya tentang dasbor, lihatLihat dasbor Danau.

Tutorial: Lihat dan jalankan contoh kueri

CloudTrail Lake menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis pertanyaan Anda sendiri. Tutorial ini menunjukkan cara memilih dan menjalankan query sampel.

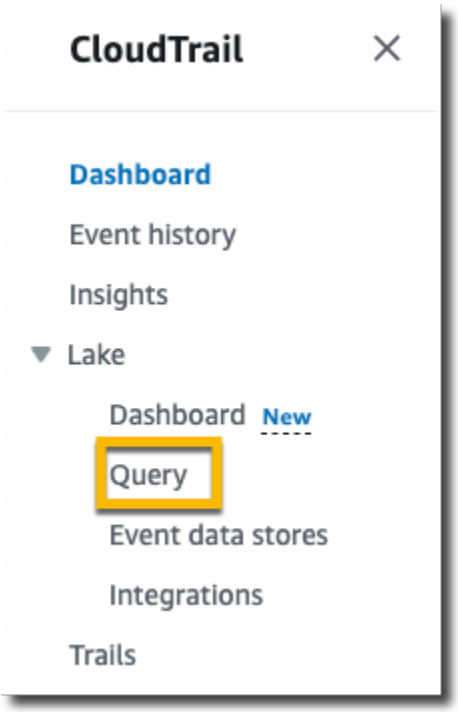
Pertanyaan di CloudTrail Lake ditulis dalam SQL. Anda dapat membuat kueri di tab CloudTrail Lake Editor dengan menulis kueri di SQL dari awal, atau dengan membuka kueri yang disimpan atau sampel dan mengeditnya. Anda tidak dapat menimpa kueri sampel yang disertakan dengan perubahan Anda, tetapi Anda dapat menyimpannya sebagai kueri baru. Untuk informasi selengkapnya tentang bahasa kueri SQL yang diizinkan, lihatCloudTrail Kendala Lake SQL.

CloudTrail kueri dikenakan biaya berdasarkan jumlah data yang dipindai. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan stempel `eventTime`

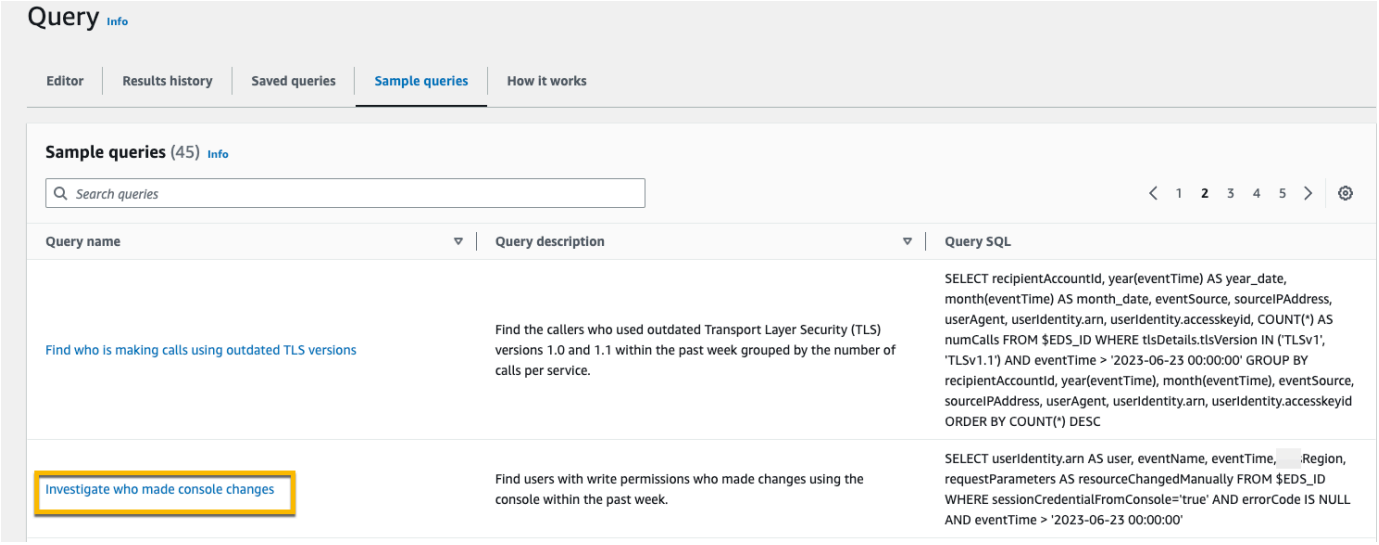
waktu mulai dan berakhir ke kueri. Untuk informasi selengkapnya tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Untuk melihat dan menjalankan kueri sampel

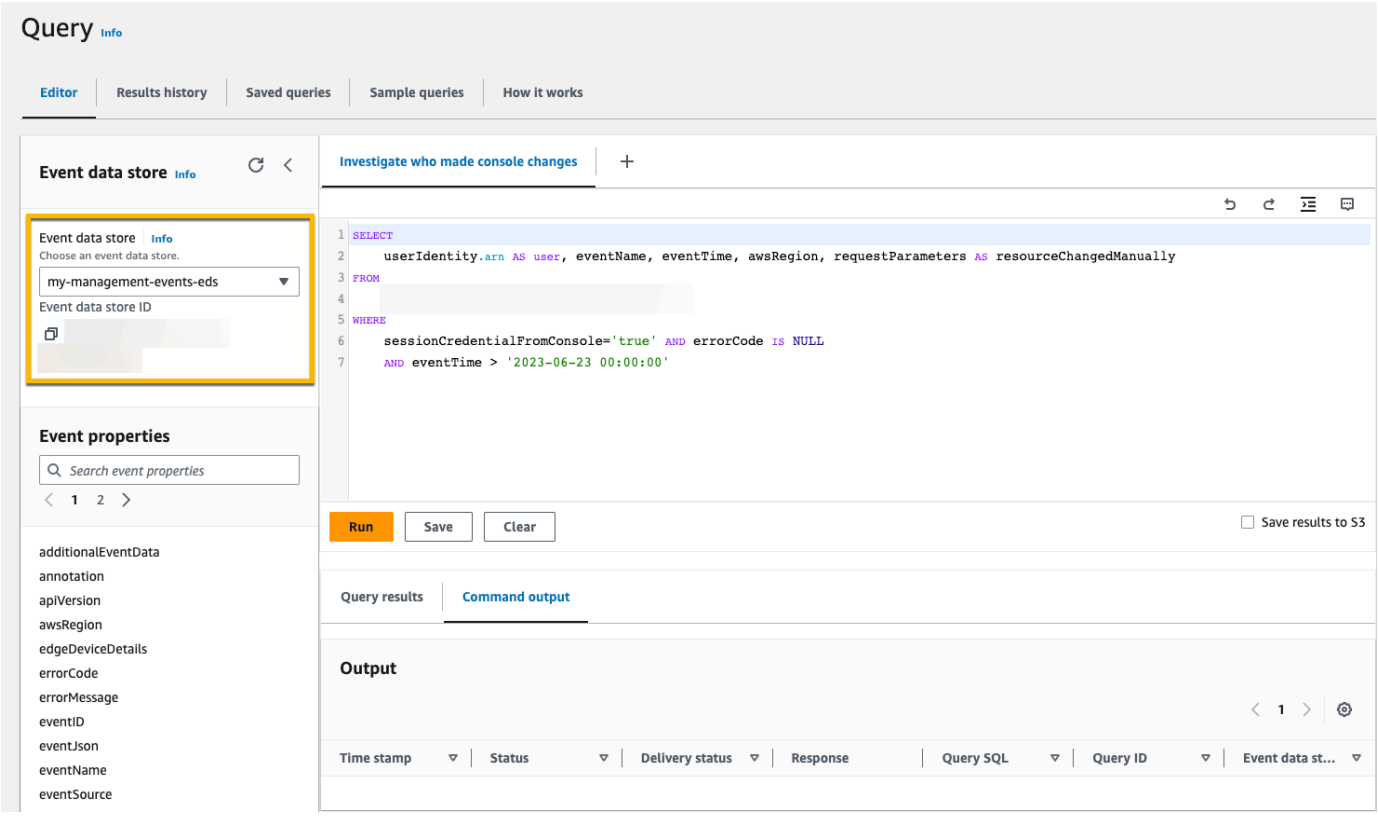
1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.



3. Pada halaman Query, pilih tab Contoh query.
4. Pilih contoh kueri dari daftar atau cari kueri untuk memfilter daftar. Dalam contoh ini, kita akan membuka kueri Selidiki siapa yang membuat perubahan konsol dengan memilih nama Query. Ini membuka kueri di tab Editor.

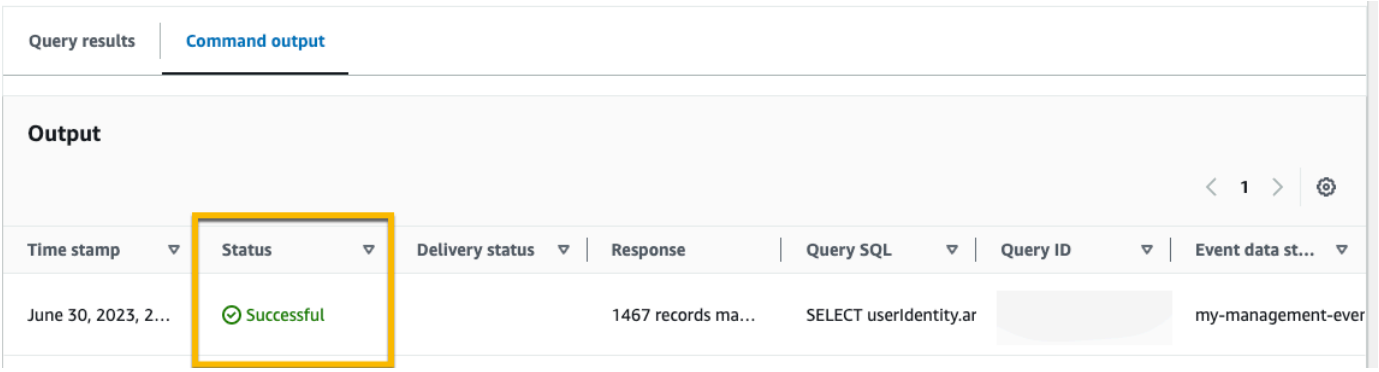


5. Pada tab Editor, pilih penyimpanan data acara yang ingin Anda jalankan kueri. Saat Anda memilih penyimpanan data acara dari daftar, CloudTrail secara otomatis mengisi ID penyimpanan data acara di `FROM` baris editor kueri.

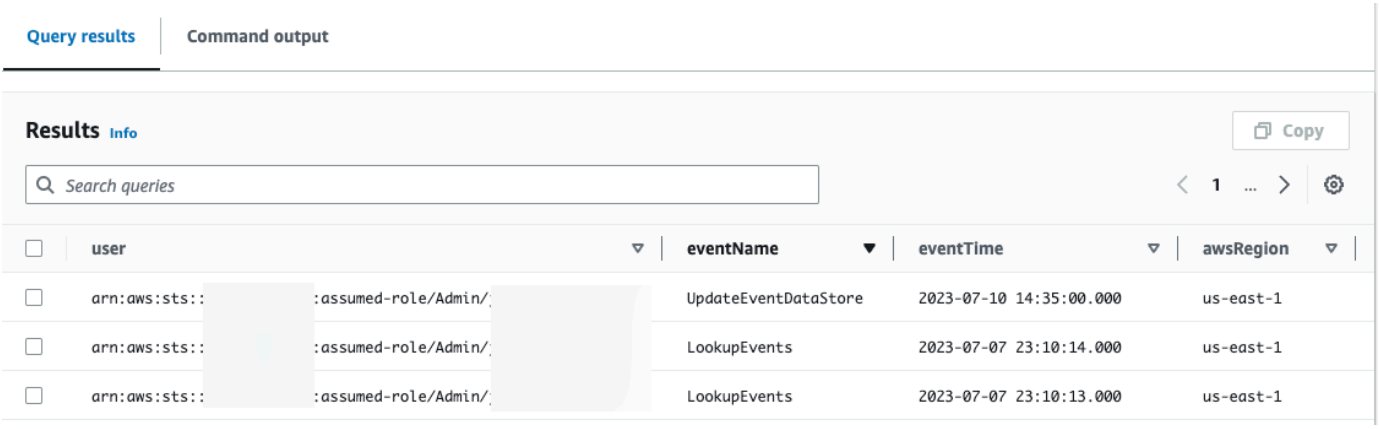


6. Pilih Jalankan untuk menjalankan kueri.

   Tab keluaran Perintah menunjukkan metadata tentang kueri Anda, seperti apakah kueri berhasil, jumlah catatan yang cocok, dan waktu proses kueri.



Tab Hasil kueri menunjukkan data peristiwa di penyimpanan data peristiwa yang dipilih yang cocok dengan kueri Anda.



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

Tutorial: Simpan hasil kueri ke bucket Amazon S3

Tutorial ini menunjukkan bagaimana Anda dapat menyimpan hasil kueri ke bucket S3 dan kemudian mengunduh hasil kueri tersebut.

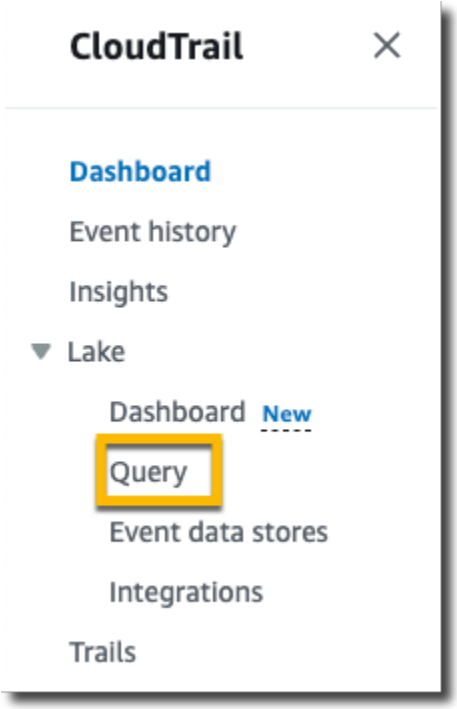
Saat menjalankan kueri di CloudTrail Lake, Anda dikenakan biaya berdasarkan jumlah data yang dipindai oleh kueri. Tidak ada biaya CloudTrail Danau tambahan untuk menyimpan hasil kueri ke ember S3, namun, ada biaya penyimpanan S3. Untuk informasi selengkapnya tentang harga S3, lihat harga Amazon S3.

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 menyimpan hasil kueri ke bucket Amazon S3

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.



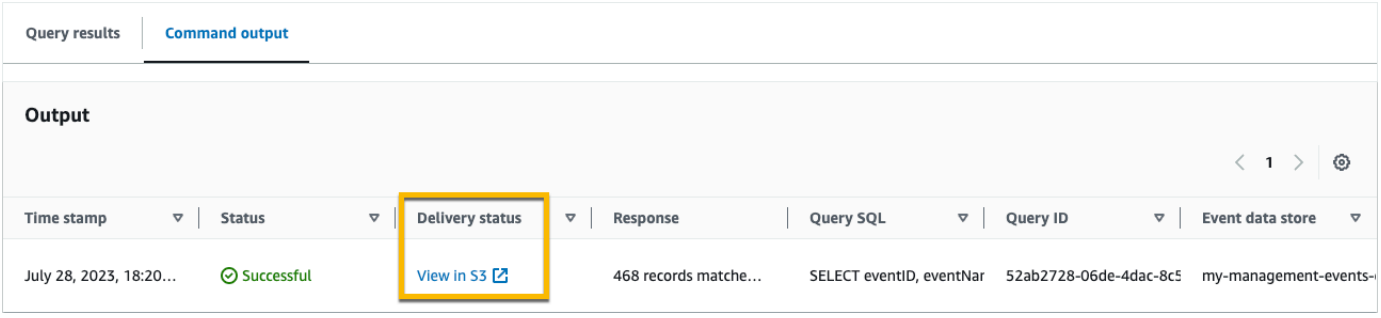
3. Pada tab Kueri sampel atau Kueri tersimpan, pilih kueri yang akan dijalankan dengan memilih nama Kueri. Dalam contoh ini, kita akan memilih contoh query bernama Investigate user actions.
4. Pada tab Editor, untuk penyimpanan data acara, pilih penyimpanan data acara dari daftar drop-down. Saat Anda 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. Untuk informasi selengkapnya tentang menyimpan hasil kueri, lihatInformasi tambahan tentang hasil kueri yang disimpan. Dalam contoh ini, kita akan menggunakan bucket S3 default.

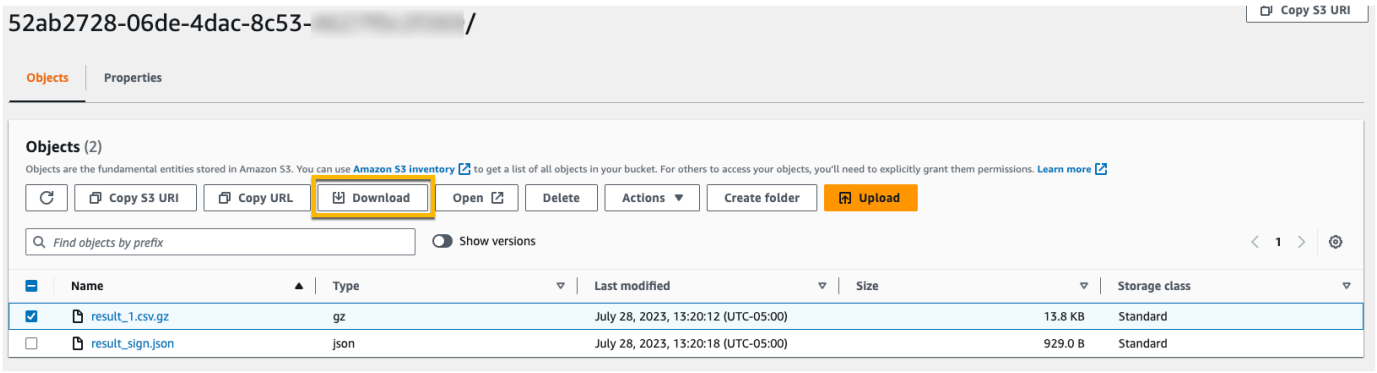
> **Note**
>
> Untuk menggunakan bucket yang berbeda, tentukan nama bucket, atau pilih Browse S3 untuk memilih bucket. Kebijakan bucket harus memberikan CloudTrail izin untuk mengirimkan hasil kueri ke bucket. Untuk informasi tentang mengedit kebijakan bucket secara manual, lihatKebijakan bucket Amazon 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 Command 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, lihatMemvalidasikan hasil kueri yang disimpan.

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 AWS Management Console, AWS Command Line Interface, dan AWS SDK dan API. 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 instans Amazon EC2) 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-eventsperintah 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 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 Riwayat acara side-by-side. Anda dapat secara terprogram mencari acara dengan menggunakan AWS SDK atau. 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 apa pun 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

Batasan berikut berlaku untuk riwayat Acara.

- Halaman Riwayat peristiwa di CloudTrail konsol hanya menampilkan peristiwa manajemen. Itu tidak menampilkan peristiwa data atau peristiwa Wawasan.
- 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 dalam riwayat Acara, atau berjalan. `LookupEvents` Lihat informasi yang lebih lengkap di Bekerja dengan AWS CloudTrail Danau dan Buat penyimpanan data acara untuk CloudTrail acara.
- 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 peristiwa CloudTrail manajemen terbaru di CloudTrail 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 side-by-side.

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 acara. 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, buat penyimpanan data acara atau jejak.
> Membuat penyimpanan data acara memungkinkan Anda memanfaatkan fitur-fitur berikut:
>
> - Anda dapat membuat penyimpanan data acara untuk mengumpulkan peristiwa CloudTrail manajemen dan data, item AWS Config konfigurasi, AWS Audit Manager bukti, atau AWS non-peristiwa dari integrasi. Lihat informasi yang lebih lengkap di Bekerja dengan AWS CloudTrail Danau dan Buat toko data acara.
> - Analisis aktivitas AWS layanan Anda dengan kueri CloudTrail Lake. 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` Pencarian riwayat peristiwa terbatas pada satu Akun AWS, hanya menampilkan peristiwa dari satu Wilayah AWS, dan tidak dapat menanyakan beberapa atribut. Sebaliknya, pengguna CloudTrail Lake dapat menjalankan kueri SQL yang kompleks di beberapa

bidang acara. Lihat informasi yang lebih lengkap di Membuat atau mengedit kueri dan Melihat contoh kueri di konsol CloudTrail .

- Lihat dasbor CloudTrail Lake untuk memvisualisasikan data di penyimpanan data acara Anda. Untuk informasi selengkapnya, lihat Lihat dasbor Danau.
- Penyimpanan data peristiwa memungkinkan Anda mengecualikan AWS Key Management Service (AWS KMS) atau peristiwa Amazon Relational Database Service Data Data API. AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Peristiwa tidak dapat dikecualikan dari riwayat Acara.

Membuat jejak memungkinkan Anda memanfaatkan integrasi berikut:

- Jejak memungkinkan Anda mencatat peristiwa CloudTrail Insights, yang dapat membantu Anda mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan panggilan API `write` manajemen. Untuk informasi selengkapnya, lihat Acara Logging Insights.
- Analisis aktivitas AWS layanan Anda dengan kueri di Amazon Athena. Untuk informasi selengkapnya, lihat Membuat Tabel untuk CloudTrail Log di CloudTrail Konsol di Panduan Pengguna Amazon Athena, atau pilih opsi untuk membuat tabel langsung dari riwayat peristiwa di CloudTrail konsol.
- Pantau log jejak Anda dan beri tahu saat aktivitas tertentu terjadi dengan CloudWatch Log Amazon. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.
- Jejak memungkinkan Anda mengecualikan AWS Key Management Service (AWS KMS) atau peristiwa Amazon Relational Database Service Data API. AWS KMS tindakan seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Peristiwa tidak dapat dikecualikan dari riwayat Acara.

Untuk melihat CloudTrail peristiwa terbaru di konsol

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/home/.
2. Pada panel navigasi, pilih Riwayat peristiwa.

   Daftar peristiwa yang difilter muncul di panel konten dengan acara terbaru terlebih dahulu. Gulir ke bawah untuk melihat lebih banyak acara.

3. Untuk membandingkan peristiwa, pilih hingga lima peristiwa dengan mengisi kotak centang di margin kiri tabel Riwayat acara. Lihat detail untuk acara yang dipilih side-by-side di tabel Bandingkan detail acara.

Tampilan default peristiwa dalam riwayat Acara menggunakan filter atribut untuk mengecualikan peristiwa hanya-baca dari daftar peristiwa yang ditampilkan. Untuk menghapus filter ini, atau untuk menerapkan filter lain, ubah pengaturan filter. Untuk informasi selengkapnya, lihat Acara penyaringan CloudTrail .

Daftar Isi

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
  - Jenis 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 AWS Management Console 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 bernama 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 kredensil 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.

Jenis 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 di konsol CloudTrail

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

Melihat acara CloudTrail 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
- Jenis 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

- Untuk menjalankan AWS CLI perintah, Anda harus menginstal file AWS CLI. Untuk selengkapnya, lihat Menginstal Antarmuka Baris AWS Perintah.
- 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 isi rekaman.

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 hanya dapat menentukan satu pasangan kunci/nilai 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 Menghasilkan Parameter JSON CLI Skeleton dan CLI Input.

Untuk mencari CloudTrail acara 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 --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

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.

Bekerja dengan AWS CloudTrail Danau

AWS CloudTrail Lake memungkinkan Anda menjalankan kueri berbasis SQL 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 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun. Penyeleksi yang Anda terapkan ke penyimpanan data acara 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 Menyimpan data acara danau

Saat Anda membuat penyimpanan data acara, Anda memilih jenis acara yang akan disertakan dalam penyimpanan data acara Anda. Anda dapat membuat penyimpanan data acara untuk menyertakan CloudTrail peristiwa, 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 acara unik untuk kategori acara. Anda dapat menyimpan acara dari organisasi AWS Organizations dalam penyimpanan data acara organisasi, termasuk peristiwa 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 point-in-time snapshot peristiwa yang dicatat ke jejak. Untuk informasi selengkapnya, lihat Salin peristiwa jejak ke 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. Untuk informasi selengkapnya, lihat Federasi toko data acara.

Secara default, semua peristiwa di penyimpanan data acara dienkripsi oleh. CloudTrail Saat Anda mengonfigurasi penyimpanan data acara, 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 di panduan ini.

Anda dapat menggunakan dasbor CloudTrail Danau untuk memvisualisasikan data di penyimpanan data acara Anda. Setiap dashboard terdiri dari beberapa widget dan setiap widget mewakili query SQL. Untuk informasi lebih lanjut tentang dasbor Danau, lihatLihat dasbor Danau.

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.

CloudTrail Lake mendukung CloudWatch metrik Amazon, yang memberikan 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 Integrasi danau

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. Setelah Anda membuat

penyimpanan data peristiwa di CloudTrail Lake dan membuat saluran untuk mencatat peristiwa aktivitas, Anda memanggil `PutAuditEvents` API untuk memasukkan CloudTrail aktivitas aplikasi Anda. 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 peristiwa ke penyimpanan data acara untuk AWS akun Anda.

Untuk informasi selengkapnya tentang integrasi, lihat Membuat integrasi dengan sumber peristiwa di luar. AWS

CloudTrail Pertanyaan danau

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` Pencarian riwayat peristiwa terbatas pada satu Akun AWS, hanya menampilkan peristiwa dari satu Wilayah AWS, dan tidak dapat menanyakan beberapa atribut. Sebaliknya, pengguna CloudTrail Lake dapat menjalankan kueri SQL yang kompleks di beberapa bidang acara. CloudTrail Lake mendukung semua `SELECT` pernyataan dan fungsi Presto yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Presto.

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.

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri. Untuk informasi selengkapnya, lihat Melihat contoh kueri di konsol CloudTrail .

CloudTrail Pertanyaan 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 danMengelola biaya CloudTrail Danau.

CloudTrail Daerah yang didukung Danau

Saat ini, CloudTrail Danau didukung sebagai berikutWilayah AWS:

Nama Wilayah	wilayah
AS Timur (Virginia Utara)	us-east-1
US East (Ohio)	us-east-2
US West (Northern California)	us-west-1
US West (Oregon)	us-west-2
Kanada (Pusat)	ca-central-1
Afrika (Cape Town)	af-selatan-1
Asia Pasifik (Hong Kong)	ap-timur-1
Asia Pasifik (Mumbai)	ap-south-1
Asia Pasifik (Tokyo)	ap-northeast-1
Asia Pasifik (Seoul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Asia Pasifik (Singapura)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Jakarta)	ap-southeast-3
Eropa (Frankfurt)	eu-central-1
Eropa (Stockholm)	eu-north-1
Eropa (Irlandia)	eu-west-1
Europe (London)	eu-west-2

Nama Wilayah	wilayah
Europe (Paris)	eu-west-3
Eropa (Milan)	eu-south-1
Timur Tengah (UEA)	eu-central-1
Timur Tengah (Bahrain)	me-south-1
AWS GovCloud (AS-Timur)	us-gov-east-1
AWS GovCloud (AS-Barat)	us-gov-west-1
Amerika Selatan (Sao Paulo)	sa-east-1

Untuk informasi tentang titik akhir CloudTrail layanan, lihat AWS CloudTrailtitik akhir dan kuota.

Untuk informasi selengkapnya tentang penggunaan CloudTrail di Wilayah AWS GovCloud (AS-Timur), lihat Titik Akhir AWS GovCloud (AS-Timur) di Panduan Pengguna. AWS GovCloud (US)

Untuk informasi selengkapnya tentang penggunaan CloudTrail di Wilayah AWS GovCloud (AS-Barat), lihat Titik Akhir AWS GovCloud (AS-Barat) di Panduan Pengguna. AWS GovCloud (US)

CloudTrail Konsep dan terminologi danau

Bagian ini menjelaskan konsep dan istilah kunci untuk membantu Anda menggunakan AWS CloudTrail Lake.

Konsep dan istilah

- Menyimpan data acara
- Integrasi
- Queries
- 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 peristiwa CloudTrail manajemen dan peristiwa data, peristiwa CloudTrail Wawasan, AWS Audit Managerbukti, 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 dan peristiwa data, 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 luarAWS, 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 Danau, 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 Federasi toko 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 CloudTrailHarga danMengelola biaya CloudTrail Danau.

Periode penahanan

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.

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 AndaAkun 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 AndaAkun 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 CloudTrailcontoh kebijakan berbasis sumber daya.

Queries

Pertanyaan di CloudTrail Lake 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. Anda tidak dapat menimpa kueri sampel yang disertakan dengan perubahan Anda, tetapi Anda dapat menyimpannya sebagai kueri baru. Untuk informasi selengkapnya, lihat Membuat atau mengedit kueri.

CloudTrail Lake mendukung semua Presto `SELECT` pernyataan dan fungsi yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web Presto dokumentasi.

Dasbor

Dengan menggunakan dasbor CloudTrail Lake, Anda dapat memvisualisasikan peristiwa di penyimpanan data acara dan melihat tren peristiwa, seperti topLayanan AWS, pengguna, dan kesalahan. Untuk informasi selengkapnya, lihat Lihat dasbor Danau.

Jenis dasbor

Jenis dasbor yang tersedia untuk penyimpanan data acara bergantung pada konfigurasi pemilih acara lanjutan dari penyimpanan data acara. Misalnya, jika tipe dasbor menampilkan informasi tentang peristiwa CloudTrail manajemen, Anda hanya dapat memilih dasbor jika penyimpanan data acara yang dipilih saat ini mengumpulkan peristiwa CloudTrail manajemen.

Berikut ini adalah jenis dasbor yang tersedia:

- Dasbor Ikhtisar - Menampilkan pengguna yang paling aktifWilayah AWS,, dan Layanan AWS berdasarkan jumlah acara. Anda juga dapat melihat informasi tentang `read` dan `write` mengelola aktivitas acara, sebagian besar peristiwa yang dibatasi, dan kesalahan teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
- Dasbor Acara Manajemen — Menampilkan peristiwa masuk konsol, mengakses peristiwa yang ditolak, tindakan destruktif, dan kesalahan teratas oleh pengguna. Anda juga dapat melihat informasi tentang versi TLS dan panggilan TLS yang sudah ketinggalan zaman oleh pengguna. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
- Dasbor Acara Data S3 - Menampilkan aktivitas akun Amazon S3, objek S3 yang paling banyak diakses, pengguna S3 teratas, dan tindakan S3 teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data Amazon S3.

- Dasbor Insights Events - Menunjukkan proporsi keseluruhan peristiwa Insights menurut jenis Insights, proporsi peristiwa Insights menurut jenis Insights untuk pengguna dan layanan teratas, dan jumlah acara Insights per hari. Dasbor juga menyertakan widget yang mencantumkan hingga 30 hari acara Insights. Dasbor ini hanya tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa 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. Untuk informasi selengkapnya, lihat Memahami penyampaian acara Wawasan.
  > - 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`

Widget

Widget adalah komponen yang membentuk dasbor dan memberikan visualisasi, seperti diagram garis atau grafik batang. Setiap widget mewakili kueri yang mendasarinya. Saat Anda memilih Jalankan kueri, CloudTrail jalankan kueri yang dihasilkan sistem untuk mengisi data untuk setiap widget.

Buat toko data acara

Saat Anda membuat penyimpanan data acara di CloudTrail Lake, Anda memilih jenis acara yang akan disertakan dalam penyimpanan data acara Anda. Anda dapat membuat penyimpanan data acara untuk menyertakan peristiwa CloudTrail data atau manajemen, 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 acara 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 acara. Kolom EventCategory menunjukkan nilai yang akan Anda tentukan dalam pemilih acara lanjutan untuk mengumpulkan peristiwa dari jenis itu.

Jenis acara (konsol)	EventCategory (API)	Deskripsi

CloudTrail acara	`Management`
	
	`Data`
		Jenis penyimpanan data acara ini dapat mengumpulkan peristiwa CloudTrail manajemen dan data. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk CloudTrail acara.

CloudTrail Insights acara	`Insight`	Jenis penyimpanan data acara 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 acara untuk peristiwa CloudTrail Wawasan.
Item konfigurasi	`Configura tionItem`	Jenis penyimpanan data acara ini dapat mengumpulkan item AWS Config konfigurasi. Untuk informasi selengkapnya, lihat Membuat penyimpanan data acara untuk item AWS Config konfigurasi.
Acara dari integrasi	`ActivityA uditLog`	Jenis penyimpanan data acara ini dapat mengumpulkan AWS non-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 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.

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.

Bagian berikut menjelaskan cara membuat, memperbarui, dan menghapus penyimpanan data acara menggunakan CloudTrail konsol. Untuk informasi tentang cara mengelola penyimpanan data acara menggunakan AWS CLI, lihatMengelola CloudTrail Danau dengan menggunakan AWS CLI.

Topik

Buat penyimpanan data acara untuk CloudTrail acara

Penyimpanan data acara untuk CloudTrail acara dapat mencatat CloudTrail manajemen dan peristiwa data. Anda dapat menyimpan data acara di penyimpanan data acara hingga 3.653 hari (sekitar 10 tahun) jika Anda memilih opsi harga retensi yang dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun..

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.

Untuk membuat penyimpanan data acara untuk CloudTrail manajemen atau peristiwa data

Gunakan prosedur ini untuk membuat penyimpanan data peristiwa yang mencatat peristiwa CloudTrail manajemen, peristiwa data, atau peristiwa manajemen dan data.

1. Masuk ke AWS Management Console 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, di Rincian umum, masukkan nama untuk penyimpanan data acara. Diperlukan nama.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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

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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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**
   >
   > Jika Anda menyalin peristiwa jejak ke penyimpanan data acara ini, tidak CloudTrail akan menyalin peristiwa jika lebih tua dari periode retensi yang ditentukan. `eventTime` 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) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya 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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko 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) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda 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 AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS

10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.

11. Pada halaman Pilih acara, pilih AWS acara, lalu pilih CloudTrailacara.

12. Untuk CloudTrail acara, pilih setidaknya satu jenis acara. Secara default, acara Manajemen dipilih. Anda dapat menambahkan acara manajemen dan data ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang acara manajemen, lihatAcara manajemen logging. Untuk informasi selengkapnya tentang peristiwa data, lihatPencatatan peristiwa data.
13. (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 acara organisasi. Untuk informasi selengkapnya tentang pertimbangan untuk menyalin peristiwa jejak, lihat. Pertimbangan untuk menyalin acara jejak
14. Agar penyimpanan data acara Anda mengumpulkan acara dari semua akun di 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.

15. Perluas Pengaturan tambahan untuk memilih apakah Anda ingin penyimpanan data acara mengumpulkan acara 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 menelan 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 mencakup acara dari semua Wilayah.

    b. Hapus pilihan acara Ingest jika Anda tidak ingin penyimpanan data acara mulai menelan peristiwa. Misalnya, Anda mungkin ingin membatalkan pilihan acara Ingest, jika Anda menyalin peristiwa jejak dan tidak ingin penyimpanan data acara menyertakan peristiwa masa depan. Secara default, penyimpanan data acara mulai menelan peristiwa saat dibuat.

16. Jika penyimpanan data acara Anda menyertakan acara manajemen, Anda dapat memilih dari opsi berikut. Untuk informasi selengkapnya tentang acara manajemen, lihatAcara manajemen logging.

a. Pilih apakah Anda ingin menyertakan acara Baca, Menulis acara, atau keduanya. Setidaknya satu diperlukan.

b. Pilih apakah akan mengecualikan AWS Key Management Service atau peristiwa Amazon RDS Data API dari penyimpanan data acara Anda.

c. Pilih apakah akan 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. Di Aktifkan Wawasan, 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 acara tujuan yang mencatat peristiwa Wawasan.

   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.

17. Untuk menyertakan peristiwa data di penyimpanan data acara Anda, lakukan hal berikut.

    a. Pilih jenis peristiwa data. Ini adalah Layanan AWS dan sumber daya di mana peristiwa data dicatat. Untuk mencatat peristiwa data untuk AWS Glue tabel yang dibuat oleh Lake Formation, pilih Lake Formation untuk tipe data.

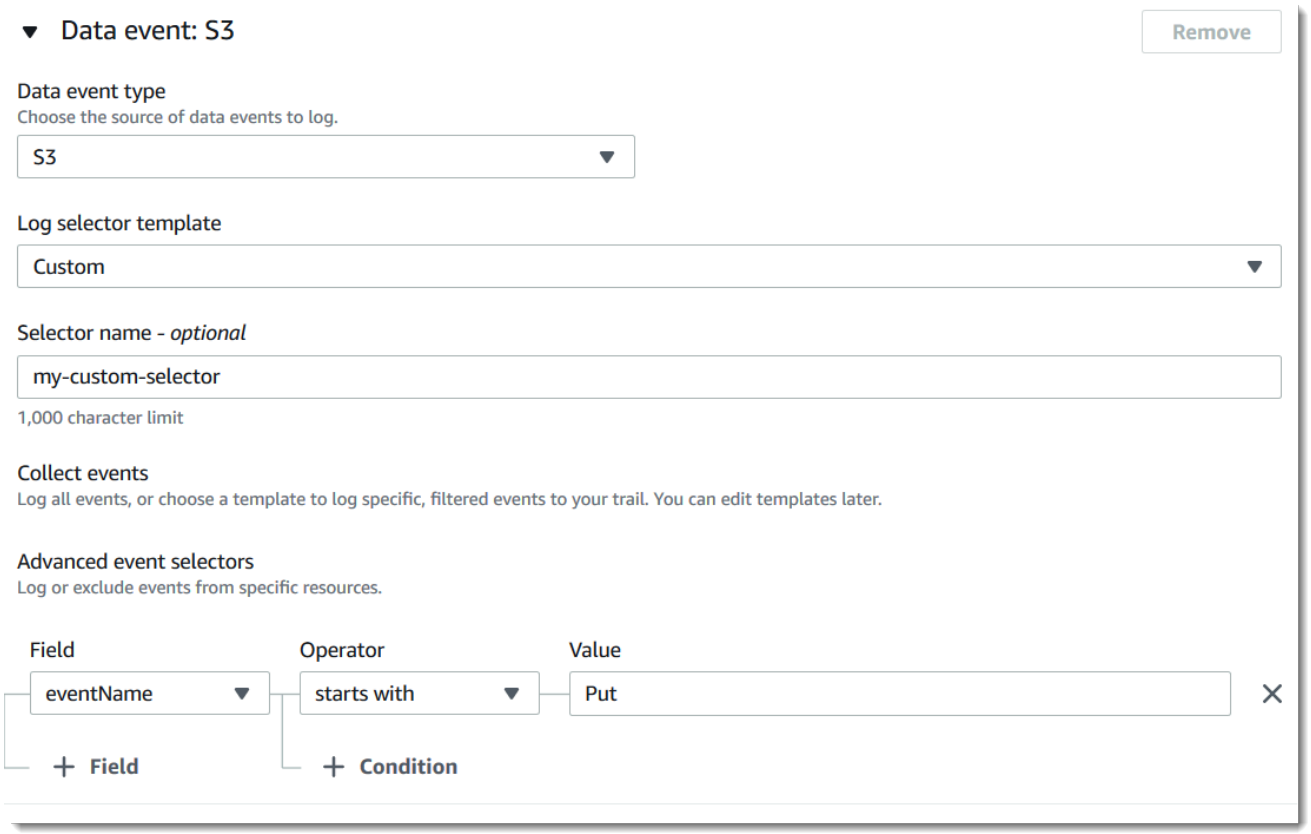
    b. Di template pemilih Log, pilih templat. Anda dapat memilih untuk mencatat semua peristiwa data, `readOnly` peristiwa, `writeOnly` peristiwa, atau Kustom untuk membuat pemilih log kustom.

    c. (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.

    d. Di Selektor acara lanjutan, buat ekspresi dengan memilih nilai untuk Field, Operator, dan Value. Penyeleksi acara lanjutan untuk penyimpanan data acara bekerja sama dengan pemilih acara tingkat lanjut yang Anda terapkan ke jejak. Untuk informasi selengkapnya

tentang cara membuat penyeleksi peristiwa tingkat lanjut, lihat Mencatat peristiwa data dengan pemilih peristiwa lanjutan.

Contoh berikut menggunakan template pemilih log Kustom untuk memilih hanya nama acara dari objek S3 yang dimulai dengan`Put`, seperti. `PutObject` Karena pemilih peristiwa lanjutan tidak menyertakan atau mengecualikan jenis peristiwa atau ARN sumber daya lainnya, semua peristiwa data S3, baik baca maupun tulis, yang memiliki nama acara dimulai dengan`Put`, disimpan di penyimpanan data peristiwa.



> **Important**
>
> Untuk mengecualikan atau menyertakan peristiwa data dengan pemilih peristiwa lanjutan dengan menggunakan ARN bucket S3, selalu gunakan operator Mulai dengan.

e. Secara opsional, perluas tampilan JSON untuk melihat pemilih acara lanjutan Anda sebagai blok JSON.

18. 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 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, lihat[Kebijakan 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.

> **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.

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 peran IAM kustom untuk menggunakan peran IAM kustom yang tidak terdaftar. Untuk Masukkan peran IAM ARN, masukkan ARN IAM.
- Pilih Gunakan peran yang ada untuk memilih peran IAM yang ada dari daftar drop-down.

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

    Mulai saat ini, penyimpanan data acara menangkap peristiwa yang cocok dengan pemilih acara lanjutannya (jika Anda tetap memilih opsi acara Ingest). Peristiwa yang terjadi sebelum Anda membuat penyimpanan data acara tidak ada di penyimpanan data acara, kecuali Anda memilih untuk menyalin peristiwa jejak yang ada.

Anda sekarang dapat menjalankan kueri di penyimpanan data acara baru Anda. Tab Contoh kueri menyediakan contoh kueri untuk membantu Anda memulai. Untuk informasi selengkapnya tentang membuat dan mengedit kueri, lihatMembuat atau mengedit kueri.

Anda juga dapat melihat dasbor CloudTrail Danau untuk memvisualisasikan peristiwa di penyimpanan data acara Anda. Untuk informasi lebih lanjut tentang dasbor Danau, lihatLihat dasbor Danau.

Membuat penyimpanan data acara untuk acara CloudTrail Insights

AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan panggilan API dan tingkat kesalahan API dengan terus menganalisis peristiwa CloudTrail manajemen. CloudTrail Wawasan 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 volume panggilan API dibuat untuk API `write` manajemen, dan peristiwa Insights tentang tingkat kesalahan API dibuat untuk keduanya `read` dan API `write` manajemen.

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.

> **Note**
>
> Untuk mencatat peristiwa Insights pada volume 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, kirimkan peristiwa CloudTrail Insights ke penyimpanan data acara tujuan Anda. Tidak seperti jenis peristiwa lain yang ditangkap dalam penyimpanan data CloudTrail peristiwa, peristiwa Insights dicatat hanya ketika CloudTrail mendeteksi perubahan dalam penggunaan API akun Anda yang berbeda secara signifikan dari pola penggunaan biasa akun.

Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data acara, diperlukan waktu hingga 7 hari CloudTrail untuk menyampaikan acara Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

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 kedua jalur dan penyimpanan data acara CloudTrail Lake. Untuk informasi tentang CloudTrail harga, lihat AWS CloudTrail Harga.

Topik

- Untuk membuat penyimpanan data acara tujuan yang mencatat peristiwa Wawasan
- Untuk membuat penyimpanan data peristiwa sumber yang memungkinkan peristiwa Insights

Untuk membuat penyimpanan data acara tujuan yang mencatat peristiwa Wawasan

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 dapat mengaktifkan Insights pada penyimpanan data acara baru atau yang sudah ada setelah Anda membuat penyimpanan data acara Insights, lalu memilih penyimpanan data acara ini sebagai penyimpanan data acara tujuan.

Prosedur ini menunjukkan cara membuat penyimpanan data acara tujuan yang mencatat peristiwa Wawasan.

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, buka submenu Danau, lalu pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Configure event data store, di Rincian umum, masukkan nama untuk penyimpanan data acara. Diperlukan nama.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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

6. Tentukan periode retensi untuk penyimpanan data acara dalam beberapa hari. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi yang dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun. Penyimpanan data peristiwa menyimpan data peristiwa untuk jumlah hari yang ditentukan.
7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya 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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko 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) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda 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 AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS
10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
11. Pada halaman Pilih acara, pilih AWS acara, lalu pilih acara CloudTrail Wawasan.
12. Dalam acara CloudTrail Wawasan, 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 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 acara sumber, lakukan hal berikut.

i. Pilih Tambahkan penyimpanan data acara sumber.

ii. Pilih penyimpanan data acara sumber.

iii. Pilih jenis Wawasan yang ingin Anda terima.

- `ApiCallRateInsight`— Tipe `ApiCallRateInsight` Insights menganalisis panggilan API manajemen khusus tulis yang digabungkan per menit terhadap volume panggilan API dasar. Untuk menerima Wawasan tentang`ApiCallRateInsight`, penyimpanan data peristiwa sumber harus mencatat peristiwa manajemen Tulis.
- `ApiErrorRateInsight`— Tipe `ApiErrorRateInsight` Insights menganalisis panggilan API manajemen yang menghasilkan kode kesalahan. Kesalahan

ditampilkan jika panggilan API tidak berhasil. Untuk menerima Wawasan tentang`ApiErrorRateInsight`, penyimpanan data peristiwa sumber harus mencatat peristiwa manajemen Tulis atau Baca.

iv. Ulangi dua langkah sebelumnya (ii dan iii) untuk menambahkan jenis Wawasan tambahan yang ingin Anda terima.

13. Pilih Berikutnya untuk meninjau pilihan Anda.
14. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
15. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.
16. Jika Anda tidak memilih penyimpanan data peristiwa sumber di langkah 10, ikuti langkah-langkah Untuk membuat penyimpanan data peristiwa sumber yang memungkinkan peristiwa Insights untuk membuat penyimpanan data acara sumber.

Untuk membuat penyimpanan data peristiwa sumber yang memungkinkan peristiwa Insights

Prosedur ini menunjukkan kepada Anda cara membuat penyimpanan data peristiwa sumber yang memungkinkan peristiwa Wawasan dan peristiwa manajemen log.

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, buka submenu Danau, lalu pilih Penyimpanan data acara.
3. Pilih Buat penyimpanan data acara.
4. Pada halaman Configure event data store, di Rincian umum, masukkan nama untuk penyimpanan data acara. Diperlukan nama.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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

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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya 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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko 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) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda 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 AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS

10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.

11. Pada halaman Pilih acara, pilih AWS acara, lalu pilih CloudTrailacara.

12. Dalam CloudTrail acara, biarkan acara Manajemen dipilih.

13. Agar penyimpanan data acara Anda mengumpulkan acara dari semua akun di AWS Organizations organisasi, pilih Aktifkan untuk semua akun di organisasi saya. Anda harus masuk ke akun manajemen agar organisasi dapat membuat penyimpanan data acara yang memungkinkan Wawasan.
14. Perluas Pengaturan tambahan untuk memilih apakah Anda ingin penyimpanan data acara mengumpulkan acara 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 menelan peristiwa saat dibuat.

    a. Pilih Sertakan hanya wilayah saat ini di penyimpanan data acara saya jika Anda hanya ingin menyertakan peristiwa yang dicatat di Wilayah saat ini. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda mencakup acara dari semua Wilayah.

    b. Biarkan acara Ingest dipilih.
15. Pilih jenis acara manajemen yang ingin Anda sertakan dalam penyimpanan data acara Anda. Anda dapat memilih Baca, Menulis, atau keduanya. Setidaknya satu diperlukan.

    > **Note**
    >
    > Untuk mencatat peristiwa Insights pada volume panggilan API, penyimpanan data peristiwa harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, penyimpanan data peristiwa harus mencatat `read` atau `write` mengelola peristiwa.
16. Anda dapat memilih untuk mengecualikan AWS Key Management Service atau peristiwa Amazon RDS Data API dari penyimpanan data acara Anda. Untuk informasi selengkapnya tentang opsi ini, lihat Acara manajemen logging.
17. Pilih Aktifkan Wawasan.
18. Di Aktifkan Wawasan, 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 acara tujuan yang mencatat peristiwa Wawasan.
19. 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.

20. Pilih Berikutnya untuk meninjau pilihan Anda.
21. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
22. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.

    Mulai saat ini, penyimpanan data acara menangkap peristiwa yang cocok dengan pemilih acara lanjutannya. Setelah mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data acara sumber Anda, diperlukan waktu hingga 7 hari untuk CloudTrail mengirimkan acara Insights pertama ke penyimpanan data acara tujuan Anda, jika aktivitas yang tidak biasa terdeteksi.

    Anda dapat melihat dasbor CloudTrail Danau untuk memvisualisasikan peristiwa Wawasan di penyimpanan data acara tujuan Anda. Untuk informasi lebih lanjut tentang dasbor Danau, lihatLihat dasbor Danau.

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.

Buat penyimpanan data acara untuk item AWS Config konfigurasi

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 acara, Anda dapat menghubungkan aturan yang tidak sesuai dengan pengguna dan sumber daya yang terkait dengan perubahan. Item konfigurasi mewakili point-in-time tampilan 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 ditangkap.

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 melakukan kueri di berbagai sumber data seperti CloudTrail peristiwa, item konfigurasi, dan evaluasi aturan. CloudTrail Kueri danau mencakup semua item AWS Config konfigurasi termasuk konfigurasi sumber daya dan riwayat kepatuhan.

Membuat penyimpanan data peristiwa untuk item konfigurasi tidak memengaruhi kueri AWS Config lanjutan yang ada, 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 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.

Batasan

Batasan berikut berlaku untuk penyimpanan data acara untuk item konfigurasi.

- Tidak ada dukungan untuk item konfigurasi khusus
- Tidak ada dukungan untuk pemfilteran acara menggunakan pemilih acara tingkat lanjut

Prasyarat

Sebelum Anda membuat penyimpanan data acara, siapkan AWS Config rekaman untuk semua akun dan Wilayah Anda. Anda dapat menggunakan Pengaturan Cepat, kemampuan AWS Systems Manager, untuk dengan cepat membuat perekam konfigurasi yang didukung oleh AWS Config.

> **Note**
>
> Anda 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 Mengelola Perekam Konfigurasi di Panduan AWS Config Pengembang.

Selain itu, tindakan berikut direkomendasikan, tetapi tidak diperlukan untuk membuat penyimpanan data acara.

- Siapkan bucket Amazon S3 untuk menerima snapshot konfigurasi berdasarkan permintaan dan riwayat konfigurasi. Untuk informasi selengkapnya tentang snapshot, lihat Mengelola Saluran Pengiriman dan Mengirimkan Snapshot Konfigurasi ke Bucket Amazon S3 di AWS Config Panduan Pengembang.
- Tentukan aturan yang ingin Anda gunakan AWS Config untuk mengevaluasi informasi kepatuhan untuk jenis sumber daya yang direkam. Beberapa pertanyaan sampel CloudTrail Danau AWS Config diperlukan Aturan AWS Config untuk 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 AWS Management Console 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, di Rincian umum, masukkan nama untuk penyimpanan data acara. Diperlukan nama.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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

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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

   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.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya 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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko 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) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda 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 AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS
10. Pilih Berikutnya.
11. Pada halaman Pilih acara, pilih AWS acara, lalu pilih item Konfigurasi.
12. 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 rekaman. Secara opsional, Anda dapat memilih Sertakan hanya wilayah saat ini di penyimpanan data acara saya untuk menyertakan hanya item konfigurasi yang ditangkap di Wilayah saat ini. Jika Anda tidak memilih opsi ini, penyimpanan data acara Anda menyertakan item konfigurasi dari semua Wilayah yang telah mengaktifkan perekaman.
13. Agar penyimpanan data acara Anda mengumpulkan item konfigurasi dari semua akun di 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.
14. Pilih Berikutnya untuk meninjau pilihan Anda.
15. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.

16. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.

    Dari titik ini ke depan, penyimpanan data acara menangkap item konfigurasi. Item konfigurasi yang terjadi sebelum Anda membuat penyimpanan data acara tidak ada di penyimpanan data acara.

Kueri Sampel

Anda sekarang dapat menjalankan kueri di penyimpanan data acara baru Anda. Tab Contoh kueri di CloudTrail konsol menyediakan contoh kueri untuk memulai. Berikut ini adalah beberapa contoh kueri yang dapat Anda jalankan terhadap penyimpanan data peristiwa item konfigurasi Anda.

Deskripsi	Query
Temukan pengguna mana yang melakukan tindakan yang menghasilkan status tidak sesuai dengan menggabungkan penyimpanan data peristiwa item konfigurasi dengan penyimpanan data CloudTrail peristiwa.	`SELECT element_at(config1.eventDat a.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventDat a.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM config_event_data_store_ID as config1 JOIN config_event_data_store_ID as config2 on element_at(config1 .eventData.configuration, 'targetRe sourceId') = config2.eventData. resourceId JOIN cloudtrail_event_data_store_ID as cloudtrail on config2.eventData. arn = element_at(cloudtrail.resou rces, 1).arn WHERE`

Deskripsi	Query
	`element_at(config1.eventDat a.configuration, 'configRuleList') is not null AND element_at(config1.eventDat a.configuration, 'complianceType') = 'NON_COMPLIANT' AND cloudtrail.eventTime > '2022-11-14 00:00:00' AND config2.eventData.resourceType = 'AWS::DynamoDB::Table'`

Deskripsi	Query

Temukan semua AWS Config aturan dan kembalikan status kepatuhan dari item konfigurasi yang dihasilkan dalam satu hari terakhir.	`SELECT`
	`    eventData.configuration,`
	` eventData.accountId, eventData`
	`.awsRegion,`
	`    eventData.resourceName, eventData`
	`.resourceCreationTime,`
	`    element_at(eventData.config`
	`uration,'complianceType') AS`
	` complianceType,`
	`    element_at(eventData.config`
	`uration, 'configRuleList') AS`
	` configRuleList,`
	`    element_at(eventData.config`
	`uration, 'resourceId') AS resourceI`
	`d,`
	`    element_at(eventData.config`
	`uration, 'resourceType') AS resourceT`
	`ype`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventData.resourceType =`
	` 'AWS::Config::ResourceCompliance'`
	`AND`
	`    eventTime > '2022-11-22 00:00:00'`
	`ORDER BY`
	`    eventData.resourceCreationTime`
	`DESC`
	`    limit 10`

Deskripsi	Query
Temukan jumlah total AWS Config sumber daya yang dikelompokkan berdasarkan jenis sumber daya, ID akun, dan Wilayah.	`SELECT eventData.resourceType, eventData.awsRegion, eventData.accountId, COUNT (*) AS resourceCount FROM config_event_data_store_ID WHERE eventTime > '2022-11-22 00:00:00' GROUP BY eventData.resourceType, eventData.awsRegion, eventData.accountId`
Temukan waktu pembuatan sumber daya untuk semua item AWS Config konfigurasi yang dihasilkan pada tanggal tertentu.	`SELECT eventData.configuration, eventData.accountId, eventData.awsRegion, eventData.resourceId, eventData.resourceName, eventData.resourceType, eventData.availabilityZone, eventData.resourceCreationTime FROM config_event_data_store_ID WHERE eventTime > '2022-11-16 00:00:00' AND eventTime < '2022-11-17 00:00:00' ORDER BY eventData.resourceCreationTime DESC limit 10;`

Untuk informasi selengkapnya tentang membuat dan mengedit kueri, lihatMembuat atau mengedit kueri.

Skema item konfigurasi

Tabel berikut menjelaskan elemen skema wajib dan opsional yang cocok dengan yang ada dalam catatan item konfigurasi. Isi `eventData` disediakan oleh item konfigurasi Anda; bidang lain disediakan oleh CloudTrail setelah konsumsi.

CloudTrail isi catatan acara dijelaskan secara lebih rinci dalamCloudTrail isi rekaman.

- Bidang yang disediakan oleh CloudTrail setelah konsumsi
- Bidang yang disediakan oleh acara Anda

Bidang yang disediakan oleh CloudTrail setelah konsumsi

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
eventVersion	string	Wajib	Versi format AWS acara.
EventKategori	string	Wajib	Kategori acara. Untuk item konfigurasi, nilai yang valid adalah`ConfigurationItem` .
eventType	string	Wajib	Jenis peristiwa. Untuk item konfigurasi, nilai yang valid adalah`AwsConfigurationItem` .
EventID	string	Wajib	ID unik untuk suatu acara.
eventTime	string	Wajib	Stempel waktu acara, dalam `yyyy-MM-DDTHH:mm:ss` format, dalam

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
			Waktu Terkoordinasi Universal (UTC).
awsRegion	string	Wajib	Tempat Wilayah AWS untuk menetapkan suatu acara.
recipientAccountId	string	Wajib	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 mencakup informasi yang hilang dan alasan mengapa itu hilang.

`eventData`Bidang di disediakan oleh item konfigurasi Anda

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
EventData	-	Wajib	Bidang di EventData disediakan oleh item konfigurasi Anda.
• configurationItemVersion	string	Opsional	Versi item konfigurasi dari sumbernya.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• configurationItemCaptureWaktu	string	Opsional	Waktu ketika perekaman konfigurasi dimulai.
• configurationItemStatus	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 ConfigurationItemdi Referensi AWS Config API.
• resourceId	string	Opsional	ID sumber daya (misalnya., sg-*xxxxxx*).
• Nama Sumber Daya	string	Opsional	Nama kustom sumber daya, jika tersedia.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• 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	Availability Zone yang terkait dengan sumber daya.
• resourceCreationTime	string	Opsional	Cap waktu saat sumber daya dibuat.
• konfigurasi	JSON	Opsional	Deskripsi konfigurasi sumber daya.
• SuplementaryConfiguration	JSON	Opsional	Atribut konfigurasi yang AWS Config mengembalikan jenis sumber daya tertentu untuk melengkapi informasi yang dikembalikan untuk parameter konfigurasi.
• RelateDevents	string	Opsional	Daftar ID CloudTrail acara.
• hubungan	-	Opsional	Daftar sumber AWS daya terkait.
• • name	string	Opsional	Jenis hubungan dengan sumber daya terkait.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• • resourceType	string	Opsional	Jenis sumber daya dari sumber daya terkait.
• • resourceId	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
     }
    }
  }
}
```

Buat penyimpanan data acara untuk acara di luar AWS

Anda dapat membuat penyimpanan data acara untuk menyertakan peristiwa di luar AWS, dan kemudian 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 hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat 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 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.

Untuk membuat penyimpanan data acara untuk acara di luar AWS

1. Masuk ke AWS Management Console 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, di Rincian umum, masukkan nama untuk penyimpanan data acara. Diperlukan nama.
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:

   - Harga retensi yang dapat diperpanjang satu tahun - Umumnya direkomendasikan jika Anda mengharapkan untuk menelan kurang dari 25 TB data acara 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 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 - Direkomendasikan jika Anda mengharapkan untuk menelan lebih dari 25 TB data acara 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
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 dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

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.

7. (Opsional) Untuk mengaktifkan enkripsi menggunakan AWS Key Management Service, pilih Gunakan milik saya 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, lihatKonfigurasikanAWS KMSkebijakan 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 Federasi toko 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.

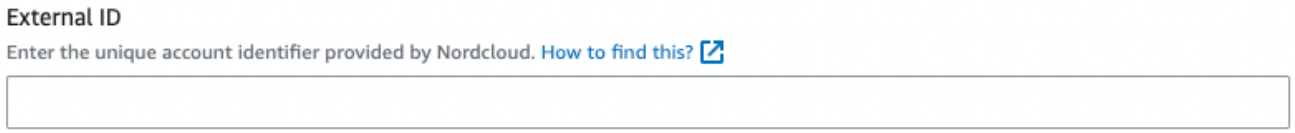
9. (Opsional) Di bagian Tag, Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Untuk informasi selengkapnya tentang cara menggunakan kebijakan IAM untuk mengotorisasi akses ke penyimpanan data peristiwa berdasarkan tag, lihat. Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag Untuk informasi selengkapnya tentang cara menggunakan tag AWS, lihat Menandai AWS sumber daya di. Referensi Umum AWS
10. Pilih Berikutnya untuk mengonfigurasi penyimpanan data acara.
11. Pada halaman Pilih acara, pilih Acara dari integrasi.
12. Dari Peristiwa dari integrasi, pilih sumber untuk mengirimkan acara ke penyimpanan data acara.
13. Berikan nama untuk mengidentifikasi saluran integrasi. Namanya bisa 3-128 karakter. Hanya huruf, angka, titik, garis bawah, dan tanda hubung yang diizinkan.
14. 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 prinsipal tertentu pada sumber daya dan dalam kondisi apa. 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 mereka mengizinkan tindakan tersebut. `cloudtrail-data:PutAuditEvents`

    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. Mitra integrasi menyediakan ID eksternal yang unik, seperti ID akun atau string yang dibuat secara acak, untuk digunakan untuk integrasi guna mencegah wakil yang bingung. Mitra bertanggung jawab untuk membuat dan menyediakan ID eksternal yang unik.

   Anda dapat memilih Bagaimana menemukan ini? untuk melihat dokumentasi mitra yang menjelaskan cara menemukan ID eksternal.



> **Note**
>
> Jika kebijakan resource 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 setiap ID AWS akun yang akan ditambahkan sebagai prinsipal dalam kebijakan.

15. Pilih Berikutnya untuk meninjau pilihan Anda.
16. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit untuk membuat perubahan pada bagian. Saat Anda siap membuat penyimpanan data acara, pilih Buat penyimpanan data acara.
17. Penyimpanan data acara baru terlihat di tabel penyimpanan data acara pada halaman penyimpanan data acara.
18. Berikan 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

Penyimpanan data acara mulai memasukkan peristiwa mitra ke dalam CloudTrail saluran integrasi saat Anda, mitra, atau aplikasi mitra memanggil `PutAuditEvents` API di saluran.

Salin peristiwa jejak ke penyimpanan data acara

Anda dapat menyalin peristiwa jejak 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. Untuk informasi selengkapnya tentang membuat penyimpanan data acara baru, lihatBuat penyimpanan data acara untuk CloudTrail acara.

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.
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
- Rincian salinan acara

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 (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 di Panduan Pengguna Amazon S3.

- 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. Akun administrator yang didelegasikan tidak dapat 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 *myBucketName*, *eventDataStoremyAccountID, region, prefix, dan Id* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

Ganti *key-region*, *keyAccountID, 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:::myBucketName"
      ],
      "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:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/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 *myAccountID*, *region*, dan *eventDataStoreArn* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* 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 *myBucketName*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:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

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 *roLearn*, *myBucketName*, *eventDataStoremyAccountID, region, dan Id* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* 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:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

Salin peristiwa jejak ke penyimpanan data acara yang ada

Gunakan prosedur berikut untuk menyalin peristiwa jejak ke penyimpanan data acara yang ada. Untuk informasi tentang cara membuat penyimpanan data acara baru, lihatBuat penyimpanan data acara untuk CloudTrail acara.

> **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 AWS Management Console 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 bahwa

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, lihatRincian salinan acara.

Rincian salinan acara

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 aktual untuk detail sepertiAwalan yang disalinmungkin lebih tinggi dari apa yang ditampilkan pada halaman. CloudTrail memperbarui detail secara bertahap selama salinan acara.

Untuk mengakses halaman detail salinan acara

1. Masuk keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi kiri, di bawahDanau, pilihPenyimpanan data acara.
3. Pilih toko data acara.
4. Pilih salinan acara diStatus salinan acarabagian.

Salin detail

DariSalin detail, Anda dapat melihat detail berikut tentang salinan acara jejak.

- Lokasi catatan acara S3- Lokasi bucket S3 sumber yang berisi file log peristiwa jejak.
- Salin ID- ID untuk salinan.
- Awalan yang disalin- Merupakan jumlah awalan S3 yang disalin. Selama salinan acara 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.
  - Dalam proses- Menunjukkan salinan acara jejak sedang berlangsung.

    > **Note**
    >
    > Anda tidak dapat menyalin peristiwa jejak jika salinan acara jejak lainnyaDalam proses. Untuk menghentikan salinan acara jejak, pilihHentikan salinan.

  - Berhenti- Menunjukkan aHentikan salinantindakan terjadi. Untuk mencoba kembali salinan acara jejak, pilihCoba lagi salin.
  - Gagal- Salinannya selesai, tetapi beberapa peristiwa jejak gagal disalin. Tinjau pesan kesalahan diKegagalan salinan. Untuk mencoba kembali salinan acara jejak, pilihCoba lagi salin. Ketika Anda mencoba lagi salinannya, CloudTrail melanjutkan 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.
- Selesai waktu- Menunjukkan kapan salinan acara jejak selesai atau dihentikan.

Kegagalan salinan

DariKegagalan salinan, 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 selainCloudTrail. Kemungkinan penyebab kegagalan lainnya terkait dengan masalah akses. Misalnya, jika bucket S3 penyimpanan data acara tidak memberikan CloudTrail akses untuk mengimpor acara, Anda akan mendapatkan`AccessDenied`kesalahan.

Untuk setiap kegagalan salinan, tinjau informasi kesalahan berikut.

- TheLokasi kesalahan- Menunjukkan lokasi di ember S3 di mana kesalahan terjadi. Jika terjadi kesalahan karena bucket S3 sumber berisi file yang tidak terkompresi,Lokasi kesalahanakan menyertakan awalan di mana Anda akan menemukan file itu.
- ThePesan kesalahan- Memberikan penjelasan mengapa kesalahan terjadi.
- TheJenis kesalahan- Menyediakan jenis kesalahan. Sebagai contoh, sebuahJenis kesalahandari`AccessDenied`, menunjukkan bahwa kesalahan terjadi karena masalah izin. Untuk informasi lebih lanjut tentang izin yang diperlukan untuk menyalin peristiwa jejak, lihatIzin yang diperlukan untuk menyalin peristiwa jejak.

Setelah menyelesaikan kegagalan, pilihCoba lagi salin. Ketika Anda mencoba lagi salinannya, CloudTrail melanjutkan salinan di lokasi di mana kegagalan terjadi.

Mengelola siklus hidup penyimpanan data acara

Berikut ini adalah tahapan siklus hidup penyimpanan data peristiwa:

- `CREATED`— Keadaan jangka pendek yang menunjukkan bahwa penyimpanan data acara telah dibuat.
- `ENABLED`— Penyimpanan data acara aktif dan menelan acara. Anda dapat menjalankan kueri dan menyalin peristiwa jejak ke penyimpanan data acara.
- `STARTING_INGESTION`— Keadaan jangka pendek yang menunjukkan bahwa penyimpanan data acara akan mulai menelan acara langsung.
- `STOPPING_INGESTION`— Keadaan jangka pendek yang menunjukkan bahwa penyimpanan data acara akan berhenti menelan acara langsung.

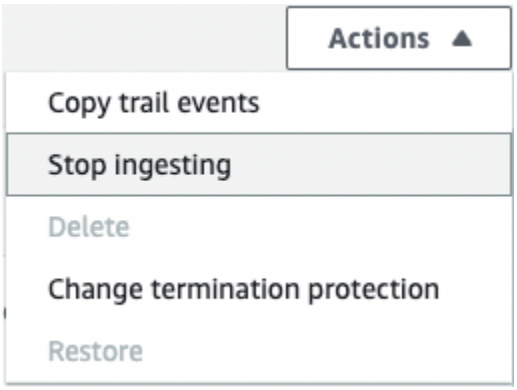
- `STOPPED_INGESTION`— Penyimpanan data acara tidak menelan acara langsung. Anda masih dapat menjalankan kueri pada acara apa pun yang sudah ada di penyimpanan data acara dan menyalin peristiwa jejak ke penyimpanan data acara.
- `PENDING_DELETION`— Penyimpanan data acara berada dalam `STOPPED_INGESTION` keadaan `ENABLED` atau dan telah dihapus tetapi dalam periode tunggu 7 hari sebelum penghapusan permanen. Anda tidak dapat menjalankan kueri pada penyimpanan data peristiwa, dan tidak ada operasi yang dapat dilakukan pada penyimpanan data peristiwa kecuali pemulihan.

Anda hanya dapat menghapus penyimpanan data acara jika perlindungan federasi dan penghentian dinonaktifkan. Perlindungan penghentian mencegah penyimpanan data peristiwa terhapus 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 acara, itu tetap dalam `PENDING_DELETION` keadaan selama 7 hari sebelum dihapus secara permanen. Anda dapat memulihkan penyimpanan data acara selama periode tunggu 7 hari. Saat berada di `PENDING_DELETION` negara bagian, 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 menelan peristiwa dan tidak menimbulkan biaya.

Tindakan yang tersedia di penyimpanan data acara

Untuk menghapus atau memulihkan penyimpanan data peristiwa, menyalin peristiwa jejak, memulai atau berhenti menelan peristiwa, atau mengaktifkan atau mematikan perlindungan penghentian penyimpanan data peristiwa, gunakan perintah pada menu Tindakan halaman detail penyimpanan data acara.



Opsi untuk Menyalin peristiwa jejak hanya tersedia di penyimpanan data acara yang berisi peristiwa CloudTrail manajemen dan data. Opsi untuk Mulai konsumsi dan Hentikan konsumsi hanya tersedia di penyimpanan data acara yang berisi peristiwa (CloudTrail peristiwa manajemen dan data), atau item konfigurasi. AWS Config

Memperbarui penyimpanan data acara

Bagian ini menjelaskan cara memperbarui pengaturan penyimpanan data acara menggunakan AWS Management Console. Untuk informasi tentang cara memperbarui penyimpanan data acara menggunakan AWS CLI, lihatPerbarui penyimpanan data acara dengan AWS CLI.

Untuk memperbarui penyimpanan data acara

1. Masuk ke AWS Management Console 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 untuk mengubah pengaturan berikut:

   - Nama penyimpanan data acara - Ubah nama yang mengidentifikasi penyimpanan data acara Anda.
   - Opsi harga - Untuk penyimpanan data acara menggunakan opsi penetapan harga retensi tujuh tahun, Anda dapat memilih untuk menggunakan harga retensi yang dapat diperpanjang satu tahun sebagai gantinya. Kami merekomendasikan harga retensi yang dapat diperpanjang satu tahun untuk penyimpanan data acara yang menelan kurang dari 25 TB data acara setiap bulan. Kami juga merekomendasikan harga retensi yang dapat diperpanjang satu tahun jika Anda mencari periode retensi yang fleksibel hingga 10 tahun. Untuk informasi lebih lanjut, lihat AWS CloudTrail Harga danMengelola biaya CloudTrail Danau.

     > **Note**
     >
     > Anda tidak dapat mengubah opsi harga untuk penyimpanan data acara yang menggunakan harga retensi yang dapat diperpanjang satu tahun. Jika Anda ingin menggunakan harga retensi tujuh tahun, hentikan konsumsi pada penyimpanan data acara Anda saat ini. Kemudian buat penyimpanan data acara baru dengan opsi harga retensi tujuh tahun.

- Periode retensi - Ubah periode retensi untuk penyimpanan data acara. Periode retensi menentukan berapa lama data peristiwa disimpan di penyimpanan data acara. Periode retensi dapat antara 7 hari dan 3.653 hari (sekitar 10 tahun) untuk opsi harga retensi yang dapat diperpanjang satu tahun, atau antara 7 hari dan 2.557 hari (sekitar tujuh tahun) untuk opsi harga retensi tujuh tahun.

  > **Note**
  >
  > Jika Anda mengurangi periode retensi penyimpanan data acara, CloudTrail akan menghapus setiap 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.

- 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 acara 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 hanya menyertakan peristiwa yang masuk saat ini Wilayah AWS, pilih Sertakan di 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 acara dari semua akun di 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 CloudTrailperistiwa atau item Konfigurasi.

Pilih Simpan perubahan setelah selesai.

5. Di federasi kueri Danau, pilih Edit untuk mengaktifkan atau menonaktifkan federasi kueri Danau. Mengaktifkan federasi kueri Lake memungkinkan Anda melihat metadata untuk penyimpanan data acara di Katalog AWS Glue Data dan menjalankan kueri SQL pada data peristiwa

menggunakan Amazon Athena. Menonaktifkan federasi kueri Lake menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Danau, Anda tidak dapat lagi menanyakan data Anda di Athena. Tidak ada data CloudTrail Danau yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Danau.

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 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 ada, pilih peran yang ingin Anda gunakan. Peran harus ada di akun Anda.

Pilih Simpan perubahan setelah Anda selesai.

6. Edit pengaturan tambahan apa pun untuk jenis Acara Anda.

Jenis peristiwa	Pengaturan yang dapat diedit
CloudTrail acara	Anda dapat mengedit pengaturan berikut untuk CloudTrail acara: • Untuk mengubah peristiwa yang menyimpan log data acara Anda, pilih Edit dalam CloudTrail acara. • Di acara Manajemen, pilih Edit untuk mengubah pengaturan acara manajemen. Untuk informasi lebih lanjut, lihat Pencatatan acara manajemen dengan AWS Management Console (langkah 3). • Dalam peristiwa Data, pilih Edit untuk mengubah pengaturan peristiwa data. Anda dapat memilih jenis peristiwa data

Jenis peristiwa	Pengaturan yang dapat diedit
	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 di AWS Management Console. Pilih Simpan perubahan setelah selesai.
Acara dari integrasi	Dalam Integrasi, pilih integrasi Anda. Kemudian pilih Edit untuk mengubah pengaturan berikut: • Dalam detail Integrasi, ubah nama yang mengidentifikasi saluran integrasi Anda. • Di lokasi pengiriman acara, pilih tujuan acara Anda. • Dalam Kebijakan sumber daya, konfigura sikan kebijakan sumber daya untuk saluran integrasi. Pilih Simpan perubahan setelah selesai. Untuk informasi selengkapnya tentang pengaturan ini, lihat Buat integrasi dengan sumber acara di luar AWS.

7. Untuk menambah, mengubah, atau menghapus tag, pilih Edit di Tag. Anda dapat menambahkan hingga 50 pasangan kunci tag untuk membantu Anda mengidentifikasi, mengurutkan, dan mengontrol akses ke penyimpanan data acara Anda. Pilih Simpan perubahan setelah selesai.

Hentikan dan mulai konsumsi acara

Secara default, penyimpanan data acara dikonfigurasi untuk menelan peristiwa. Anda dapat menghentikan penyimpanan data peristiwa dari menelan peristiwa dengan menggunakan konsol, AWS CLI, atau API.

Opsi untuk Mulai konsumsi dan Hentikan konsumsi hanya tersedia di penyimpanan data acara yang berisi peristiwa (CloudTrail peristiwa manajemen dan data), atau item konfigurasi. AWS Config

Saat Anda menghentikan konsumsi pada penyimpanan data peristiwa, status penyimpanan data acara 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 acara (jika hanya berisi peristiwa CloudTrail manajemen atau data).

Untuk menghentikan penyimpanan data acara dari menelan acara

1. Masuk ke AWS Management Console 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.
4. Dari Tindakan, pilih Hentikan konsumsi.
5. Saat Anda diminta untuk mengonfirmasi, pilih Hentikan konsumsi. Penyimpanan data acara akan berhenti menelan acara langsung.
6. Untuk melanjutkan konsumsi, pilih Mulai konsumsi.

Untuk memulai ulang konsumsi acara

1. Masuk ke AWS Management Console 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.
4. Dari Tindakan, pilih Mulai konsumsi.

Federasi toko data acara

Menggabungkan penyimpanan data peristiwa memungkinkan Anda melihat metadata yang terkait dengan penyimpanan data peristiwa di Katalog Data, mendaftarkan Katalog AWS Glue Data dengan AWS Lake Formation, dan memungkinkan Anda menjalankan kueri SQL terhadap data peristiwa Anda 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 EnableFederationAPI. Saat Anda mengaktifkan federasi kueri Lake, CloudTrail buat database terkelola bernama `aws:cloudtrail` (jika database belum ada) dan tabel federasi terkelola dalam Katalog AWS Glue Data. ID penyimpanan data acara digunakan untuk nama tabel. CloudTrail mendaftarkan peran federasi ARN dan penyimpanan data acara AWS Lake Formationdi, 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 ada. Lake Formation menggunakan peran ini untuk mengelola izin penyimpanan data acara 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 DisableFederationAPI. Saat Anda menonaktifkan federasi, CloudTrail menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Danau, Anda tidak dapat lagi menanyakan data acara Anda di Athena. Tidak ada data CloudTrail Danau yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Danau.

Tidak ada CloudTrail biaya untuk federasi penyimpanan data acara CloudTrail Lake. Ada biaya untuk menjalankan kueri di Amazon Athena. Untuk informasi lebih lanjut tentang harga Athena, lihat Harga Amazon Athena.

Topik

- Pertimbangan
- Izin yang diperlukan untuk federasi
- Aktifkan federasi kueri Danau

- Nonaktifkan federasi kueri Lake
- Mengelola sumber daya federasi CloudTrail Danau dengan AWS Lake Formation

Pertimbangan

Pertimbangkan faktor-faktor berikut saat menggabungkan penyimpanan data acara:

- Tidak ada CloudTrail biaya untuk federasi penyimpanan data acara CloudTrail Lake. Ada biaya untuk menjalankan kueri di Amazon Athena. Untuk informasi lebih lanjut tentang harga Athena, lihat Harga Amazon Athena.
- Lake Formation 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 Lake Formation, 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: AmazonAthenaFullAccessmemungkinkan tindakan ini. Jika Anda menggunakan kebijakan inline, pastikan untuk memperbarui kebijakan izin untuk mengizinkan tindakan ini. Untuk informasi selengkapnya, lihat Mengelola 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 kumpulan data di Amazon QuickSight, Anda harus memilih opsi Use custom SQL. Untuk informasi selengkapnya, lihat Membuat kumpulan data menggunakan data Amazon Athena.
- Jika federasi diaktifkan, Anda tidak dapat menghapus penyimpanan data acara. Untuk menghapus penyimpanan data acara federasi, Anda harus terlebih dahulu menonaktifkan federasi dan perlindungan penghentian 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 lain yang didelegasikan 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 membuat federasi penyimpanan data acara, 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 federasi 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, 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 memberikan izin yang diperlukan untuk mengaktifkan federasi. Bagian ini memberikan contoh izin peran IAM dan kebijakan kepercayaan yang diperlukan.

Contoh berikut memberikan kebijakan izin untuk peran federasi. Untuk pernyataan pertama berikan ARN lengkap dari penyimpanan data acara Anda untuk. `Resource`

Pernyataan kedua dalam kebijakan ini memungkinkan Lake Formation untuk mendekripsi data untuk penyimpanan data peristiwa yang dienkripsi dengan kunci KMS. Ganti *`key-region`*, *`account-id`*, *`dan key-id`* dengan nilai untuk kunci KMS Anda. Anda dapat menghilangkan pernyataan ini jika penyimpanan data acara Anda tidak menggunakan kunci KMS untuk enkripsi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
```

```
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

Contoh berikut memberikan kebijakan kepercayaan IAM, yang memungkinkan AWS Lake Formation untuk mengambil peran IAM untuk mengelola izin untuk penyimpanan data acara federasi.

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

Izin yang diperlukan untuk mengaktifkan federasi

Kebijakan contoh berikut memberikan izin minimum yang diperlukan untuk mengaktifkan federasi pada penyimpanan data acara. Kebijakan ini memungkinkan CloudTrail untuk mengaktifkan federasi pada penyimpanan data acara, AWS Glue untuk membuat sumber daya federasi dalam Katalog AWS Glue Data, dan AWS Lake Formation mengelola pendaftaran sumber daya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
```

```
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Izin yang diperlukan untuk menonaktifkan federasi

Contoh kebijakan berikut menyediakan sumber daya minimum yang diperlukan untuk menonaktifkan federasi pada penyimpanan data acara. Kebijakan ini memungkinkan CloudTrail untuk menonaktifkan federasi pada penyimpanan data peristiwa, AWS Glue menghapus tabel federasi terkelola dalam Katalog AWS Glue Data, dan Lake Formation untuk membatalkan pendaftaran sumber daya federasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "Allow Lake Formation to deregister the resource",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Aktifkan federasi kueri Danau

Anda dapat mengaktifkan federasi kueri Lake dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi EnableFederationAPI. Saat Anda mengaktifkan federasi kueri Lake, CloudTrail buat database terkelola bernama `aws:cloudtrail` (jika database belum ada) dan tabel federasi terkelola dalam Katalog AWS Glue Data. ID penyimpanan data acara digunakan untuk nama tabel.

CloudTrail mendaftarkan peran federasi ARN dan penyimpanan data acara AWS Lake Formationdi, 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 kepada Anda cara mengaktifkan federasi kueri Lake pada penyimpanan data acara yang ada.

1. Masuk ke AWS Management Console 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. Ini membuka halaman detail toko data acara.
4. Di federasi kueri Danau, pilih Edit lalu 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 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 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, 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 kueri Lake

Anda dapat menonaktifkan federasi dengan menggunakan CloudTrail konsol, AWS CLI, atau operasi DisableFederationAPI. Saat Anda menonaktifkan federasi, CloudTrail menonaktifkan integrasi dengan AWS Glue, AWS Lake Formation, dan Amazon Athena. Setelah menonaktifkan federasi kueri Danau, Anda tidak dapat lagi menanyakan data acara Anda di Athena. Tidak ada data CloudTrail Danau yang dihapus saat Anda menonaktifkan federasi dan Anda dapat terus menjalankan kueri di CloudTrail Danau.

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 acara yang ada.

1. Masuk ke AWS Management Console 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. Ini membuka halaman detail toko 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 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.

Mengelola sumber daya federasi CloudTrail Danau dengan AWS Lake Formation

Saat Anda menggabungkan penyimpanan data acara, CloudTrail mendaftarkan peran federasi ARN dan penyimpanan data acara AWS Lake Formation, layanan yang bertanggung jawab untuk mengizinkan kontrol akses berbutir halus dari sumber daya federasi dalam Katalog Data. AWS Glue Bagian ini menjelaskan bagaimana Anda dapat menggunakan Lake Formation untuk mengelola sumber daya federasi CloudTrail Danau.

Saat Anda mengaktifkan federasi, CloudTrail buat sumber daya berikut di Katalog AWS Glue Data.

- Database terkelola - CloudTrail membuat 1 database dengan nama `aws:cloudtrail` per akun. CloudTrail mengelola database. Anda tidak dapat menghapus atau memodifikasi database di AWS Glue.
- Tabel federasi terkelola - CloudTrail membuat 1 tabel untuk setiap penyimpanan data acara 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 terkelola.

- Kontrol akses hanya IAM - Dengan kontrol akses hanya 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 IAM.

  Pada konsol Lake Formation, metode ini muncul sebagai Gunakan hanya kontrol akses IAM.

> **Note**
>
> Jika Anda ingin membuat filter data dan menggunakan fitur Lake Formation lainnya, Anda harus menggunakan kontrol akses Lake Formation.

- Kontrol akses Lake Formation — Metode ini memberikan keuntungan sebagai berikut.
  - Anda dapat menerapkan keamanan tingkat kolom, tingkat baris, dan tingkat sel dengan membuat filter data.
  - Database dan tabel hanya dapat dilihat oleh administrator Lake Formation dan pencipta 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 berbutir halus.

Menentukan metode izin untuk sumber daya federasi

Saat Anda mengaktifkan federasi untuk pertama kalinya, CloudTrail buat database terkelola dan tabel federasi terkelola menggunakan pengaturan danau data Lake Formation Anda.

Setelah CloudTrail mengaktifkan federasi, Anda dapat memverifikasi metode izin yang Anda gunakan untuk database terkelola dan tabel federasi terkelola dengan memeriksa izin untuk sumber daya tersebut. Jika `ALL` (Super) ke `IAM_ALLOWED_PRINCIPALS` pengaturan hadir untuk sumber daya, sumber daya dikelola secara eksklusif oleh izin IAM. Jika pengaturan tidak ada, sumber daya dikelola oleh izin Lake Formation. Untuk informasi selengkapnya tentang izin Lake Formation, lihat referensi izin Lake Formation.

Metode izin untuk database terkelola dan tabel federasi terkelola dapat berbeda. Misalnya, jika Anda memeriksa nilai untuk database dan tabel, Anda bisa melihat yang berikut:

- Untuk database, nilai yang menetapkan `ALL` (Super) `IAM_ALLOWED_PRINCIPALS` hadir dalam izin yang menunjukkan bahwa Anda menggunakan kontrol akses IAM hanya untuk database.
- Untuk tabel, nilai yang menetapkan `ALL` (Super) untuk `IAM_ALLOWED_PRINCIPALS` tidak hadir, yang menunjukkan kontrol akses oleh izin Lake Formation.

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.

Berbagi lintas akun menggunakan Lake Formation

Bagian ini menjelaskan cara membagikan database terkelola dan tabel federasi terkelola di seluruh akun dengan menggunakan Lake Formation.

Anda dapat membagikan 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 Lake Formation.
3. Berikan `Describe` izin ke akun eksternal pada database.
4. Jika sumber daya Katalog Data dibagikan dengan 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 individu tabel federasi terkelola dengan akun eksternal dengan mengambil 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 Lake Formation.
3. (Opsional) Tentukan filter data apa pun untuk membatasi kolom atau baris.
4. Berikan `Select` izin ke akun eksternal di atas meja.
5. Jika sumber daya Katalog Data dibagikan dengan 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

Ubah perlindungan penghentian

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 acara, Anda harus menonaktifkan perlindungan penghentian. Anda dapat menonaktifkan perlindungan terminasi dengan menggunakan AWS Management Console, AWS CLI, atau operasi API.

Untuk mematikan perlindungan terminasi

1. Masuk ke AWS Management Console 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.
4. Dari Tindakan, pilih Ubah perlindungan penghentian.
5. Pilih Dinonaktifkan.
6. Pilih Simpan. Anda sekarang dapat menghapus penyimpanan data acara.

Untuk mengaktifkan perlindungan terminasi

1. Masuk ke AWS Management Console 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.
4. Dari Tindakan, pilih Ubah perlindungan penghentian.
5. Untuk mengaktifkan perlindungan penghentian, pilih Diaktifkan.
6. Pilih Simpan.

Hapus penyimpanan data acara

Bagian ini menjelaskan cara menghapus penyimpanan data acara menggunakan AWS CloudTrail konsol. Untuk informasi tentang cara menghapus penyimpanan data acara 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, CloudTrail memungkinkan perlindungan penghentian untuk melindungi penyimpanan data peristiwa agar tidak terhapus secara tidak sengaja.
> Untuk menghapus penyimpanan data peristiwa dengan jenis acara 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. Lihat informasi yang lebih lengkap di Hapus saluran untuk menghapus integrasi dengan AWS CLI

Untuk menghapus penyimpanan data acara

1. Masuk ke AWS Management Console 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.
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 acara berubah menjadi `PENDING_DELETION` dan tetap dalam keadaan itu selama 7 hari. Anda dapat memulihkan penyimpanan data acara selama periode tunggu 7 hari. Saat berada di `PENDING_DELETION` negara bagian, 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 menelan peristiwa dan tidak menimbulkan biaya.

Mengembalikan penyimpanan data acara

Setelah Anda menghapus penyimpanan data acara di AWS CloudTrail Lake, statusnya berubah menjadi `PENDING_DELETION` dan tetap dalam keadaan itu selama 7 hari. Selama waktu ini, Anda dapat memulihkan penyimpanan data peristiwa dengan menggunakan AWS Management Console, AWS CLI, atau operasi RestoreEventDataStoreAPI.

Bagian ini menjelaskan cara memulihkan penyimpanan data acara menggunakan konsol. Untuk informasi tentang cara memulihkan penyimpanan data acara menggunakan AWS CLI, lihatKembalikan penyimpanan data acara dengan AWS CLI.

Untuk memulihkan penyimpanan data acara

1. Masuk ke AWS Management Console 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.
4. Dari Tindakan, pilih Pulihkan.

Menyimpan data acara organisasi

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]
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
Lihat dasbor CloudTrail Lake untuk penyimpan an data acara organisasi.	Ya	Ya

[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 AWS Management Console 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.

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
```

Lihat juga

- Administrator yang didelegasikan organisasi
- Menambahkan administrator yang CloudTrail didelegasikan
- Menghapus administrator yang CloudTrail didelegasikan

Buat integrasi dengan sumber acara di luar AWS

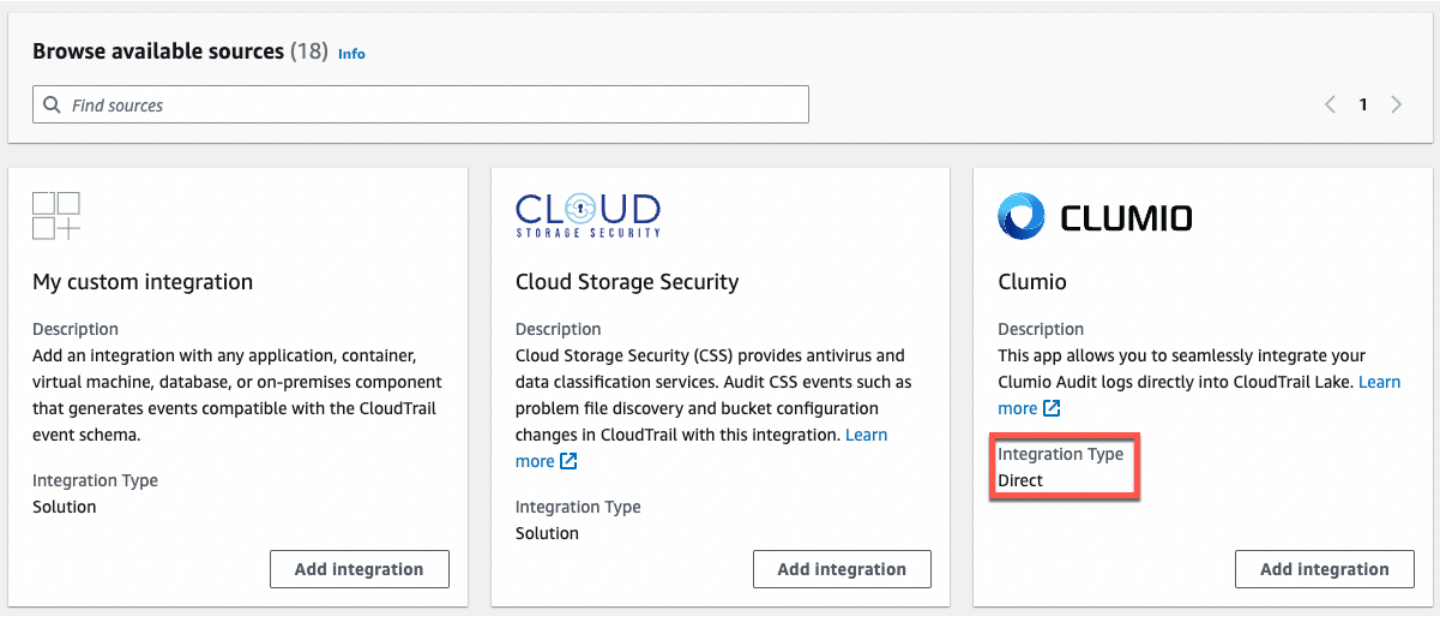
Anda dapat menggunakan CloudTrail untuk mencatat dan menyimpan data aktivitas pengguna dari sumber apa pun di lingkungan hybrid Anda, seperti aplikasi internal atau SaaS yang dihosting di tempat atau di cloud, mesin virtual, atau wadah. Anda dapat menyimpan, mengakses, menganalisis, memecahkan masalah, 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 luarAWS, Anda dapat memilih salah satu mitra ini sebagai sumber acara Anda, atau memilih Integrasi kustom saya untuk mengintegrasikan peristiwa dari sumber Anda sendiri 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
- Buat integrasi kustom
- Informasi tambahan tentang mitra integrasi
- CloudTrail Skema acara integrasi danau

Buat integrasi dengan CloudTrail mitra

Saat Anda membuat integrasi dengan sumber acara di luarAWS, 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 AWS Management Console 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.

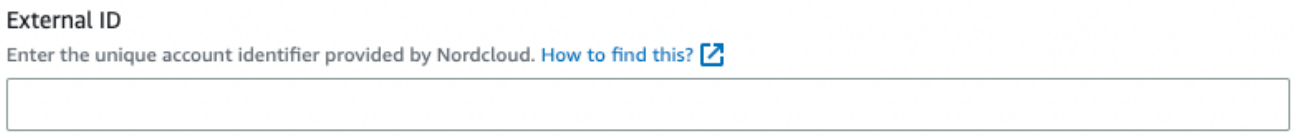
   Jika Anda memilih untuk mencatat peristiwa aktivitas ke satu atau beberapa penyimpanan data peristiwa yang ada, pilih penyimpanan data acara dari daftar. Penyimpanan data acara hanya dapat menyertakan peristiwa aktivitas. Jenis acara di konsol harus Peristiwa dari integrasi. Di API, `eventCategory` nilainya 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 prinsipal tertentu pada sumber daya dan dalam kondisi apa. 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 mereka mengizinkan tindakan tersebut. `cloudtrail-data:PutAuditEvents`

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. Mitra integrasi menyediakan ID eksternal yang unik, seperti ID akun atau string yang dibuat secara acak, untuk digunakan untuk integrasi guna mencegah wakil yang bingung. Mitra bertanggung jawab untuk membuat dan menyediakan 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 tagAWS, 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 kustom

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 wadah. 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 AWS Management Console 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 dapat diperpanjang satu tahun, atau hingga 2.557 hari (sekitar 7 tahun) jika Anda memilih opsi harga retensi tujuh tahun.

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 prinsipal tertentu pada sumber daya dan dalam kondisi apa. 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 tagAWS, 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 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`.

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 Cloud Storage	`CloudStorageSecurityConsole`	solusi
Clumio	`Clumio`	langsung
CrowdStrike	`CrowdStrike`	solusi
CyberArk	`CyberArk`	solusi
GitHub	`GitHub`	solusi
Hongkong 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 AWS Management Console 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 isi rekaman.

- Bidang yang disediakan oleh CloudTrail setelah konsumsi
- Bidang yang disediakan oleh acara Anda

Bidang yang 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	Tipe peristiwa. Untuk AWS non-

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
			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 Waktu Terkoordinasi Universal (UTC).
awsRegion	string	Diperlukan	Di Wilayah AWS mana `PutAuditEvents` panggilan itu dibuat.
recipientAccountId	string	Diperlukan	Merupakan ID akun yang menerima acara ini. CloudTrail mengisi bidang ini dengan menghitungnya dari payload acara.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
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.
• UpdatedFields	string	Opsional	Bidang catatan acara yang diperbarui oleh addendum. Ini hanya disediakan jika alasannyaUPDATED_DATA .
• OriginaLuid	string	Opsional	Event asli UID dari sumbernya. Ini hanya disediakan jika alasannyaUPDATED_DATA .
• OriginalEventid	string	Opsional	ID acara asli. Ini hanya disediakan jika alasannyaUPDATED_DATA .

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
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 yang 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

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
			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.
• 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.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• 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` format, dalam Waktu Terkoordinasi Universal (UTC).
• 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.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• 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.
• 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.

Nama bidang	Jenis masukan	Persyaratan	Deskripsi
• recipientAccountId	string	Diperlukan	Merupakan ID akun yang menerima acara ini. ID akun harus sama dengan ID AWS akun yang memiliki saluran.
• additionalEventData	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
        }
    }
}
```

Lihat dasbor Danau

Anda dapat menggunakan dasbor CloudTrail Danau untuk memvisualisasikan peristiwa di penyimpanan data acara. Anda dapat memilih dari beberapa jenis dasbor yang berbeda. Jenis dasbor yang tersedia untuk penyimpanan data acara bergantung pada konfigurasi pemilih acara lanjutan dari penyimpanan data acara. Misalnya, jika tipe dasbor menampilkan informasi tentang peristiwa CloudTrail manajemen, Anda hanya dapat memilih dasbor jika penyimpanan data acara yang dipilih saat ini mengumpulkan peristiwa CloudTrail manajemen.

Setiap jenis dasbor terdiri dari beberapa widget dan setiap widget mewakili kueri SQL. Untuk melihat kueri widget, pilih Lihat dan analisis di editor kueri untuk membuka editor kueri. Anda tidak dapat

memodifikasi kueri yang dihasilkan sistem yang digunakan untuk mengisi widget, tetapi Anda dapat mengedit kueri dan menjalankan kueri di editor kueri untuk analisis lebih lanjut.

Untuk mengisi dan memperbarui dasbor, pilih Jalankan kueri. Saat Anda memilih Jalankan kueri, CloudTrail jalankan kueri yang dihasilkan sistem atas nama Anda. Karena menjalankan kueri menimbulkan biaya, CloudTrail meminta Anda untuk mengetahui biaya yang terkait dengan menjalankan kueri. Ini adalah konfirmasi satu kali. Untuk informasi selengkapnya tentang CloudTrail harga, lihat CloudTrail Harga.

Topik

Batasan

Batasan berikut berlaku untuk rilis saat ini.

- Rilis saat ini tidak mendukung dasbor, widget, atau kueri yang disesuaikan.
- Rilis saat ini hanya menyediakan dasbor untuk penyimpanan data peristiwa yang mengumpulkan CloudTrail peristiwa (peristiwa data, peristiwa manajemen) dan peristiwa Wawasan.
- Rilis saat ini tidak mendukung pengeditan kueri yang dihasilkan sistem yang digunakan untuk mengisi dasbor. Anda dapat melihat dan mengedit kueri dasar untuk widget apa pun di tab Editor Kueri, namun, setiap perubahan yang Anda buat pada kueri dimaksudkan untuk analisis tambahan di luar dasbor.

Prasyarat

Prasyarat berikut berlaku untuk dasbor Danau.

- 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, lihatBuat penyimpanan data acara untuk CloudTrail acara. Untuk

informasi tentang membuat penyimpanan data acara menggunakanAWS CLI, lihatMengelola CloudTrail Danau dengan menggunakan AWS CLI.

- Untuk mengisi dasbor, CloudTrail jalankan kueri atas nama Anda. Saat pertama kali Anda melihat halaman Dasbor, CloudTrail meminta Anda untuk mengetahui biaya yang terkait dengan menjalankan kueri. Pilih Saya setuju untuk mengakui biaya menjalankan kueri.

Memilih dasbor

Gunakan prosedur berikut untuk memilih penyimpanan data acara dan jenis dasbor untuk dilihat.

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi kiri, di bawah Danau, pilih Dasbor.
3. Pilih penyimpanan data acara yang ingin Anda visualisasikan datanya.
4. Pilih jenis dasbor yang ingin Anda lihat. Daftar dasbor diisi berdasarkan konfigurasi pemilih acara lanjutan dari penyimpanan data acara yang dipilih.

   Berikut ini adalah jenis dasbor yang mungkin.

   - Dasbor Ikhtisar - Menampilkan pengguna yang paling aktifWilayah AWS,, dan Layanan AWS berdasarkan jumlah acara. Anda juga dapat melihat informasi tentang `read` dan `write` mengelola aktivitas acara, sebagian besar peristiwa yang dibatasi, dan kesalahan teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
   - Dasbor Acara Manajemen - Menampilkan peristiwa masuk konsol, mengakses peristiwa yang ditolak, tindakan destruktif, dan kesalahan teratas oleh pengguna. Anda juga dapat melihat informasi tentang versi TLS dan panggilan TLS yang sudah ketinggalan zaman oleh pengguna. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan acara manajemen.
   - Dasbor Acara Data S3 - Menampilkan aktivitas akun S3, objek S3 yang paling banyak diakses, pengguna S3 teratas, dan tindakan S3 teratas. Dasbor ini tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa data Amazon S3.
   - Dasbor Insights Events - Menunjukkan proporsi keseluruhan peristiwa Insights menurut jenis Insights, proporsi peristiwa Insights menurut jenis Insights untuk pengguna dan layanan teratas, dan jumlah acara Insights per hari. Dasbor juga menyertakan widget yang mencantumkan hingga 30 hari acara Insights. Dasbor ini hanya tersedia untuk penyimpanan data acara yang mengumpulkan peristiwa 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. Untuk informasi selengkapnya, lihat Memahami penyampaian acara Wawasan.
> - 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 Wawasan. `ApiErrorRateInsight`

5. 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 lebih lanjut tentang harga CloudTrail , lihat Harga AWS CloudTrail.

6. Pilih Jalankan kueri untuk menjalankan kueri widget dasbor.

Memfilter dasbor pada rentang tanggal atau waktu

Secara default, dasbor menampilkan data selama 24 jam terakhir. Anda dapat memfilter 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.

Setelah memilih rentang waktu, pilih Jalankan kueri untuk menyegarkan dasbor.

> **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 lebih lanjut tentang harga CloudTrail , lihat Harga AWS CloudTrail.

Melihat kueri untuk widget dasbor

Setiap widget mewakili query SQL. Untuk melihat kueri widget, pilih Lihat dan analisis di editor kueri untuk membuka editor kueri. Dengan menggunakan editor kueri, Anda dapat menyempurnakan kueri di luar dasbor dan menjalankan kueri untuk melihat hasil kueri yang diperbarui. Untuk informasi selengkapnya tentang bekerja dengan kueri, lihatMembuat atau mengedit kueri.

> **Note**
>
> Anda tidak dapat memodifikasi kueri yang dihasilkan sistem untuk widget dasbor. Setiap perubahan yang dilakukan pada kueri pada tab Editor Kueri dimaksudkan semata-mata untuk analisis lebih lanjut di luar dasbor.

Pertanyaan danau

Pertanyaan di CloudTrail Lake 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. 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 (sepertiSELECT * 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'
```

Topik

- Membuat atau mengedit kueri
- Kueri contoh
- Jalankan kueri dan simpan hasil kueri
- Lihat hasil kueri
- Dapatkan dan unduh hasil kueri yang disimpan
- Memvalidasikan hasil kueri yang disimpan

Membuat atau mengedit kueri

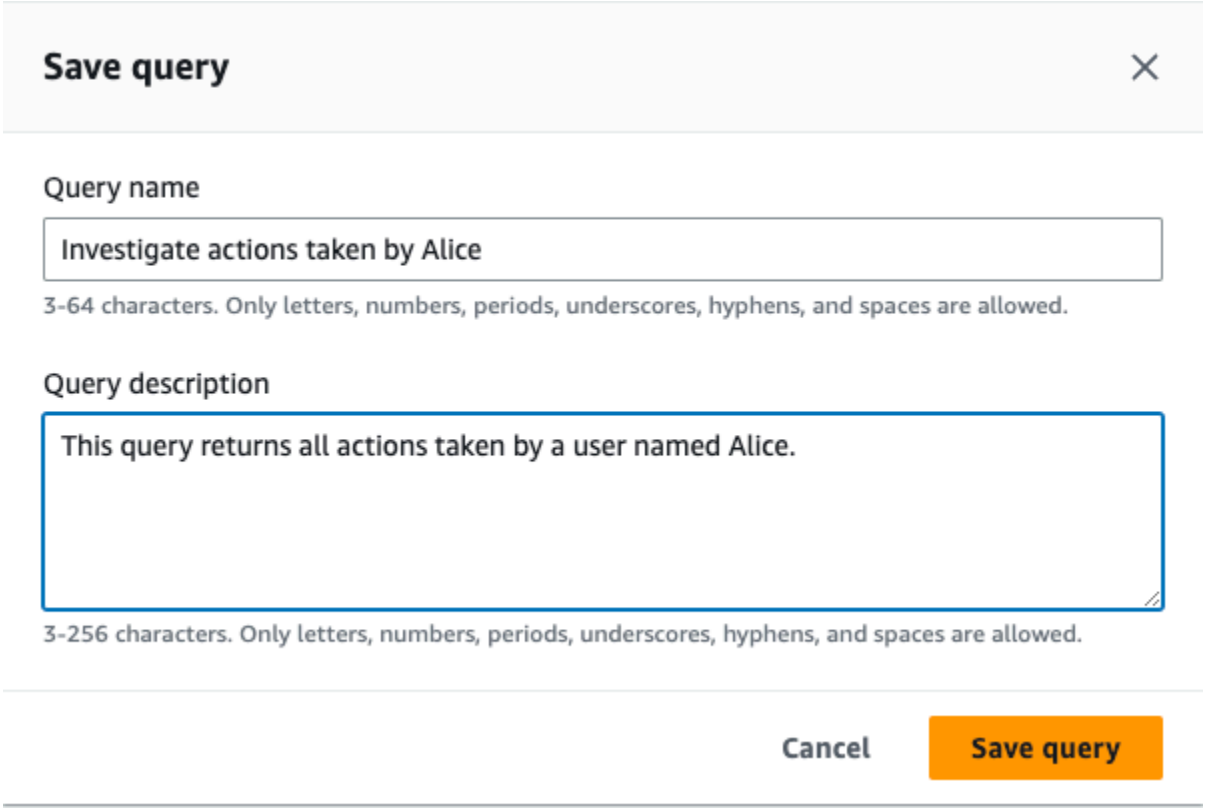
Dalam panduan ini, kami membuka salah satu contoh kueri, mengeditnya untuk menemukan tindakan yang diambil oleh pengguna tertentu bernama`Alice`, dan menyimpannya sebagai kueri baru. Anda juga dapat mengedit kueri tersimpan di tab Kueri tersimpan, jika Anda telah menyimpan kueri. Untuk membantu mengontrol biaya, sebaiknya Anda membatasi kueri dengan menambahkan stempel `eventTime` waktu mulai dan berakhir ke kueri.

1. Masuk ke AWS Management Console 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
   ```

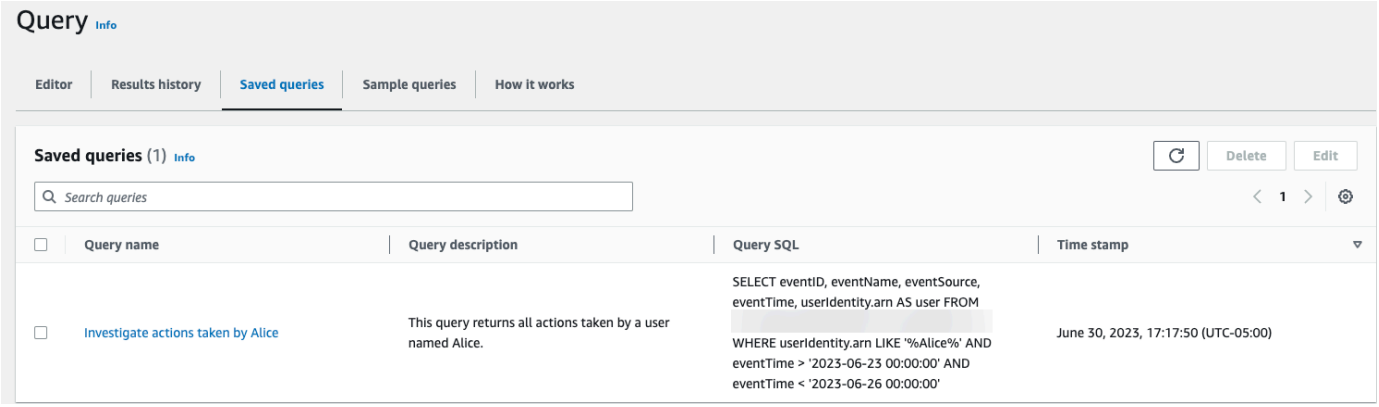
```
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

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.



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.
- Komentar/batalkan komentar dipilih - Komentar bagian yang dipilih dari kueri jika belum dikomentari. Jika bagian yang dipilih sudah dikomentari, memilih opsi ini akan menghapus komentar.

Kueri contoh

Bagian ini menjelaskan bagaimana Anda dapat mengakses kueri sampel di CloudTrail konsol dan menyertakan beberapa contoh kueri CloudTrail Lake untuk membantu Anda memulai.

> **Note**
>
> Anda juga dapat melihat kueri yang dibuat oleh GitHub komunitas. Untuk informasi selengkapnya dan untuk melihat contoh kueri ini, lihat kueri sampel CloudTrail Lake di situs web. GitHub AWS CloudTrailbelum mengevaluasi kueri di. GitHub

Topik

Melihat contoh kueri di konsol CloudTrail

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri.

Untuk mengakses kueri sampel di konsol CloudTrail

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Dari panel navigasi, di bawah Danau, pilih Kueri.
3. Pilih tab Contoh kueri.
4. Untuk mengedit kueri sampel, pilih nama Kueri. Untuk informasi tentang menjalankan kueri, lihatJalankan kueri dan simpan hasil kueri.

Contoh: Temukan semua identitas pengguna utama yang menelepon **`CreateBucket`** pada 22 Januari 2023

```
SELECT
```

```
    userIdentity.principalid,
    eventName
FROM
    event_data_store_ID
WHERE
    userIdentity.principalid IS NOT NULL
AND
    eventTime > '2023-01-22 00:00:00'
AND
    eventTime < '2023-01-23 00:00:00'
AND
    eventName='CreateBucket'
```

Hasil

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 1,
        "TotalResultsCount": 1,
        "BytesScanned": 25077
    },
    "QueryResultRows": [
        [
            {
                "principalid": "principal_ID"
            },
            {
                "eventName": "CreateBucket"
            }
        ]
    ]
}
```

Contoh: Temukan semua API yang dipanggil pengguna pada 22 Januari 2023

```
SELECT
    eventID,
    eventName,
    eventSource,
    eventTime
FROM
    event_data_store_ID
```

```
WHERE
    userIdentity.username = 'bob'
AND
    eventTime > '2023-01-22 00:00:00'
AND
    eventTime < '2023-01-23 00:00:00'
```

Hasil


```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 2,
        "TotalResultsCount": 2,
        "BytesScanned": 13287
    },
    "QueryResultRows": [
        [
            {
                "eventID": "EXAMPLE-c3b6-43e4-aa35-b2490EXAMPLE"
            },
            {
                "eventName": "DescribeQuery"
            },
            {
                "eventSource": "cloudtrail.amazonaws.com"
            },
            {
                "eventTime": "2023-01-22 16:53:53.000"
            }
        ],
        [
            {
                "eventID": "EXAMPLE6-ac95-4b37-b587-76a80EXAMPLE"
            },
            {
                "eventName": "ListBuckets"
            },
            {
                "eventSource": "s3.amazonaws.com"
            },
            {
                "eventTime": "2023-01-22 20:25:01.000"
```

```
            }
        ]
    ]
}
```

Contoh: Temukan jumlah panggilan API sejak 1 Januari 2023, dikelompokkan berdasarkan dan **eventNameeventSource**

```
SELECT
    eventSource,
    eventName,
    COUNT(*) AS apiCount
FROM
    event_data_store_ID
WHERE
    eventTime > '2023-01-01 00:00:00'
GROUP BY
    eventSource, eventName
ORDER BY
    apiCount DESC
```

Hasil

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 3,
        "TotalResultsCount": 3,
        "BytesScanned": 10442
    },
    "QueryResultRows": [
        [
            {
                "eventSource": "s3.amazonaws.com"
            },
            {
                "eventName": "PutObject"
            },
            {
                "apiCount": "96059"
            }
        ],
```

```
        [
            {
                "eventSource": "dynamodb.amazonaws.com"
            },
            {
                "eventName": "DescribeTable"
            },
            {
                "apiCount": "49426"
            }
        ],
        [
            {
                "eventSource": "sts.amazonaws.com"
            },
            {
                "eventName": "AssumeRole"
            },
            {
                "apiCount": "45617"
            }
        ]
    ]
}
```

Contoh: Temukan semua pengguna yang masuk ke konsol dalam satu set Wilayah

```
SELECT
    eventTime,
    useridentity.arn,
    awsRegion
FROM
    event_data_store_ID
WHERE
    awsRegion in ('us-east-1', 'us-west-2')
AND
    eventName = 'ConsoleLogin'
```

Hasil

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
```

```
        "ResultsCount": 2,
        "TotalResultsCount": 2,
        "BytesScanned": 15580
    },
    "QueryResultRows": [
        [
            {
                "eventTime": "2022-02-08 19:54:44.000"
            },
            {
                "arn": "arn:aws:sts::123456789012:assumed-role/example-identity"
            },
            {
                "awsRegion": "us-east-1"
            }
        ],
        [
            {
                "eventTime": "2022-01-21 16:38:27.000"
            },
            {
                "arn": "arn:aws:sts::123456789012:assumed-role/example-identity"
            },
            {
                "awsRegion": "us-west-2"
            }
        ]
    ]
}
```

Contoh: Temukan semua kueri CloudTrail Danau yang dijalankan pada Januari 2023

```
SELECT
    element_at(responseElements, 'queryId'),
    element_at(requestParameters, 'queryStatement')
FROM
    event_data_store_ID
WHERE
    eventName='StartQuery'
AND
    eventSource = 'cloudtrail.amazonaws.com'
AND
    responseElements IS NOT NULL
```

```
AND
    eventTime > '2023-01-01 00:00:00'
AND
    eventTime < '2023-02-01 00:00:00'
```

Hasil

```
{
    "QueryStatus": "FINISHED",
    "QueryStatistics": {
        "ResultsCount": 1,
        "TotalResultsCount": 1,
        "BytesScanned": 13002
    },
    "QueryResultRows": [
        [
            {
                "_col0": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE"
            },
            {
                "_col1": "select * from event_data_store_ID limit 1;"
            }
        ]
    ]
}
```

Jalankan kueri dan simpan hasil kueri

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 AWS Management Console 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. 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 Command 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, lihatDapatkan dan unduh 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, lihatMemvalidasikan hasil kueri yang disimpan.

Lihat hasil kueri

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.

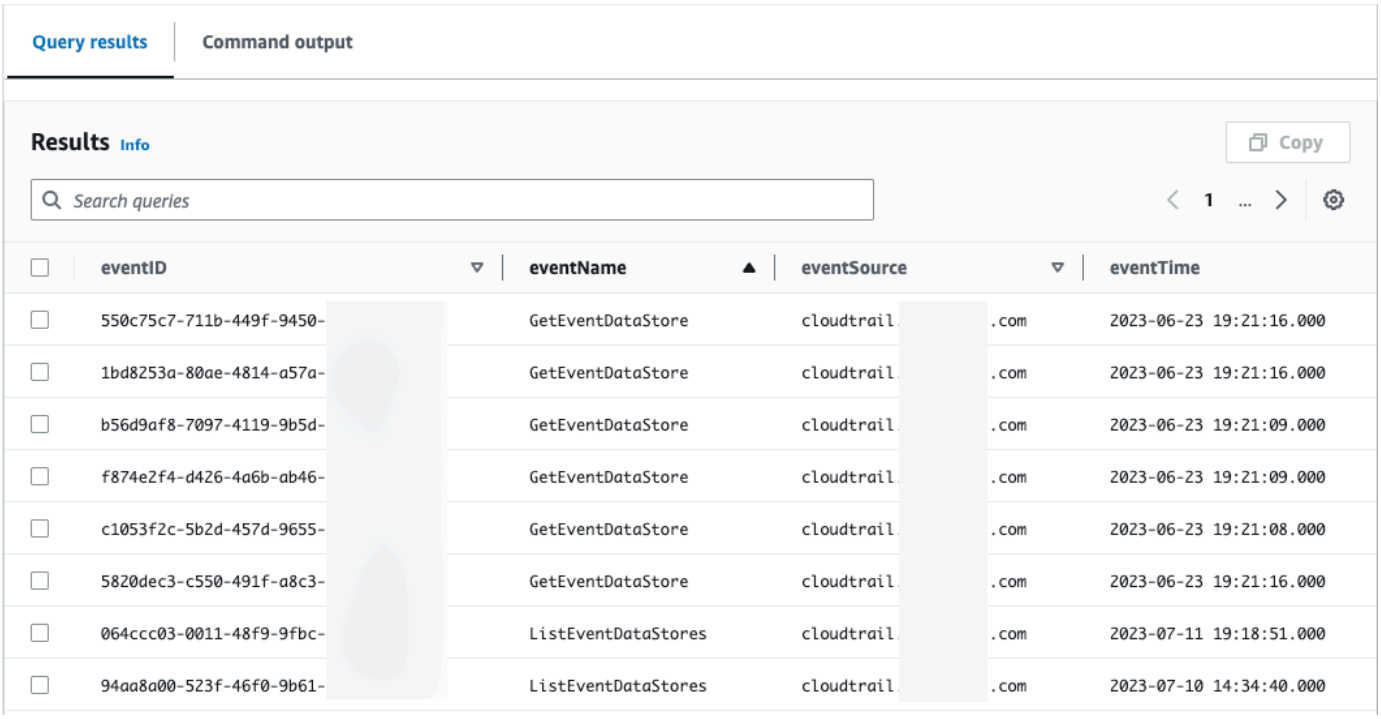
Hasil kueri dapat berubah dari proses kueri yang lebih lama ke yang lebih baru, karena peristiwa selanjutnya dalam periode kueri dapat dicatat di antara kueri.

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, lihatDapatkan dan unduh hasil kueri yang disimpan.

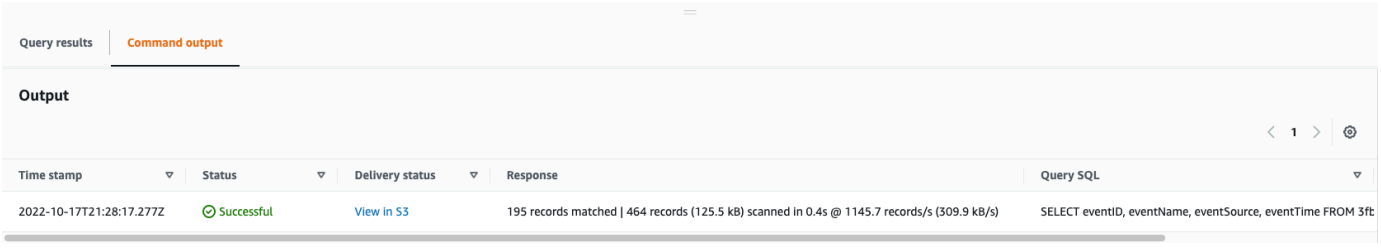
> **Note**
>
> Kueri yang berjalan lebih dari satu jam mungkin habis. Anda masih bisa mendapatkan sebagian hasil yang diproses sebelum waktu kueri habis. CloudTrail tidak memberikan hasil

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.

1. 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. 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.



Dapatkan dan 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 sejak CloudTrail memberikan hasil kueri setelah pemindaian kueri selesai. Sementara sebagian besar kueri selesai dalam beberapa menit, tergantung pada ukuran penyimpanan data acara Anda, itu bisa memakan waktu jauh lebih lama CloudTrail untuk memberikan hasil kueri 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 Anda CloudTrail Lake menyimpan hasil kueri

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, lihatMemvalidasikan hasil kueri yang disimpan.

Untuk mengambil hasil kueri atau file tanda, Anda dapat menggunakan konsol Amazon S3, antarmuka baris perintah (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
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

Unduh Anda CloudTrail Lake menyimpan hasil kueri

Saat Anda menyimpan hasil kueri, CloudTrail mengirimkan dua jenis file ke bucket Amazon S3 Anda.

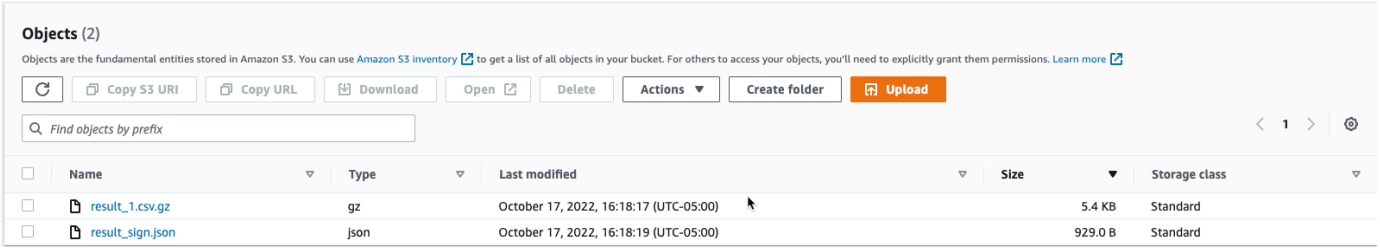
- File tanda dalam format JSON yang dapat Anda gunakan untuk memvalidasi file hasil kueri. Berkas tanda bernama result_sign.json. Untuk informasi selengkapnya tentang file tanda tangan, lihatCloudTrail struktur file tanda.
- Satu atau lebih file hasil kueri dalam format CSV, yang berisi hasil dari kueri. 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_*nomor*.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 lalu pilih file yang ingin Anda unduh.



3. PilihUnduhdan 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, lahkan ke langkah 5.

4. Gunakan produk seperti7-Zipuntuk mengekstrak file hasil kueri.
5. Buka hasil kueri atau tandatangani file.

Memvalidasikan hasil kueri yang disimpan

Untuk menentukan apakah hasil kueri diubah, dihapus, atau tidak berubah setelahnya CloudTrail menyampaikan hasil query, Anda dapat menggunakan CloudTrail validasi integritas hasil 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 CloudTrail file hasil 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. The CloudTrail proses validasi integritas file hasil kueri juga memungkinkan Anda mengetahui apakah file hasil kueri telah dihapus atau diubah.

Topik

- Validasi hasil kueri yang disimpan denganAWS CLI
- CloudTrail struktur file tanda
- Implementasi kustom CloudTrail validasi integritas file hasil kueri

Validasi hasil kueri yang disimpan denganAWS CLI

Anda dapat memvalidasi integritas file hasil kueri dan menandatangani file dengan menggunakanaws cloudtrail verify-query-resultsperintah.

Prasyarat

Untuk memonfirmasi integritas hasil kueri dengan baris perintah, kondisi berikut harus dipenuhi:

- Anda harus memiliki konektivitas online untukAWS.
- Anda harus menggunakanAWS CLIversi 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-pathparameter.
  - 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 ke bucket Amazon S3 yang berisi file hasil kueri dan file tanda.
  - Awalan S3 yang ditentukan harus berisi file hasil kueri dan file tanda. Tentukan awalan S3 sebagai nilai untuk--s3-prefixparameter.

verify-query-results

Theverify-query-resultsperintah memverifikasi nilai hash dari setiap file hasil query dengan membandingkan nilai dengan`fileHashValue`di file tanda, dan kemudian memvalidasi`hashSignature`dalam file tanda.

Saat Anda memverifikasi hasil kueri, Anda dapat menggunakan salah satu--s3-bucketdan--s3-prefixopsi baris perintah untuk memvalidasi file hasil kueri dan menandatangani file yang disimpan dalam ember S3, atau Anda dapat menggunakan--local-export-pathopsi baris perintah untuk melakukan validasi lokal dari file hasil kueri yang diunduh dan file tanda tangan.

> **Note**
>
> Theverify-query-resultsPerintah adalah Region spesifik. Anda harus menentukan--regionopsi global untuk memvalidasi hasil kueri untuk spesifikWilayah AWS.

Berikut ini adalah opsi untukverify-query-resultsperintah.

--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-bucketatau--s3-prefix.

Contoh

Contoh berikut memvalidasi hasil query menggunakan--s3-bucketdan--s3-prefixopsi baris perintah untuk menentukan nama bucket S3 dan awalan yang berisi file hasil kueri dan file tanda.

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

Contoh berikut memvalidasi hasil query download menggunakan--local-export-pathopsi baris perintah untuk menentukan jalur lokal untuk file hasil kueri dan file tanda. Untuk informasi selengkapnya tentang mengunduh file hasil kueri, lihatUnduh Anda CloudTrail Lake menyimpan hasil kueri.

```
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`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

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 dikirimkan ke bucket Amazon S3 yang mengikuti sintaks ini.

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

Contoh isi file tanda

Contoh file tanda berikut berisi informasi untuk CloudTrail Hasil kueri danau.

```
{
```

```
  "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 untukAWSakun yang digunakan untuk menyimpan hasil query.

`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 kapan 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 yang dikodekan heksadesimal dari kunci publik yang digunakan untuk menandatangani file.

Implementasi kustom CloudTrail validasi integritas file hasil kueri

Karena CloudTrail menggunakan standar industri, algoritma kriptografi yang tersedia secara terbuka dan fungsi hash, Anda dapat membuat alat Anda sendiri untuk memvalidasi integritas CloudTrail file hasil kueri. Saat Anda menyimpan hasil kueri ke bucket Amazon S3, CloudTrail memberikan file tanda ke ember S3. Anda dapat menerapkan solusi validasi Anda sendiri untuk memvalidasi tanda tangan dan file hasil kueri. Tabel berikut tentang file ini, lihatCloudTrail struktur file tanda.

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.

Tabel berikut memahami bagaimana CloudTrail Berkas tanda ditandatangani

CloudTrail file tanda ditandatangani dengan tanda tangan digital RSA. Untuk setiap berkas tanda, CloudTrailmelakukan 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. Tabel ini 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`StartTime`lebih awal dari`queryCompleteTime`dan sebuah`EndTime`lebih lambat dari`queryCompleteTime`.
6. Dari antara kunci publik yang diambil, pilih kunci publik yang sidik jarinya cocok`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. Tabel ini mencantumkan`fileHashValue`untuk setiap file hasil kueri.

   Misalnya, jika file tanda tangan Anda`files`array berisi tiga file hasil query 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`fileHashValue`untuk file hasil kueri yang direkam dalam file tanda. Jika hash cocok, file hasil kueri valid.

Bagian berikut menjelaskan proses secara detail.

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 satuAWS CLIatau 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 kunci pribadi/publik 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.

Tabel ini.AWS CLIuntuk mengambil kunci publik

Untuk mengambil kunci publik untuk file tanda dengan menggunakanAWS CLI, gunakan`cloudtrail list-public-keys`perintah. Perintah ini 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.

Tabel Tabel

Responsnya akan berupa daftar objek JSON yang mewakili kunci (atau kunci) yang dikembalikan:

Tabel ini. CloudTrail API untuk mengambil kunci publik

Untuk mengambil kunci publik untuk file tanda dengan menggunakan CloudTrail API, berikan nilai waktu mulai dan waktu akhir ke`ListPublicKeys`API. The`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**
>
> Tabel ini.`ListPublicKeys`dapat berubah.

Tabel Permintaan

Nama	Penjelasan
`StartTime`	Secara opsional menentukan, di UTC, awal rentang waktu untuk mencari kunci publik CloudTrail file tanda tangan. Jika StartTime tidak 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 CloudTrail menandatangani file. Jika EndTime tidak ditentuka n, waktu saat ini. Jenis: DateTime

Tabel Tabel Tabel

`PublicKeyList`, sebuah array`PublicKey`objek yang berisi:

Nama	Deskripsi
`Value`	Tabel ini mengkodekan nilai ini. #1 Jenis: Gumpalan
`ValidityS tartTime`	Waktu mulai validitas kunci.

	Jenis: DateTime
`ValidityEndTime`	Waktu akhir validitas. Jenis: DateTime
`Fingerprint`	Tabel ini. Sidik jari dapat digunakan untuk mengidentifikasi kunci publik yang harus Anda gunakan untuk memvalidasi file tanda. Jenis: 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 setelahnya CloudTrail mengirimkannya, hash SHA-256 akan berubah, dan tanda tangan dari file tanda tidak akan cocok.

Gunakan prosedur berikut untuk memvalidasi file hasil kueri yang tercantum dalam file tanda`files`array.

1. Ambil hash asli dari file dari`files.fileHashValue`bidang dalam file tanda.
2. Hash konten terkompresi dari file hasil kueri dengan algoritma hashing yang ditentukan dalam`hashAlgorithm`.
3. Bandingkan nilai hash yang Anda hasilkan untuk setiap file hasil kueri dengan`files.fileHashValue`dalam file tanda. 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.

Tabel Publik

Untuk memvalidasi offline, kunci publik yang Anda perlukan 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

Contoh cuplikan berikut menyediakan kode kerangka untuk memvalidasi CloudTrail tanda dan kueri file hasil. Kode kerangka adalah agnostik online/offline; artinya, terserah Anda untuk memutuskan apakah akan menerapkannya dengan atau tanpa konektivitas online keAWS. Implementasi yang disarankan menggunakanEkstensi Kriptografi Java (JCE)danKastil Bouncysebagai 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`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.");
    }
}
```

Sumber belajar

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 Lake (video) YouTube
- Log Peristiwa Aktivitas dari AWS Non-Sumber di AWS CloudTrail Danau (YouTube video)
- Dapatkan visibilitas ke log aktivitas untuk tenaga kerja dan identitas pelanggan Anda (blog) AWS
- Menggunakan AWS CloudTrail Lake untuk mengidentifikasi koneksi TLS yang lebih lama ke titik akhir AWS layanan (blog) AWS
- Bagaimana Serigala Arktik menggunakan AWS CloudTrail Danau untuk Menyederhanakan Keamanan dan Operasi (blog) AWS

- CloudTrail Lake FAQ
- AWS CloudTrailReferensi API
- AWS CloudTrailData API Referensi
- AWS CloudTrailPanduan Orientasi Mitra

Mengelola CloudTrail Danau dengan menggunakan AWS CLI

Berikut ini adalah contoh AWS CLI perintah untuk membuat dan mengelola penyimpanan data acara dan kueri di CloudTrail Lake.

Topik

- Buat toko data acara dengan AWS CLI
- Impor peristiwa jejak ke penyimpanan data acara dengan AWS CLI
- Buat integrasi untuk mencatat peristiwa dari luar AWS dengan AWS CLI
- Dapatkan penyimpanan data acara dengan AWS CLI
- Daftar semua penyimpanan data acara di akun dengan AWS CLI
- Perbarui penyimpanan data acara 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
- Hapus penyimpanan data acara dengan AWS CLI
- Kembalikan penyimpanan data acara dengan AWS CLI
- Daftar semua saluran dengan AWS CLI
- Perbarui saluran dengan AWS CLI
- Hapus saluran untuk menghapus integrasi dengan AWS CLI
- Mulai kueri dengan AWS CLI
- Dapatkan metadata tentang kueri dengan AWS CLI
- Dapatkan hasil kueri dengan AWS CLI
- Daftar semua kueri pada penyimpanan data acara dengan AWS CLI
- Batalkan kueri yang sedang berjalan dengan AWS CLI

Buat toko data acara dengan AWS CLI

Gunakan `create-event-data-store`perintah untuk membuat penyimpanan data acara.

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 AWS KMS yang akan 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`- Mengaktifkan 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`

adaEXTENDABLE_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-ingestionParameter ini hanya valid jika eventCategory adalahManagement,Data, atauConfigurationItem.

Contoh berikut menunjukkan cara membuat berbagai jenis penyimpanan data acara.

Topik

- Buat penyimpanan data acara untuk peristiwa data S3 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 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 CLIcreate-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` parameter, 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, diperlukan waktu hingga 7 hari CloudTrail untuk menyampaikan acara Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

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 CloudTrailHarga.

Impor peristiwa jejak ke penyimpanan data acara dengan AWS CLI

Di dalamAWS CLI, Anda dapat mengimpor peristiwa jejak ke penyimpanan data acara. Prosedur di bagian ini menunjukkan cara membuat dan mengkonfigurasi penyimpanan data peristiwa dengan menjalankan create-event-data-storeperintah dan kemudian mengimpor peristiwa ke penyimpanan data peristiwa dengan menggunakan start-importperintah. Untuk informasi selengkapnya tentang mengimpor peristiwa jejak termasuk informasi tentang pertimbangan dan izin yang diperlukan, lihat. Salin peristiwa jejak ke penyimpanan data acara

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 respon:

   ```
   {
       "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` `eventTime`Untuk `--start-event-time` tentukan acara tertua yang ingin Anda salin dan `--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 `ImportStatus` of `COMPLETED` jika tidak ada kegagalan, atau `FAILED` jika ada kegagalan.

Jika impor memiliki`FailedEntries`, 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
```

Buat integrasi untuk mencatat peristiwa dari luar AWS dengan AWS CLI

Di dalamAWS CLI, Anda membuat integrasi yang mencatat peristiwa dari luar AWS dalam empat perintah (tiga jika Anda sudah memiliki penyimpanan data peristiwa 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 organisasiAWS 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 CLIPerintah contoh berikut membuat penyimpanan data peristiwa yang mencatat peristiwa dari luarAWS. 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. Perintah contoh berikut membuat saluran yang mengirimkan peristiwa ke dua penyimpanan data peristiwa, diwakili oleh ID mereka 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 luarAWS, 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 prinsipal tertentu pada sumber daya dan dalam kondisi apa. 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 kebijakan harus berisi ID AWS akun mitra, dan mengharuskan Anda memasukkan ID eksternal unik yang disediakan oleh mitra. CloudTrail secara otomatis menambahkan ID AWS akun mitra 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 CloudTrailcontoh 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 identifikasi 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 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.

```
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`.

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:::bucketName"
                    ]
                },
                {
                    "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 CLIlist-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"
        }
    ]
```

```
}
```

Perbarui penyimpanan data acara dengan AWS CLI

Contoh berikut menunjukkan cara memperbarui penyimpanan data acara.

Topik

- 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-mode`Untuk 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 ke`FIXED_RETENTION_PRICING`, Anda dapat mengubah nilainya menjadi`EXTENDABLE_RETENTION_PRICING`. `EXTENDABLE_RETENTION_PRICING`Umumnya 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 CloudTrailHarga dan Mengelola 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 luarAWS.

> **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"
}
```

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 menjalankanstart-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.

Hapus penyimpanan data acara dengan AWS CLI

Contoh AWS CLI delete-event-data-store perintah berikut menonaktifkan penyimpanan data peristiwa yang ditentukan oleh`--event-data-store`, yang menerima ARN penyimpanan data peristiwa, atau akhiran ID dari ARN. Setelah Anda menjalankandelete-event-data-store, status akhir 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 saat penghapusan tertunda.

> **Note**
>
> Anda tidak dapat menghapus penyimpanan data peristiwa jika `--termination-protection-enabled` disetel atau `FederationStatus` sudah diatur`ENABLED`.

```
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.

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.

Daftar semua saluran dengan AWS CLI

Untuk membuat daftar semua saluran di akun Anda, jalankan list-channels perintah. Berikut adalah contohnya.

```
aws cloudtrail list-channels
```

Perbarui saluran dengan AWS CLI

Untuk memperbarui nama saluran atau penyimpanan data peristiwa tujuan, jalankan update-channel perintah. parameter `--channel` diperlukan. Anda tidak dapat memperbarui sumber saluran. Berikut adalah contohnya.

```
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

Untuk berhenti menelan mitra atau peristiwa aktivitas lain di luarAWS, hapus saluran dengan menjalankan delete-channel perintah. ARN atau ID saluran (akhiran ARN) dari saluran yang ingin Anda hapus diperlukan. Berikut adalah contohnya.

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

Mulai kueri dengan AWS CLI

AWS CLIstart-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-s3uri`, 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-s3uri "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-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.

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"
}
```

Daftar semua kueri pada penyimpanan 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

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.

CloudTrail Lake mendukung semua `SELECT` pernyataan, fungsi, dan operator Presto SQL yang valid. Untuk informasi selengkapnya tentang fungsi dan operator SQL yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Presto.

CloudTrail Konsol menyediakan sejumlah contoh kueri yang dapat membantu Anda mulai menulis kueri Anda sendiri. Untuk informasi selengkapnya, lihat Melihat contoh kueri di konsol CloudTrail .

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 Presto. Untuk informasi selengkapnya tentang fungsi yang didukung, lihat Fungsi dan Operator di situs web dokumentasi Presto.

CloudTrail Danau tidak mendukung `INTERVAL` kata kunci.

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 toko 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

Bagian berikut menyediakan skema SQL yang didukung untuk setiap jenis penyimpanan data peristiwa.

Topik

Skema yang didukung untuk bidang catatan CloudTrail acara

Berikut ini adalah skema SQL yang valid untuk CloudTrail bidang catatan peristiwa manajemen dan data. Untuk informasi selengkapnya tentang bidang catatan CloudTrail peristiwa, lihatCloudTrail isi rekaman.

```
[
    {
        "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>,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": "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": "eventjsonchecksum",
        "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`.

```
[
    {
        "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>>"
    }
]
```

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 ManagerPanduan 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>>"
    }
]
```

Mengontrol izin pengguna untuk Lake CloudTrail

AWS CloudTrailterintegrasi dengan AWS Identity and Access Management (IAM) untuk membantu Anda mengontrol akses ke CloudTrail Danau dan AWS sumber daya lain yang CloudTrail membutuhkan. Anda dapat menggunakan IAM untuk mengontrol AWS pengguna mana yang dapat membuat, mengonfigurasi, atau menghapus penyimpanan data CloudTrail peristiwa, atau saluran, memulai dan menghentikan konsumsi acara, dan menyalin peristiwa jejak. Untuk mempelajari selengkapnya, lihat Identity and Access Management untuk AWS CloudTrail.

Topik berikut membantu Anda memahami izin, kebijakan, dan CloudTrail keamanan:

- Pemberian izin untuk administrasi CloudTrail
- Kebijakan bucket Amazon S3 untuk hasil kueri CloudTrail Lake
- Izin yang diperlukan untuk menyalin peristiwa jejak
- Izin yang diperlukan untuk federasi

- Contoh kebijakan yang membatasi akses ke penyimpanan data peristiwa berdasarkan tag: Contoh: Menolak akses untuk membuat atau menghapus penyimpanan data acara berdasarkan tag
- AWS CloudTrailcontoh kebijakan berbasis sumber daya
- Izin yang diperlukan untuk menetapkan administrator yang didelegasikan
- Kebijakan kunci KMS standar untuk CloudTrail Toko data acara danau

Mengelola biaya CloudTrail Danau

AWS CloudTrail Penyimpanan data acara danau dan kueri dikenakan biaya. Sebagai praktik terbaik, kami merekomendasikan penggunaan Layanan AWS dan alat yang dapat membantu Anda mengelola CloudTrail biaya. Anda juga 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
- Alat untuk membantu mengelola 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 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 hari dan jumlah hari yang ingin Anda simpan di penyimpanan

Jenis biaya	Bagaimana Anda dikenakan biaya
	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.
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.

Jenis biaya	Bagaimana Anda dikenakan biaya
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 CloudTrail manajemen atau peristiwa data, saring peristiwa yang tidak menarik dengan menggunakan pemilih acara lanjutan.

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.

Jika Anda membuat penyimpanan data acara untuk mengumpulkan peristiwa data, Anda dapat menggunakan pemilih acara lanjutan untuk memfilter pada`eventName`,, `resources.type`resources.`ARN`, dan `readOnly` bidang. Sebagai contoh, lihat Tutorial: Membuat penyimpanan data acara untuk acara data S3.

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.

Alat untuk membantu mengelola biaya

AWS Anggaran, fitur AWS Billing and Cost Management, memungkinkan Anda mengatur anggaran khusus yang mengingatkan Anda ketika biaya atau penggunaan Anda melebihi (atau diperkirakan melebihi) jumlah yang dianggarkan Anda.

Saat Anda membuat penyimpanan data acara, membuat anggaran untuk CloudTrail menggunakan AWS Anggaran adalah praktik terbaik yang direkomendasikan, dan dapat membantu Anda melacak CloudTrail pengeluaran Anda. Anggaran berbasis biaya 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.

Setelah Anda membuat anggaran, Anda dapat menggunakan AWS Cost Explorer untuk melihat bagaimana CloudTrail biaya Anda mempengaruhi keseluruhan AWS tagihan Anda. Di AWS Cost Explorer, setelah menambahkan CloudTrail ke filter Layanan, Anda dapat membandingkan CloudTrail pengeluaran historis Anda dengan pengeluaran Anda saat ini month-to-date (MTD), menurut Wilayah dan akun. Fitur ini membantu Anda memantau dan mendeteksi biaya tak terduga dalam CloudTrail pengeluaran bulanan Anda. Fitur tambahan di Cost Explorer memungkinkan Anda membandingkan CloudTrail pengeluaran dengan pengeluaran bulanan di tingkat sumber daya tertentu, memberikan informasi tentang apa yang mungkin mendorong kenaikan atau penurunan biaya tagihan Anda.

Untuk memulai dengan AWS Anggaran, buka AWS Billing and Cost Management, 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 Anggaran dan Praktik Terbaik untuk AWS Anggaran.

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 manajemen atau peristiwa data prosedur.
- Untuk membuat tag menggunakan CloudTrail API, lihat CreateEventDataStoredan AddTagsdi Referensi AWS CloudTrail API.
- Untuk membuat tag menggunakan AWS CLI, lihat create-event-data-storedan tambahkan tag di AWS CLI Command Reference.

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

Lihat juga

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

CloudWatch Metrik yang didukung

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 AndaAWS.

`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

Metrik	Deskripsi	Unit
`TotalStorageBytes`	Total byte terkompresi dalam penyimpanan data acara pada hari ini. Metrik ini tersedia untuk semua jenis penyimpanan data peristiwa.	Byte

Metrik	Deskripsi	Unit
`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 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, penyimpanan. pay-as-you-go Untuk informasi tentang harga, lihat AWS CloudTrailHarga. Metrik ini hanya tersedia untuk penyimpanan data acara menggunakan opsi harga retensi yang dapat diperpanjang satu tahun.	Byte

Metrik	Deskripsi	Unit
`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

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

Jika Anda telah membuat organisasi diAWS Organizations, Anda dapat membuat jejak yang akan mencatat semua peristiwa untuk semua Akun AWS di organisasi itu. Membuat jejak organisasi membantu Anda menentukan strategi pencatatan peristiwa yang seragam untuk organisasi Anda.

Topik

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 yang mencatat peristiwa di semua AWS Wilayah, itu akan muncul di konsol di semua Wilayah di AWS partisi tempat Anda bekerja. Jika Anda membuat jejak yang hanya mencatat peristiwa di satu Wilayah, Anda dapat melihat dan mengelolanya hanya di Wilayah tersebut. Membuat jejak Multi-wilayah adalah opsi default jika Anda membuat jejak dengan menggunakan AWS CloudTrail konsol, dan merupakan praktik terbaik yang disarankan. Untuk membuat jejak wilayah Tunggal, Anda harus menggunakan. AWS CLI

Jika Anda menggunakanAWS 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 organisasi.

Topik

- Membuat dan memperbarui jejak dengan konsol
- Membuat, memperbarui, dan mengelola jalur dengan AWS Command Line Interface

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 satuWilayah AWS,menggunakanAWS CLI.

Anda dapat membuat hingga lima jalur untuk setiap Wilayah. Setelah Anda membuat jejak, CloudTrailsecara otomatis mulai mencatat panggilan API dan kejadian terkait di akun Anda ke bucket Amazon S3 yang Anda tentukan. Untuk menghentikan logging, Anda dapat mematikan logging untuk jejak atau menghapusnya.

Menggunakan CloudTrail konsol untuk membuat atau memperbarui jejak memberikan keuntungan sebagai berikut.

- Jika ini adalah pertama kalinya Anda membuat jejak, menggunakan CloudTrail konsol memungkinkan Anda melihat fitur dan opsi yang tersedia.
- Jika Anda mengonfigurasi jejak untuk mencatat peristiwa data, gunakan CloudTrail konsol memungkinkan Anda melihat tipe data yang tersedia. Untuk informasi selengkapnya tentang kejadian dari semua Wilayah tersebut mencatat kejadian dari semua Wilayah di data, lihatPencatatan peristiwa data.

Untuk informasi spesifik untuk membuat jejak bagi organisasi diAWS Organizations, lihatMembuat jejak untuk organisasi.

Topik

Membuat jejak

Sebagai praktik terbaik, buat jejak yang berlaku untuk semua Wilayah AWS. Ini adalah pengaturan default saat Anda membuat jejak di CloudTrail konsol. Jika jejak berlaku untuk semua Wilayah, CloudTrail mengirimkan file log dari semua Wilayah di AWS partisi tempat Anda bekerja ke bucket S3 yang Anda tentukan. Setelah Anda membuat jejak, AWS CloudTrail secara otomatis mulai mencatat peristiwa yang Anda tentukan.

> **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 di konsol

Gunakan prosedur berikut untuk membuat jejak yang mencatat peristiwa Wilayah AWS di semua AWS partisi tempat Anda bekerja. Ini adalah praktik terbaik yang direkomendasikan. Untuk mencatat peristiwa di satu Wilayah (tidak disarankan), gunakan AWS CLI.

Untuk membuat CloudTrail jejak dengan AWS Management Console

1. Masuk ke AWS Management Console 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.
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 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.

   > **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 enkripsi SSE-KMS berkas Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda menggunakan enkripsi SSE-KMS alih-alih enkripsi SSE-S3. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan enkripsi SSE-KMS, log 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).

   Jika Anda mengaktifkan enkripsi SSE-KMS, 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. 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. Kebijakan kunci harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasikanAWS KMSkebijakan 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 berkas 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 yang berlaku untuk semua Wilayah, pemberitahuan SNS untuk pengiriman file log dari semua Wilayah 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 selengkapnya, lihat Panduan Memulai Layanan Notifikasi Sederhana Amazon.

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 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 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, tambahkan satu atau beberapa tag kustom (pasangan nilai kunci) 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. Lihat informasi yang lebih lengkap di AWS Resource Groups dan Mengapa menggunakan tag untuk CloudTrail sumber daya?.
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 Acara 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. Volume rendah, 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 Harga AWS CloudTrail.
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 peristiwa data 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 peristiwa Data, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang tipe peristiwa data yang tersedia, lihatPeristiwa data.

    Note

    Untuk mencatat peristiwa data untuk AWS Glue tabel yang dibuat oleh Lake Formation, pilih Lake Formation.

13. Pilih templat pemilih log. CloudTrail termasuk template yang telah ditetapkan yang mencatat semua peristiwa data untuk jenis sumber daya. Untuk membuat template pemilih log kustom, pilih Kustom.

    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 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 (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. Di Advanced event selectors, buat ekspresi untuk sumber daya spesifik tempat Anda ingin mencatat peristiwa data. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

    a. Pilih dari bidang berikut.

    - **readOnly**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Peristiwa data hanya-baca 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,PutItem, atauGetSnapshotBlock.
    - **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`

Tabel berikut menunjukkan format ARN yang valid untuk masing-masing. `resources.type`

> **Note**
>
> Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

resources.type	Sumber Daya.arn
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`
`AWS::AppConfig::Configuration`	`arn:partition :appconfig: region:account_ID :application/ application_ID /environment/ environment_ID /configuration/ configuration_profile_ID`
`AWS::B2BI::Transformer`	`arn:partition :b2bi:region:account_ID :transformer/ transformer_ID`
`AWS::Bedrock::AgentAlias`	`arn:partition :bedrock: region:account_ID :agent-alias/ agent_ID/alias_ID`

resources.type	Sumber Daya.arn
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*

resources.type	Sumber Daya.arn
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*

resources.type	Sumber Daya.arn
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	Sumber Daya.arn
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*

resources.type	Sumber Daya.arn
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	Sumber Daya.arn
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN harus berada dalam salah satu format berikut: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*

resources.type	Sumber Daya.arn
`AWS::ThinClient::Device`	`arn:partition :thinclient: region:account_ID :device/device_ID`
`AWS::ThinClient::Environment`	`arn:partition :thinclient: region:account_ID :environment/ environment_ID`
`AWS::Timestream::Database`	`arn:partition :timestream: region:account_ID :database/ database_name`
`AWS::Timestream::Table`	`arn:partition :timestream: region:account_ID :database/ database_name /table/table_name`
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table`. Jika Anda menentukan `AWS::DynamoDB::Table` untuk`resources.type`, itu akan mencatat kedua tabel DynamoDB dan peristiwa aliran DynamoDB secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.

[2] Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok. Slash trailing disengaja; jangan mengecualikannya.

[3] Untuk mencatat peristiwa pada semua objek di titik akses S3, kami sarankan Anda hanya menggunakan titik akses ARN, jangan sertakan jalur objek, dan gunakan `StartsWith` operator atau. `NotStartsWith`

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Tindakan, sumber daya, dan kunci kondisi di AWS Identity and Access Management Panduan Pengguna.

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 jejak Anda, Anda dapat mengatur bidang ke Resources.arn, menyetel operator untuk tidak memulai, lalu menempelkan di ARN bucket S3, atau menelusuri 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.

   > **Note**
   >
   > Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi di jalan setapak. 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.
   > 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 mencatat semua fungsi dengan template pemilih yang telah ditentukan, 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.

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 tipe data lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 12 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk tipe peristiwa data.

17. 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, lihatAcara Logging Insights. 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`S3bucketName/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `S3bucketName/AWSLogs/CloudTrail-Insight/`

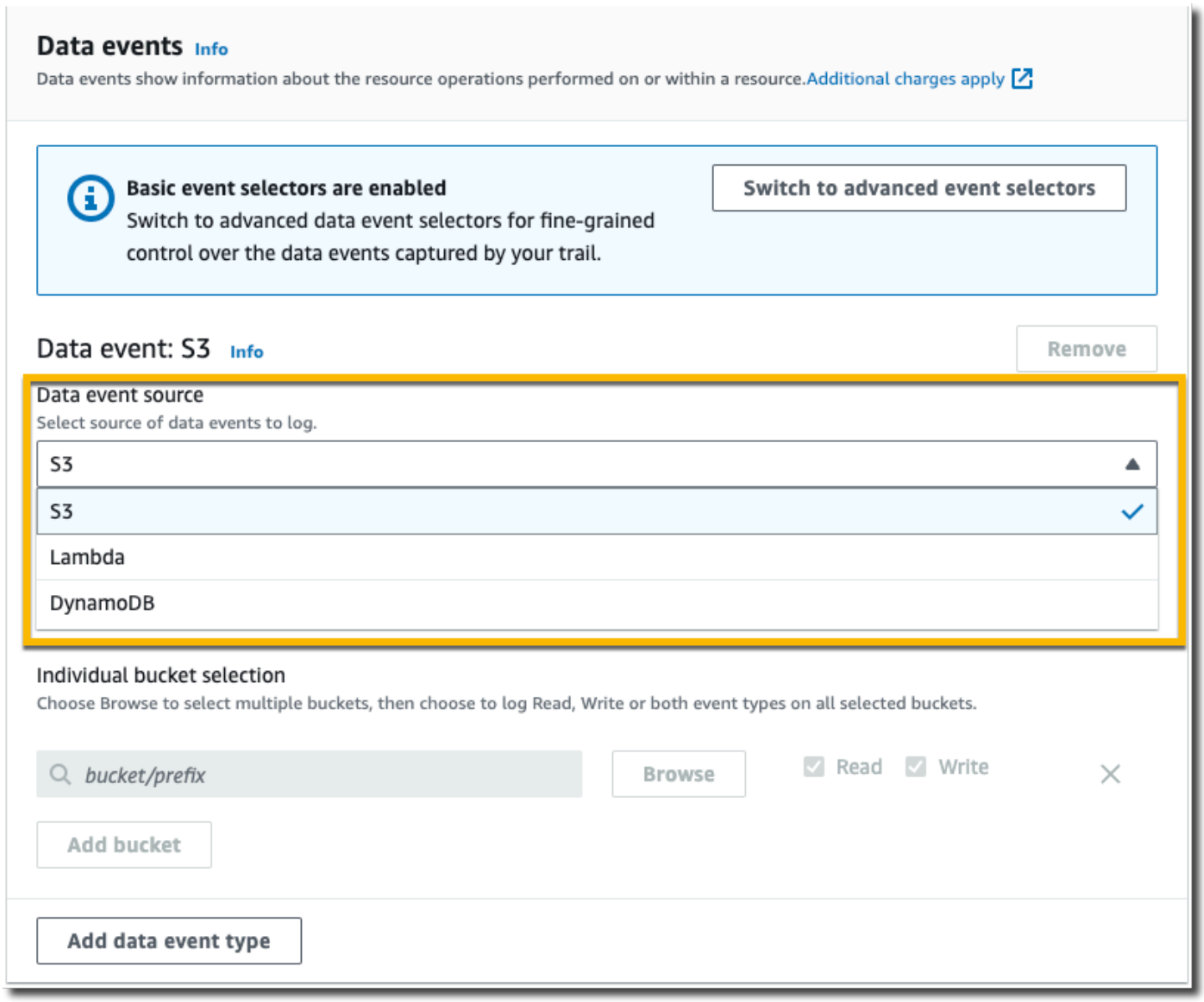
18. Setelah selesai memilih jenis acara untuk dicatat, pilih Berikutnya.
19. Pada halaman Tinjau dan buat, tinjau pilihan Anda. Pilih Edit di bagian untuk mengubah pengaturan jejak yang ditampilkan di bagian itu. Saat Anda siap untuk membuat jejak, pilih Buat jejak.
20. Jejak baru muncul di halaman Trails. 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. Diperlukan waktu hingga 36 jam CloudTrail untuk menyampaikan acara Insights pertama, jika Anda telah mengaktifkan pencatatan peristiwa Insights, dan aktivitas yang tidak biasa terdeteksi.

> **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.

Konfigurasikan pengaturan peristiwa data menggunakan pemilih acara dasar

Anda dapat menggunakan pemilih acara lanjutan untuk mengonfigurasi semua jenis peristiwa data. 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.



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 Harga AWS CloudTrail.
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 tipe data 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 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 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 pengaturan 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 kustom (pasangan kunci-nilai) ke jejak.

- Untuk membuat jejak lain, buka halaman Trails, dan pilih Create trail.

Memperbarui jejak

Bagian ini menjelaskan cara mengubah pengaturan jejak.

Untuk memperbarui jejak wilayah Tunggal untuk mencatat peristiwa Wilayah AWS di semua AWS partisi tempat Anda bekerja, atau memperbarui jejak Multi-wilayah untuk mencatat peristiwa hanya di satu Wilayah, Anda harus menggunakan. AWS CLI Untuk informasi selengkapnya tentang cara memperbarui jejak wilayah Tunggal untuk mencatat peristiwa di semua Wilayah, lihatMengonversi jejak yang berlaku untuk satu Wilayah untuk diterapkan ke semua Wilayah. Untuk informasi selengkapnya tentang cara memperbarui jejak Multi-wilayah untuk mencatat peristiwa di satu Wilayah, lihatMengubah jejak Multi-wilayah menjadi jalur Single-region.

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 AWS Management Console

1. Masuk ke AWS Management Console 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.
   - File log enkripsi SSE-KMS - 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 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.

> **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 kepadanya. 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 enkripsi SSE-KMS berkas Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda menggunakan enkripsi SSE-KMS alih-alih enkripsi SSE-S3. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan enkripsi SSE-KMS, log 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).

   Jika Anda mengaktifkan enkripsi SSE-KMS, 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. 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. Kebijakan kunci harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasikanAWS KMSkebijakan 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 berkas 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 yang berlaku untuk semua Wilayah, pemberitahuan SNS untuk pengiriman file log dari semua Wilayah 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 selengkapnya, lihat Panduan Memulai Layanan Notifikasi Sederhana Amazon.

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 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 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. Tambahkan satu atau beberapa tag kustom (pasangan nilai kunci) 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. Lihat informasi yang lebih lengkap di AWS Resource Groups dan Mengapa menggunakan tag untuk CloudTrail sumber daya?.
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 Acara 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. Volume rendah, 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. 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 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 peristiwa Data, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang tipe peristiwa data yang tersedia, lihatPeristiwa data.

> **Note**
>
> Untuk mencatat peristiwa data untuk AWS Glue tabel yang dibuat oleh Lake Formation, pilih Lake Formation.

8. Pilih templat pemilih log. CloudTrail termasuk template yang telah ditetapkan yang mencatat semua peristiwa data untuk jenis sumber daya. Untuk membuat template pemilih log kustom, pilih Kustom.

> **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 (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. Di Advanced event selectors, buat ekspresi untuk sumber daya spesifik tempat Anda ingin mengumpulkan peristiwa data. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

    a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. 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` atau`GetSnapshotBlock`.
- **`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`

  Tabel berikut menunjukkan format ARN yang valid untuk masing-masing. `resources.type`

  > **Note**
  >
  > Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

resources.type	Sumber Daya.arn
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	Sumber Daya.arn
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	Sumber Daya.arn
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	Sumber Daya.arn
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*

resources.type	Sumber Daya.arn
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	Sumber Daya.arn
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	Sumber Daya.arn
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	Sumber Daya.arn
AWS::SSM::ManagedNode	ARN harus berada dalam salah satu format berikut: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	Sumber Daya.arn
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table`. Jika Anda menentukan `AWS::DynamoDB::Table` untuk`resources.type`, itu akan mencatat kedua tabel DynamoDB dan DynamoDB stream peristiwa secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.

[2] Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok. Slash trailing disengaja; jangan mengecualikannya.

[3] Untuk mencatat peristiwa pada semua objek di titik akses S3, kami sarankan Anda hanya menggunakan titik akses ARN, jangan sertakan jalur objek, dan gunakan `StartsWith` operator atau. `NotStartsWith`

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Tindakan, sumber daya, dan kunci kondisi di AWS Identity and Access Management Panduan Pengguna.

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 jejak Anda, Anda dapat menyetel bidang ke Resources.arn, menyetel operator untuk tidak memulai, lalu menempelkan di ARN bucket S3, atau menelusuri 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.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi di jalan setapak. 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.
> 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 mencatat semua fungsi dengan template pemilih yang telah ditentukan, 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.

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 tipe data lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 3 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk tipe peristiwa data.
12. Di acara Wawasan, pilih Edit 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, lihatAcara Logging Insights. Biaya tambahan berlaku untuk acara logging Insights. Untuk CloudTrail harga, lihat AWS CloudTrail Harga.

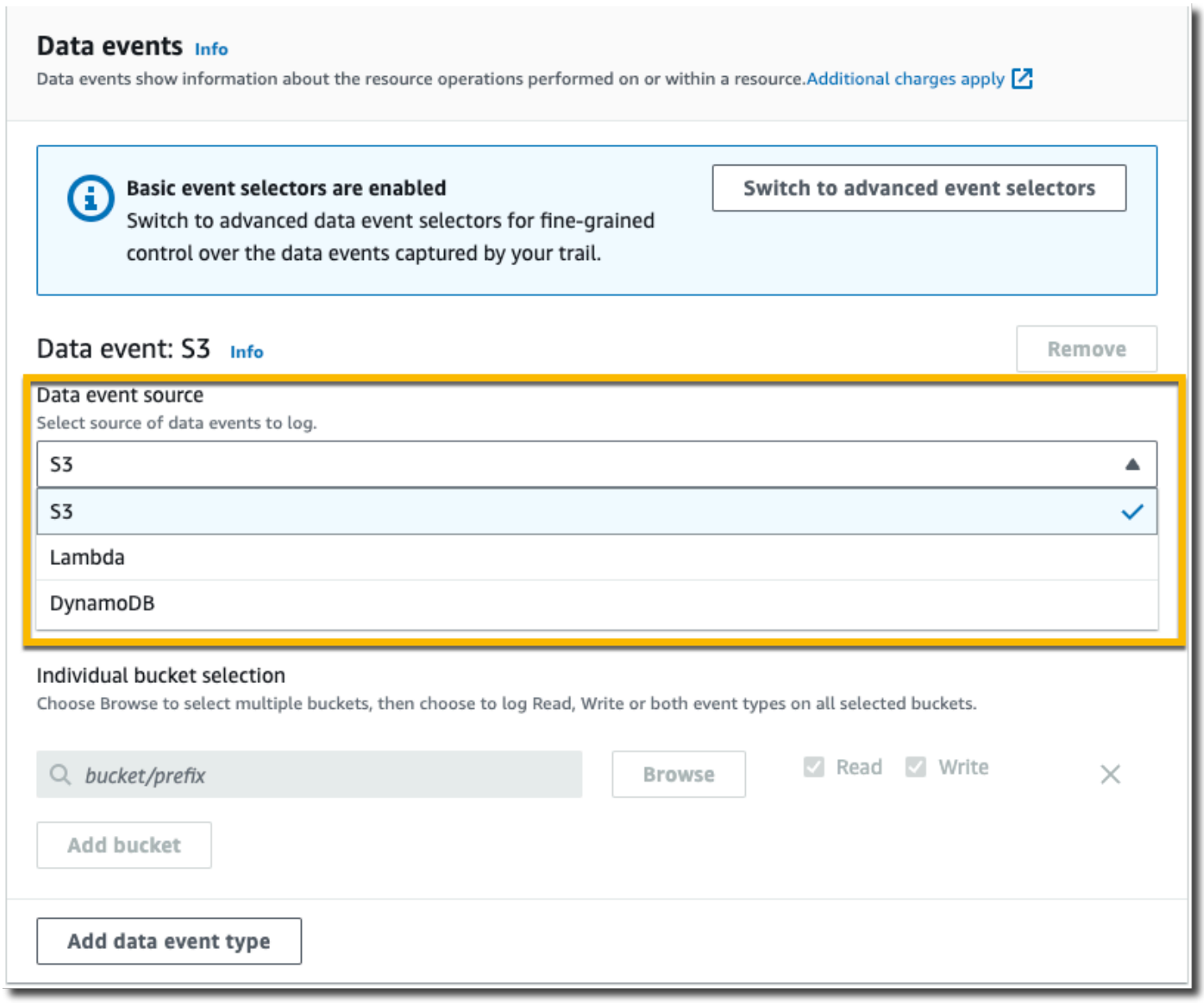
Peristiwa Insights dikirimkan ke folder berbeda bernama `/CloudTrail-Insight` bucket S3 yang sama yang ditentukan di area lokasi penyimpanan halaman detail jejak. CloudTrailmenciptakan awalan baru untuk Anda. Misalnya, jika bucket S3 tujuan Anda saat ini diberi nama`S3bucketName/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `S3bucketName/AWSLogs/CloudTrail-Insight/`

13. 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. 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.



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. Tipe 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 tipe data 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 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.

4. Untuk menambahkan tipe data 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

Menghapus jejak

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.

Jika Anda telah mengaktifkan CloudTrail peristiwa manajemen di Amazon Security Lake, Anda diharuskan untuk mempertahankan setidaknya satu jejak organisasi yang Multi-wilayah dan mencatat keduanya`read`dan`write`acara manajemen. Anda tidak dapat menghapus jejak jika itu adalah satu-satunya jejak yang Anda miliki yang memenuhi persyaratan ini, kecuali jika Anda mematikannya CloudTrail acara manajemen di Security Lake.

Untuk menghapus jejak dengan CloudTrail konsol

1. Log masuk keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. BukaJalan setapakhalaman dari CloudTrail konsol.

3. Pilih nama jejak.
4. Di bagian atas halaman detail jejak, pilihHapus.
5. Ketika Anda diminta untuk mengonfirmasi, pilihHapusuntuk menghapus jejak secara permanen. Jejak dihapus dari daftar jalan setapak. Log yang dikirimkan ke bucket Amazon S3 tidak dikirimkan.

> **Note**
>
> Konten yang dikirimkan ke bucket Amazon S3 mungkin berisi konten pelanggan. Untuk informasi selengkapnya tentang menghapus data sensitif, lihatBagaimana cara mengosongkan bucket S3?atauBagaimana Cara Menghapus bucket S3?.

Mematikan logging untuk jalan setapak

Saat Anda membuat jejak, pencatatan dihidupkan secara otomatis. Anda dapat mematikan logging untuk jalan setapak.

Saat Anda mematikan logging, log yang ada masih disimpan di bucket Amazon S3 trail dan terus dikenakan biaya S3.

Untuk mematikan logging untuk jalan setapak dengan CloudTrail konsol

1. Masuk keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilihJejak, dan kemudian pilih nama jejak.
3. Di bagian atas halaman detail jejak, pilihHentikan pencatatanuntuk mematikan penebangan untuk jalan setapak.
4. Saat Anda diminta untuk mengonfirmasi, pilihHentikan pencatatan. CloudTrailmenghentikan aktivitas logging untuk jejak itu.
5. Untuk melanjutkan pencatatan untuk jejak itu, pilihMulai loggingdi halaman konfigurasi jejak.

Membuat, memperbarui, dan mengelola jalur dengan AWS Command Line Interface

Anda dapat menggunakan AWS CLI untuk membuat, memperbarui, dan mengelola jejak Anda. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di AWS Wilayah 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 jejak di CloudTrail antaranya:

- create-trailuntuk membuat jejak.
- update-trailuntuk mengubah konfigurasi jejak yang ada.
- add-tagsuntuk menambahkan satu atau lebih tag (pasangan nilai kunci) 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 penyeleksi acara untuk jejak.
- put-insight-selectorsuntuk menambahkan atau memodifikasi pemilih acara Insights untuk jejak yang ada, dan mengaktifkan atau menonaktifkan peristiwa Insights.
- start-logginguntuk memulai acara logging dengan jejak Anda.
- stop-logginguntuk menjeda peristiwa pencatatan dengan jejak Anda.
- delete-trailuntuk menghapus jejak. Perintah ini tidak menghapus bucket Amazon S3 yang berisi file log untuk jejak itu, jika ada.
- describe-trailsuntuk mengembalikan informasi tentang jalur di suatu AWS Wilayah.
- get-trailuntuk mengembalikan informasi pengaturan untuk jejak.
- get-trail-statusuntuk mengembalikan informasi tentang status jejak saat ini.
- get-event-selectorsuntuk mengembalikan informasi tentang penyeleksi acara yang dikonfigurasi untuk jejak.

- get-insight-selectorsuntuk mengembalikan informasi tentang pemilih acara Insights yang dikonfigurasi untuk jejak.

Perintah yang didukung untuk membuat dan memperbarui jalur: create-trail dan update-trail

`update-trail`Perintah `create-trail` 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. Dalam sebagian besar keadaan, Anda harus membuat jejak yang mencatat peristiwa di semua AWS Wilayah.
- Membuat jejak yang menerima log untuk semua AWS akun di organisasi dengan --is-organization-trail opsi.
- Mengonversi jejak Multi-wilayah ke jalur Single-region dengan opsi. `--no-is-multi-region-trail`
- Mengaktifkan atau menonaktifkan enkripsi file log dengan opsi. `--kms-key-id` Opsi ini menentukan AWS KMS kunci yang telah Anda buat dan yang telah Anda lampirkan kebijakan yang memungkinkan CloudTrail untuk mengenkripsi log Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan CloudTrail enkripsi file log denganAWS CLI.
- Mengaktifkan atau menonaktifkan validasi file log dengan opsi dan. `--enable-log-file-validation` `--no-enable-log-file-validation` Untuk informasi selengkapnya, lihat Memvalidasi CloudTrail integritas berkas log.
- Menentukan grup CloudWatch log Log dan peran sehingga CloudTrail dapat mengirimkan peristiwa ke grup CloudWatch log Log. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Perintah usang: create-subscription dan update-subscription

> **Important**
>
> `update-subscription`Perintah `create-subscription` dan digunakan untuk membuat dan memperbarui jejak, 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 Anda memperbarui kode atau skrip untuk menggunakan perintah yang didukung seperticreate-trail.

Menggunakan create-trail

Anda dapat menjalankan `create-trail` perintah untuk membuat jejak yang secara khusus dikonfigurasi untuk memenuhi kebutuhan bisnis Anda. Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di AWS Wilayah 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 yang berlaku untuk semua Wilayah

Untuk membuat jejak yang berlaku untuk semua 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 acara manajemen di AWS akun Anda, Anda harus membuat jejak yang mencatat peristiwa di semua AWS Wilayah.

> **Note**
>
> Saat membuat jejak, jika Anda menentukan bucket Amazon S3 yang tidak dibuat CloudTrail, Anda harus melampirkan kebijakan yang sesuai. Lihat Kebijakan bucket Amazon S3 untuk CloudTrail.

Contoh berikut membuat jejak dengan nama *my-trail* dan tag dengan kunci bernama *Grup* dengan nilai *Pemasaran* yang mengirimkan log dari semua Wilayah ke bucket yang ada bernama. *my-bucket*

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

Untuk mengonfirmasi bahwa jejak Anda ada di semua Wilayah, `IsMultiRegionTrail` elemen dalam output akan 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": "my-bucket"
}
```

> **Note**
>
> Gunakan `start-logging` perintah untuk mulai masuk ke jejak Anda.

Mulai logging untuk jalan setapak

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 logging untuk 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 masuk, `IsLogging` elemen dalam output akan 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 Single-region

Perintah berikut membuat jejak Single-region. Bucket Amazon S3 yang ditentukan harus sudah ada dan 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 my-bucket
```

Untuk informasi selengkapnya, lihat Persyaratan penamaan.

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": "my-bucket"
}
```

Membuat jejak yang berlaku untuk semua Wilayah dan 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 berkas log.

Contoh berikut membuat jejak yang mengirimkan log dari semua Wilayah ke bucket yang ditentukan. Perintah menggunakan `--enable-log-file-validation` opsi.

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --enable-log-file-validation
```

Untuk mengonfirmasi bahwa validasi file log diaktifkan, `LogFileValidationEnabled` elemen dalam output menunjukkan`true`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Menggunakan update-trail

> **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-timur-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.

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 AWS Wilayah tempat jejak itu dibuat (Wilayah Asalnya). Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di AWS Wilayah 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 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**
>
> Jika Anda menggunakan AWS CLI atau salah satu AWS SDK untuk memodifikasi jejak, pastikan bahwa kebijakan bucket trail tersebut. up-to-date 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

Mengonversi jejak yang berlaku untuk satu Wilayah untuk diterapkan ke semua Wilayah

Untuk mengubah jejak yang ada sehingga berlaku untuk semua Wilayah, gunakan `--is-multi-region-trail` opsi.

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

Untuk mengonfirmasi bahwa jejak sekarang berlaku untuk semua Wilayah, `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": "my-bucket"
}
```

Mengubah jejak Multi-wilayah menjadi jalur Single-region

Untuk mengubah jejak 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 menunjukkan`false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Mengaktifkan dan menonaktifkan pencatatan peristiwa layanan global

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 akan 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": "my-bucket"
}
```

Untuk mengubah jejak sehingga mencatat peristiwa layanan global, gunakan `--include-global-service-events` opsi.

Jalur Single-Region tidak akan lagi menerima acara layanan global mulai 22 November 2021, kecuali jejak tersebut sudah muncul di Wilayah AS Timur (Virginia N.), us-timur-1. Untuk terus menangkap peristiwa layanan global, perbarui konfigurasi jejak ke jejak Multi-wilayah. Misalnya, perintah ini memperbarui jejak wilayah Tunggal di AS Timur (Ohio), us-timur-2, menjadi jejak Multi-wilayah. *myExistingSingleRegionTrailWithGanti GSE* 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 US East (Virginia N.) mulai 22 November 2021, Anda juga dapat membuat jalur Single-region untuk berlangganan acara layanan global di Wilayah AS Timur (Virginia N.), us-timur-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 DOC-EXAMPLE-BUCKET
```

Mengaktifkan validasi file log

Untuk mengaktifkan validasi file log untuk jejak, gunakan `--enable-log-file-validation` opsi. File Digest dikirim ke bucket Amazon S3 untuk jejak itu.

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

Untuk mengonfirmasi bahwa validasi file log diaktifkan, `LogFileValidationEnabled` elemen dalam output menunjukkan`true`.

```
{
```

```
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-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 menunjukkan`false`.

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

Untuk memvalidasi file log dengan AWS CLI, lihatMemvalidasi CloudTrail integritas file log denganAWS CLI.

Mengelola jalur dengan AWS CLI

AWS CLI Termasuk beberapa perintah lain yang membantu Anda mengelola jejak 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 AWS Wilayah yang sama tempat jejak dibuat (Wilayah Asalnya). Saat menggunakan AWS CLI, ingatlah bahwa perintah Anda berjalan di AWS Wilayah 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

Tambahkan satu atau beberapa tag ke jejak

Untuk menambahkan satu atau beberapa tag ke jejak yang ada, jalankan add-tags perintah.

Contoh berikut menambahkan tag dengan nama Pemilik dan nilai Mary ke jejak dengan ARN of 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 jejak 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"
            }
        ]
    }
  ]
}
```

Hapus satu atau beberapa tag dari jejak

Untuk menghapus satu atau beberapa tag dari jejak yang ada, jalankan remove-tags perintah.

Contoh berikut menghapus tag dengan nama Lokasi dan Nama 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

Jalankan `describe-trails` perintah untuk mengambil informasi tentang jejak di Wilayah. AWS Contoh berikut mengembalikan informasi tentang jalur yang dikonfigurasi di Wilayah Timur AS (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": "my-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,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "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": "my-bucket",
      "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
```

```
    }
  ]
}
```

Jalankan `get-trail` 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": "my-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 AWS Wilayah tempat ia dibuat (Wilayah Beranda), atau Anda harus menentukan Wilayah itu dengan menambahkan --region parameter.

> **Note**
>
> Jika jejak adalah jejak organisasi dan Anda adalah akun anggota dalam 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 CloudTrail jika tidak dapat mengirimkan file log ke ember.

Mengonfigurasi pemilih CloudTrail acara Wawasan

Aktifkan peristiwa Insights pada jejak dengan menjalankanput-insight-selectors, dan menentukan `ApiCallRateInsightApiErrorRateInsight`,, atau keduanya sebagai nilai atribut. `InsightType` Untuk melihat setelan pemilih Insights untuk jejak, jalankan perintah. `get-insight-selectors` Anda harus menjalankan perintah ini dari AWS Wilayah tempat jejak dibuat (Wilayah 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 Insights`ApiErrorRateInsight`, jejak harus mencatat `read` atau `write` mengelola peristiwa.

Contoh jejak yang mencatat peristiwa Insights

*Contoh berikut digunakan **put-insight-selectors** untuk membuat pemilih acara Insights untuk jejak bernama TrailName 3.* Ini memungkinkan pengumpulan acara Insights untuk *TrailName3* jejak. Pemilih peristiwa Insights mencatat keduanya `ApiErrorRateInsight` dan jenis peristiwa `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 koleksi acara Insights

*Contoh berikut digunakan **put-insight-selectors** untuk menghapus pemilih peristiwa Insights untuk jejak bernama TrailName 3. Menghapus string JSON dari pemilih Insights menonaktifkan koleksi acara Insights untuk 3 jejak. TrailName*

```
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 penyeleksi acara

Untuk melihat pengaturan pemilih acara untuk jejak, jalankan `get-event-selectors` perintah. Anda harus menjalankan perintah ini dari AWS Wilayah tempat ia dibuat (Wilayah Rumah), 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 dalam organisasi di AWS Organizations, Anda harus memberikan ARN lengkap dari jejak itu, dan bukan hanya namanya.

Contoh berikut mengembalikan pengaturan default untuk pemilih acara untuk jejak.

```
{
    "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 Insights di jejak, pastikan pemilih acara mengaktifkan pencatatan jenis Wawasan yang ingin Anda konfigurasi jejak Anda. Untuk informasi selengkapnya tentang mencatat peristiwa Wawasan, lihatAcara Logging Insights.

Ketika suatu peristiwa terjadi di akun Anda, CloudTrail evaluasi konfigurasi untuk jejak Anda. Jika acara cocok dengan pemilih acara apa pun untuk jejak, jejak akan memproses dan mencatat peristiwa tersebut. Anda dapat mengonfigurasi hingga 5 penyeleksi acara untuk jejak dan hingga 250 sumber daya data untuk jejak. Untuk informasi selengkapnya, lihat Pencatatan peristiwa data.

Topik

Contoh jejak dengan pemilih acara tertentu

Contoh berikut membuat pemilih peristiwa untuk jejak bernama *TrailName* untuk menyertakan peristiwa manajemen hanya-baca dan hanya tulis, peristiwa data untuk dua kombinasi bucket/awalan 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:::mybucket/
prefix","arn:aws:s3:::mybucket2/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:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/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, termasuk peristiwa manajemen hanya-baca dan hanya tulis, dan semua peristiwa data untuk semua bucket Amazon S3, fungsi AWS Lambda , dan tabel Amazon DynamoDB di akun. AWS Karena contoh ini menggunakan pemilih peristiwa dasar, contoh ini tidak dapat mengonfigurasi pencatatan untuk peristiwa S3 AWS Outposts, panggilan Amazon Managed Blockchain JSON-RPC pada node Ethereum, atau jenis sumber daya pemilih acara lanjutan lainnya. Anda harus menggunakan pemilih acara lanjutan untuk mencatat peristiwa data untuk sumber daya tersebut. Untuk informasi selengkapnya, lihat Mengkonfigurasi pemilih acara tingkat lanjut.

> **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. Penyeleksi 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 penyeleksi 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 acara untuk jejak bernama *TrailName*untuk menyertakan peristiwa manajemen hanya-baca dan hanya tulis, 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. 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 pencatatan AWS KMS peristiwa.

Untuk mulai mencatat AWS KMS 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 acara 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 memulai logging 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 peristiwa volume rendah AWS Key Management Service yang relevan

Contoh berikut membuat pemilih acara untuk jejak bernama *TrailName*untuk menyertakan acara dan acara manajemen khusus tulis. 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. Pengguna dalam contoh ini telah memilih untuk menyertakan peristiwa AWS KMS Tulis, yang akan mencakup`Disable`, `Delete` dan`ScheduleKey`, tetapi tidak lagi menyertakan tindakan volume tinggi seperti`Encrypt`,`Decrypt`, dan `GenerateDataKey` (ini sekarang diperlakukan sebagai peristiwa Baca).

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

Contoh mengembalikan pemilih acara yang dikonfigurasi untuk jejak. Ini mencatat peristiwa manajemen khusus tulis, 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 bernama *TrailName*untuk menyertakan peristiwa manajemen hanya-baca dan hanya-tulis, tetapi untuk mengecualikan peristiwa Amazon RDS Data API. Karena peristiwa Amazon RDS Data API 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 Amazon RDS Data API dari setiap jejak kecuali satu. Untuk mengecualikan sumber peristiwa, tambahkan `ExcludeManagementEventSources` ke pemilih acara Anda, dan tentukan sumber peristiwa Amazon RDS Data API dalam nilai string:. `rdsdata.amazonaws.com`

Jika Anda memilih untuk tidak mencatat peristiwa manajemen, peristiwa Amazon RDS Data API tidak dicatat, dan Anda tidak dapat mengubah pengaturan pencatatan peristiwa.

Untuk mulai mencatat peristiwa pengelolaan Amazon RDS Data API ke jejak lagi, teruskan 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 acara 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 pengelolaan Amazon RDS Data API ke jejak lagi, teruskan 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]}]'
```

Mengkonfigurasi pemilih acara tingkat lanjut

Untuk menggunakan pemilih acara lanjutan untuk menyertakan atau mengecualikan peristiwa data alih-alih pemilih acara dasar, gunakan pemilih acara lanjutan di halaman detail jejak. Penyeleksi acara tingkat lanjut memungkinkan Anda mencatat peristiwa data pada lebih banyak jenis sumber daya daripada pemilih acara dasar. Selektor dasar mencatat aktivitas objek S3, aktivitas eksekusi AWS Lambda fungsi, dan tabel DynamoDB.

Di pemilih peristiwa lanjutan, buat ekspresi untuk mengumpulkan peristiwa data pada jenis sumber daya tertentu seperti bucket S3, fungsi, tabel DynamoDB AWS Lambda , titik akses Lambda Objek S3, API langsung Amazon EBS pada snapshot EBS, titik akses S3, aliran DynamoDB, tabel yang dibuat oleh Lake Formation, dan banyak lagi. AWS Glue

Untuk informasi selengkapnya pemilih acara lanjutan, lihatMengkonfigurasi pemilih acara tingkat lanjut.

Untuk melihat pengaturan pemilih acara lanjutan untuk jejak, jalankan `get-event-selectors` perintah berikut. Anda harus menjalankan perintah ini dari AWS Wilayah tempat jejak dibuat (Wilayah Rumah), 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 jejak, dan bukan hanya namanya.

Contoh berikut mengembalikan pengaturan default untuk pemilih acara lanjutan untuk jejak. Secara default, tidak ada pemilih acara lanjutan yang dikonfigurasi untuk jejak.

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Untuk membuat pemilih acara lanjutan, jalankan `put-event-selectors` perintah. Ketika peristiwa data terjadi di akun Anda, CloudTrail evaluasi konfigurasi untuk jejak Anda. Jika acara cocok dengan pemilih acara lanjutan mana pun untuk jejak, jejak akan memproses dan mencatat peristiwa tersebut. Anda dapat mengonfigurasi hingga 500 kondisi pada jejak, termasuk semua nilai yang ditentukan untuk semua penyeleksi acara lanjutan di jejak Anda. Untuk informasi selengkapnya, lihat Pencatatan peristiwa data.

Topik

- Contoh jejak dengan pemilih acara lanjutan tertentu
- Contoh jejak yang menggunakan pemilih peristiwa lanjutan khusus untuk mencatat Amazon S3 AWS Outposts pada peristiwa data
- Contoh jejak yang menggunakan penyeleksi acara lanjutan untuk mengecualikan AWS Key Management Service acara
- Contoh jejak yang menggunakan penyeleksi peristiwa lanjutan untuk mengecualikan peristiwa manajemen Amazon RDS Data API

Contoh jejak dengan pemilih acara lanjutan tertentu

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 kombinasi bucket/awalan Amazon S3 kecuali untuk bucket bernama dan peristiwa data untuk fungsi bernama. `sample_bucket_name` 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:::sample_bucket_name/"] }
    ]
  },
  {
    "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:::sample_bucket_name/" ]
        },
      ]
    },
{
      "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"
}
```

Contoh jejak yang menggunakan pemilih peristiwa lanjutan khusus untuk mencatat Amazon S3 AWS Outposts pada 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 peristiwa untuk `resources.type` bidang tersebut 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 penyeleksi acara lanjutan untuk mengecualikan AWS Key Management Service acara

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 jejak yang menggunakan penyeleksi peristiwa lanjutan untuk mengecualikan peristiwa manajemen Amazon RDS Data API

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 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"] }
    ]
  }
]'
```

Menghentikan dan memulai pencatatan untuk jalan setapak

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 peristiwa ke bucket. Jika Anda tidak berhenti masuk, CloudTrail coba kirimkan file log ke bucket dengan nama yang sama untuk jangka waktu terbatas.
> Jika Anda berhenti mencatat atau menghapus jejak, CloudTrail Wawasan akan dinonaktifkan pada jejak tersebut.

Menghapus jejak

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.

Anda dapat menghapus jejak dengan perintah berikut. Anda dapat menghapus jejak hanya di Wilayah itu dibuat (Wilayah Rumah).

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

Saat menghapus jejak, Anda tidak menghapus bucket Amazon S3 atau topik Amazon SNS yang terkait dengannya. Gunakan AWS Management Console, AWS CLI, atau API layanan untuk menghapus sumber daya ini secara terpisah.

Membuat jejak untuk 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 OPT, 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 OPT, salinan jejak 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.

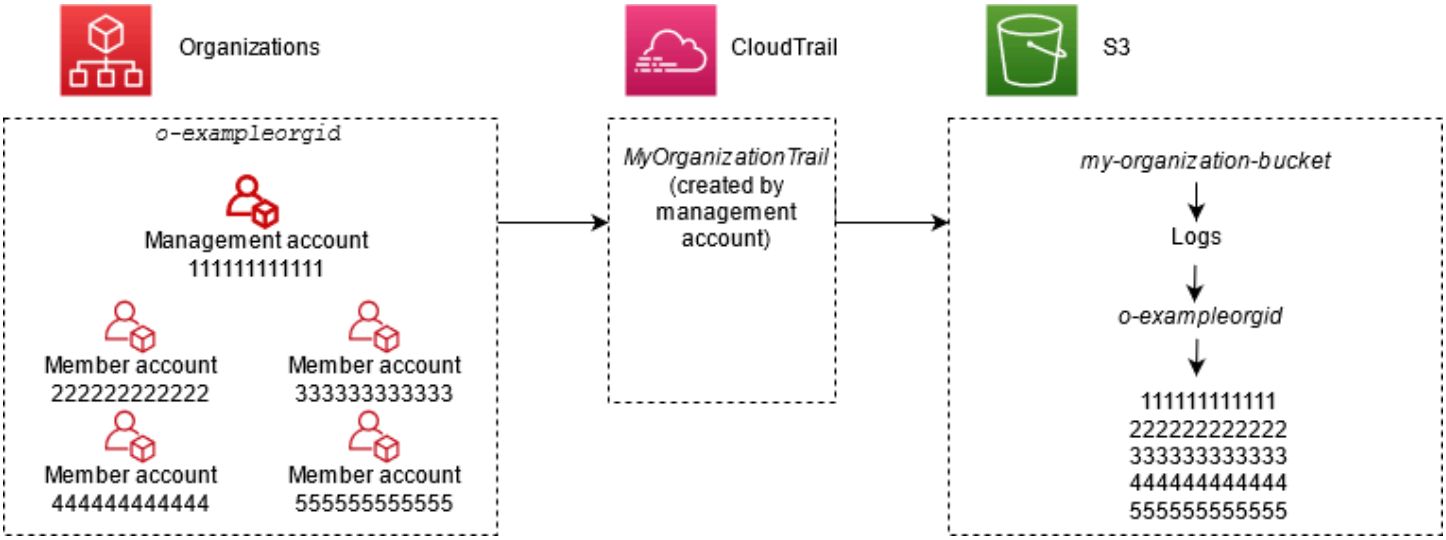
> **Note**
>
> CloudTrail membuat jejak organisasi di akun anggota meskipun validasi sumber daya gagal. Contoh kegagalan validasi meliputi:
>
> - kebijakan bucket Amazon S3 yang salah
> - kebijakan topik Amazon SNS yang salah
> - ketidakmampuan untuk mengirimkan ke grup CloudWatch log Log
> - izin yang 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 AWS 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, atau saat Anda mengaktifkan CloudTrail sebagai layanan tepercaya di Organizations, ini akan membuat 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 MyOrganizationTrailuntuk organisasi 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 *my-organization-bucket*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 4444444444444444, 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 di semua Wilayah atau satu Wilayah, dan jenis acara 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, lihatBekerja dengan file CloudTrail log.

> **Note**
>
> Di konsol, Anda membuat jejak yang mencatat semua Wilayah. Ini adalah praktik terbaik yang direkomendasikan; aktivitas logging di semua Wilayah membantu Anda menjaga AWS lingkungan Anda lebih aman. Untuk membuat jejak wilayah Tunggal, gunakan. AWS CLI

Anda juga 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

Sejarah acara dan jalur organisasi

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.

Praktik terbaik untuk berpindah 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. 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
```

```
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "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 Command Line Interface.
- 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.

```
{
    "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 inPemantauan CloudTrail Log Files dengan Amazon CloudWatch Log. 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
- KonfigurasikanAWS KMSkebijakan 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.

Anda dapat mengonfigurasi jejak organisasi dengan berbagai cara. Misalnya, Anda dapat mengonfigurasi detail berikut untuk jejak organisasi Anda:

- Secara default, saat Anda membuat jejak di konsol, jejak mencatat semua Wilayah AWS di AWS partisi tempat Anda bekerja. Sebagai praktik terbaik, kami sangat menyarankan acara logging di semua Wilayah di Anda Akun AWS. Untuk membuat jejak untuk satu Wilayah, gunakan AWS CLI. Untuk informasi selengkapnya, lihat Bagaimana cara CloudTrail kerja.
- Tentukan apakah akan menerapkan jejak ke organisasi Anda. Secara default, jejak tidak diterapkan ke organisasi. Anda harus memilih opsi ini untuk membuat jejak organisasi.
- Tentukan bucket Amazon S3 mana yang menerima file log untuk jejak organisasi. Anda dapat memilih bucket Amazon S3 yang ada, atau membuatnya khusus untuk jejak organisasi.
- Untuk peristiwa manajemen dan data, tentukan apakah Anda ingin mencatat peristiwa Baca, Menulis peristiwa, atau keduanya. CloudTrailInsights event dicatat hanya pada event manajemen. Anda dapat menentukan peristiwa data pencatatan untuk sumber daya di akun manajemen dengan memilihnya dari daftar di konsol, dan di akun anggota jika Anda menentukan ARN dari setiap sumber daya yang ingin Anda aktifkan pencatatan peristiwa data. Untuk informasi selengkapnya, lihat Peristiwa data.

Untuk membuat jejak organisasi dengan AWS Management Console

1. Masuk ke AWS Management Console 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.
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 enkripsi SSE-KMS berkas Log, pilih Diaktifkan jika Anda ingin mengenkripsi file log Anda menggunakan enkripsi SSE-KMS alih-alih enkripsi SSE-S3. Defaultnya adalah Diaktifkan. Jika Anda tidak mengaktifkan enkripsi SSE-KMS, log 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).

   Jika Anda mengaktifkan enkripsi SSE-KMS, 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.

   > **Note**
   >
   > Anda juga dapat mengetikkan ARN kunci dari akun lain. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda. Kebijakan kunci harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasikanAWS KMSkebijakan 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 berkas 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 yang berlaku untuk semua Wilayah, pemberitahuan SNS untuk pengiriman file log dari semua Wilayah 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 selengkapnya, lihat Panduan Memulai Layanan Notifikasi Sederhana Amazon.

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, tambahkan satu atau beberapa tag kustom (pasangan nilai kunci) 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. Lihat informasi yang lebih lengkap di AWS Resource Groups dan Mengapa menggunakan tag untuk CloudTrail sumber daya?.

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 Acara 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. Volume rendah, AWS KMS tindakan yang relevan sepertiDisable,Delete, dan ScheduleKey (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

Untuk mengecualikan peristiwa bervolume tinggi sepertiEncrypt,Decrypt, danGenerateDataKey, tetapi masih mencatat peristiwa yang relevan sepertiDisable, Delete danScheduleKey, 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 Harga AWS CloudTrail.

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 peristiwa data 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 peristiwa Data, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data. Untuk informasi selengkapnya tentang tipe peristiwa data yang tersedia, lihatPeristiwa data.

    Note

    Untuk mencatat peristiwa data untuk AWS Glue tabel yang dibuat oleh Lake Formation, pilih Lake Formation.

13. Pilih templat pemilih log. CloudTrail termasuk template yang telah ditetapkan yang mencatat semua peristiwa data untuk jenis sumber daya. Untuk membuat template pemilih log kustom, pilih Kustom.

> **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 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 (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. Di Advanced event selectors, buat ekspresi untuk sumber daya spesifik tempat Anda ingin mencatat peristiwa data. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

    a. Pilih dari bidang berikut.

- **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Peristiwa data hanya-baca 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,PutItem, atauGetSnapshotBlock.
- **`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`

  Tabel berikut menunjukkan format ARN yang valid untuk masing-masing. `resources.type`

  > **Note**
  >
  > Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

resources.type	Sumber Daya.arn
`AWS::DynamoDB::Table` [1]	`arn:partition :dynamodb : region:account_ID :table/table_name`
`AWS::Lambda::Function`	`arn:partition :lambda:region:account_ID :function: function_name`
`AWS::S3::Object` [2]	`arn:partition :s3:::bucket_name / arn:partition :s3:::bucket_name /object_or_file_name /`

resources.type	Sumber Daya.arn
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	Sumber Daya.arn
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	Sumber Daya.arn
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*

resources.type	Sumber Daya.arn
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	Sumber Daya.arn
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	Sumber Daya.arn
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	Sumber Daya.arn
AWS::SSM::ManagedNode	ARN harus berada dalam salah satu format berikut: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	Sumber Daya.arn
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table`. Jika Anda menentukan `AWS::DynamoDB::Table` untuk`resources.type`, itu akan mencatat kedua tabel DynamoDB dan peristiwa aliran DynamoDB secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.

[2] Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok. Slash trailing disengaja; jangan mengecualikannya.

[3] Untuk mencatat peristiwa pada semua objek di titik akses S3, kami sarankan Anda hanya menggunakan titik akses ARN, jangan sertakan jalur objek, dan gunakan `StartsWith` operator atau. `NotStartsWith`

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Tindakan, sumber daya, dan kunci kondisi di AWS Identity and Access Management Panduan Pengguna.

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 jejak Anda, Anda dapat mengatur bidang ke Resources.arn, menyetel operator untuk tidak memulai, lalu menempelkan di ARN bucket S3, atau menelusuri 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.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi di jalan setapak. 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.
> 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 mencatat semua fungsi dengan template pemilih yang telah ditentukan, 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.

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 tipe data lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 12 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk tipe peristiwa data.
17. 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 Wawasan 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, lihatAcara Logging Insights. 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`S3bucketName/AWSLogs/CloudTrail/`, nama bucket S3 dengan awalan baru akan diberi nama. `S3bucketName/AWSLogs/CloudTrail-Insight/`

18. Setelah selesai memilih jenis acara untuk dicatat, pilih Berikutnya.
19. 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.
20. Jejak baru muncul di halaman Trails. Jejak organisasi mungkin membutuhkan waktu hingga 24 jam untuk dibuat di semua Wilayah 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.
- 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 kustom (pasangan kunci-nilai) 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 Command Line Interface

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 Anda telah menginstal atau memperbarui ke AWS CLI versi terbaru sebelum memulai.

> **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 *myOrganizationBucket*, yang dimiliki oleh akun manajemen organisasi. Ganti *myOrganizationBucket*, *region*, *ManagementAccountID, trailName, dan O-OrganizationId* dengan 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "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:::myOrganizationBucket/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:::myOrganizationBucket/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*my-bucket*:

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-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": "my-bucket"
}
```

> **Note**
>
> Jalankan `start-logging` perintah untuk mulai mencatat jejak Anda. Untuk informasi selengkapnya, lihat Menghentikan dan memulai pencatatan untuk jalan setapak.

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 my-bucket --is-
organization-trail
```

Untuk informasi selengkapnya, lihat Persyaratan penamaan.

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": "my-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 update-trail 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 dibuat.

> **Note**
>
> Jika Anda menggunakan AWS CLI atau salah satu AWS SDK untuk memperbarui jejak, pastikan bahwa kebijakan bucket trail tersebut. up-to-date Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dengan AWS Command Line Interface.
> 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": "my-bucket"
}
```

Pada contoh sebelumnya, jejak dikonfigurasi untuk diterapkan ke semua Regions ()`"IsMultiRegionTrail": true`. Jejak yang diterapkan hanya pada satu Wilayah akan ditampilkan `"IsMultiRegionTrail": false` dalam output.

Mengonversi jejak organisasi yang berlaku untuk satu Wilayah untuk diterapkan ke semua Wilayah

Untuk mengubah jejak organisasi yang ada sehingga berlaku untuk semua 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 berlaku untuk semua Wilayah, `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": "my-bucket"
}
```

Pemecahan Masalah

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.

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 Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Melihat acara CloudTrail Wawasan untuk jalur

Setelah mengaktifkan CloudTrail Insights on a trail, Anda dapat melihat hingga 90 hari peristiwa Insights menggunakan CloudTrail konsol atau. AWS CLI Bagian ini menjelaskan cara melihat, mencari, dan mengunduh file peristiwa Wawasan. Untuk informasi tentang penggunaan `LookupEvents` API untuk mengambil informasi dari CloudTrail peristiwa, lihat Referensi AWS CloudTrail API. Untuk informasi lebih lanjut tentang CloudTrail Wawasan, lihat Acara Logging Insights di panduan ini.

Untuk informasi tentang cara membuat jejak, lihat Membuat jejak danMendapatkan dan melihat file CloudTrail log Anda.

> **Note**
>
> Untuk mencatat peristiwa Insights pada volume panggilan API, jejak harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mencatat `read` atau `write` mengelola peristiwa.

Topik

- Melihat peristiwa CloudTrail Wawasan untuk jejak di konsol CloudTrail
- Melihat acara CloudTrail Wawasan untuk jalur dengan AWS CLI

Melihat peristiwa CloudTrail Wawasan untuk jejak di konsol CloudTrail

Setelah Anda mengaktifkan peristiwa CloudTrail Insights di jejak, saat CloudTrail mendeteksi aktivitas API atau tingkat kesalahan yang tidak biasa, buat peristiwa CloudTrail Insights dan tampilkan peristiwa tersebut di halaman Dasbor dan Wawasan di halaman. AWS Management Console Anda dapat melihat peristiwa Wawasan di konsol dan memecahkan masalah aktivitas yang tidak biasa. Acara Insights 90 hari terbaru ditampilkan di konsol. Anda juga dapat mengunduh acara Insights dengan menggunakan AWS CloudTrail konsol. Anda dapat secara terprogram mencari acara dengan

menggunakan AWS SDK atau. AWS Command Line Interface Untuk informasi selengkapnya tentang acara CloudTrail Wawasan, lihat Acara Logging Insights di panduan ini.

> **Note**
>
> Untuk mencatat peristiwa Insights pada volume panggilan API, jejak harus mencatat peristiwa `write` manajemen. Untuk mencatat peristiwa Insights pada tingkat kesalahan API, jejak harus mencatat `read` atau `write` mengelola peristiwa.

Setelah peristiwa Wawasan dicatat, peristiwa ditampilkan di halaman Wawasan selama 90 hari. Anda tidak dapat menghapus peristiwa secara manual dari halaman Wawasan. Karena Anda harus membuat jejak sebelum mengaktifkan CloudTrail Insights, Anda dapat melihat peristiwa Insights yang dicatat ke jejak Anda selama Anda menyimpannya di bucket S3 yang dikonfigurasi dalam pengaturan jejak Anda.

Pantau log jejak Anda dan beri tahu saat aktivitas peristiwa Wawasan tertentu terjadi dengan Log Amazon CloudWatch . Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Untuk melihat acara Insights

CloudTrail Acara Insights harus diaktifkan di jejak Anda untuk melihat peristiwa Insights di konsol. Biarkan hingga 36 jam CloudTrail untuk menyampaikan peristiwa Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/home/.
2. Di panel navigasi, pilih Dasbor untuk melihat lima peristiwa Wawasan terbaru, atau Wawasan untuk melihat semua peristiwa Wawasan yang masuk ke akun Anda dalam 90 hari terakhir.

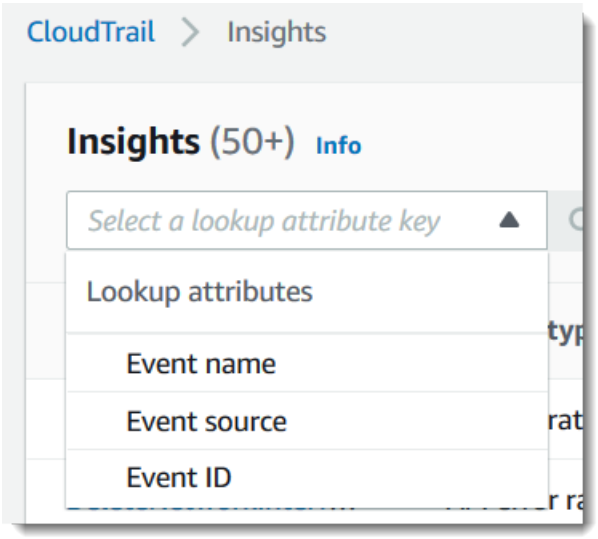
   Di halaman Wawasan, Anda dapat memfilter peristiwa Insights berdasarkan kriteria termasuk sumber API peristiwa, nama peristiwa, dan ID peristiwa, serta membatasi peristiwa yang ditampilkan pada peristiwa yang terjadi dalam rentang waktu tertentu. Untuk informasi selengkapnya tentang memfilter peristiwa Wawasan, lihat. Memfilter acara Wawasan

Daftar Isi

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

Memfilter acara Wawasan

Tampilan default peristiwa di Wawasan menunjukkan peristiwa dalam urutan kronologis terbalik. Acara Insights terbaru, diurutkan berdasarkan waktu mulai acara, berada di puncak. Daftar berikut menjelaskan atribut yang tersedia. Anda dapat memfilter pada tiga atribut pertama: Nama acara, Sumber acara, dan ID Acara.



Nama peristiwa

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

Jenis wawasan

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

Sumber peristiwa

AWSLayanan tempat permintaan dibuat, seperti `iam.amazonaws.com` ataus`3.amazonaws.com`. Anda dapat menggulir daftar sumber acara setelah Anda memilih filter sumber acara.

ID peristiwa

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

Waktu mulai acara

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

Rata-rata dasar

Pola normal tingkat panggilan API atau aktivitas tingkat kesalahan. Rata-rata dasar dihitung selama tujuh hari sebelum dimulainya acara Insights. Meskipun nilai durasi dasar — periode yang CloudTrail menganalisis aktivitas normal pada APIS — adalah sekitar tujuh hari, membulatkan durasi dasar menjadi satu hari bilangan CloudTrail bulat penuh, sehingga durasi dasar yang tepat dapat bervariasi.

Rata-rata wawasan

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

Perubahan nilai

Perbedaan antara nilai rata-rata Baseline dan rata-rata Insight, diukur sebagai persentase. Misalnya, jika rata-rata dasar `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 Insights dicatat karena aktivitas berada di bawah rata-rata baseline, perubahan Rate menunjukkan panah bawah di samping persentase.

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 lookup dari menu drop-down, 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 berakhir.

Untuk memfilter berdasarkan tanggal dan waktu mulai dan berakhir

1. Untuk mempersempit rentang waktu untuk peristiwa yang ingin Anda lihat, pilih rentang waktu pada bilah rentang waktu di bagian atas tabel. Rentang waktu preset meliputi 30 menit, 1 jam, 3 jam, atau 12 jam. Untuk menentukan rentang waktu kustom, pilih Kustom.
2. Pilih salah satu tab berikut.
   - Absolute - Memungkinkan Anda memilih waktu tertentu. Lanjutkan ke langkah berikutnya.
   - Relatif terhadap acara yang dipilih - Dipilih secara default. Memungkinkan Anda memilih periode waktu relatif terhadap waktu mulai acara Wawasan. Lanjutkan ke langkah 4.
3. Untuk mengatur rentang waktu Absolute, lakukan hal berikut.
   a. Pada tab Absolute, pilih hari yang Anda inginkan untuk memulai rentang waktu. 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 Apply (Terapkan).
4. Untuk menyetel Relatif ke rentang waktu acara yang dipilih, lakukan hal berikut.

a. Pilih periode waktu yang telah ditetapkan relatif terhadap waktu mulai acara Insights. Nilai preset tersedia dalam hitungan menit, jam, hari, atau minggu. Periode waktu relatif maksimum adalah 12 minggu.

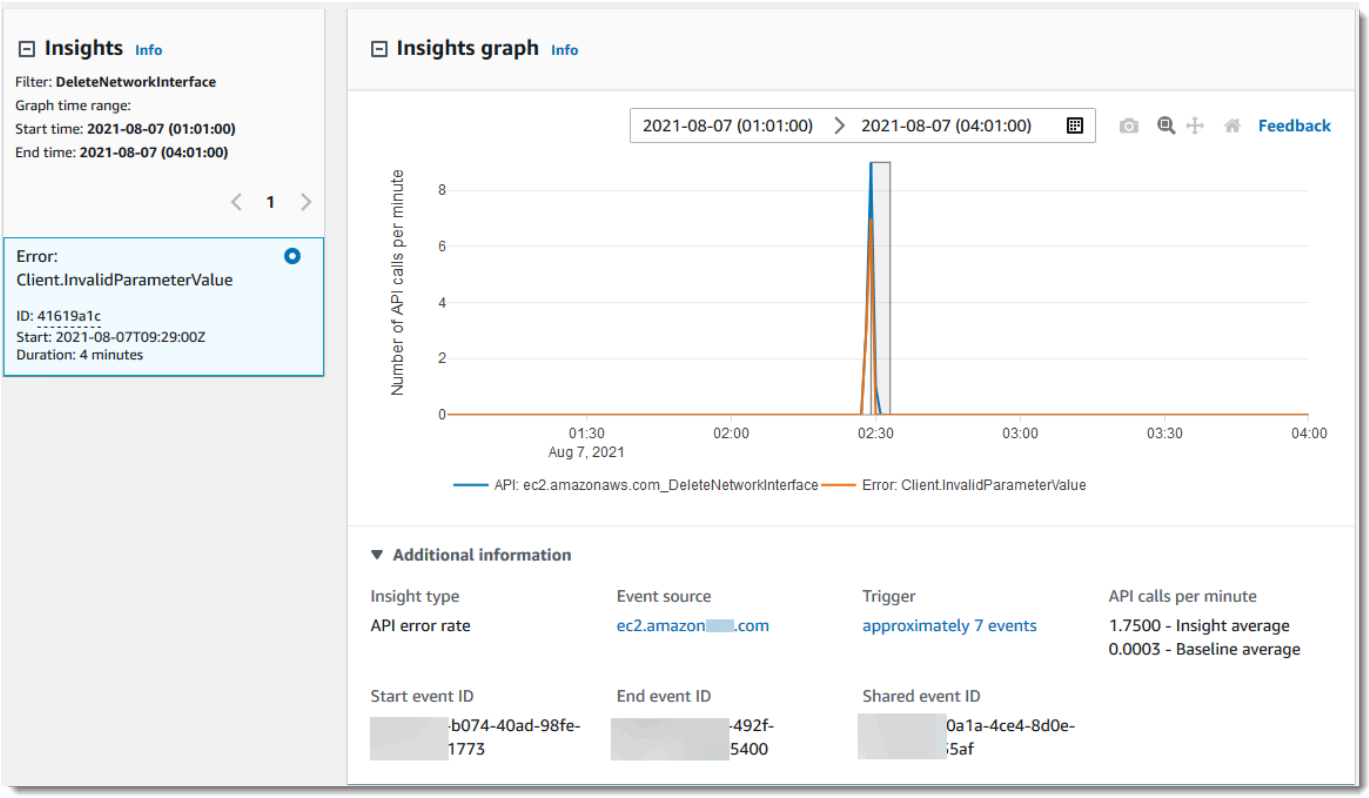
b. Jika diperlukan, sesuaikan nilai preset di kotak di bawah preset. Pilih Hapus untuk mengatur ulang perubahan Anda jika diperlukan. Ketika Anda telah mengatur waktu relatif yang Anda inginkan, pilih Terapkan.

5. Di Kepada, pilih hari dan tentukan waktu yang Anda inginkan untuk menjadi akhir rentang waktu. Pilih Apply (Terapkan).

6. Untuk menghapus filter rentang waktu, pilih ikon kalender di sebelah kanan kotak Rentang waktu, lalu pilih Hapus.

Melihat detail acara Wawasan

1. Pilih acara Wawasan dalam daftar hasil untuk menampilkan detailnya. Halaman detail untuk acara Insights menunjukkan grafik timeline aktivitas yang tidak biasa.



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

Informasi berikut ditampilkan di area informasi tambahan dari grafik:

- Jenis wawasan. Ini bisa berupa tingkat panggilan API atau tingkat kesalahan API.
- Pemicu. Ini adalah tautan ke tab peristiwa Cloudtrail, yang mencantumkan peristiwa manajemen yang dianalisis untuk menentukan bahwa aktivitas yang tidak biasa terjadi.
- Panggilan API per menit
  - Rata-rata dasar - Tingkat kejadian tipikal per menit pada API tempat peristiwa Insights dicatat, yang diukur dalam kira-kira tujuh hari sebelumnya, di Wilayah tertentu di akun Anda.
  - Insights average - Tingkat kemunculan per menit pada API ini yang memicu peristiwa Insights. Rata-rata CloudTrail Insights untuk acara mulai adalah tingkat panggilan atau error per menit pada API yang memicu peristiwa Insights. Biasanya, ini adalah menit pertama aktivitas yang tidak biasa. Rata-rata Insights untuk acara akhir adalah tingkat panggilan API atau error per menit selama durasi aktivitas yang tidak biasa, antara peristiwa Insights awal dan peristiwa Insights akhir.
- Sumber acara. Titik akhir AWS layanan di mana jumlah panggilan atau kesalahan API yang tidak biasa dicatat. Pada gambar sebelumnya, sumbernya adalah, yang merupakan `ec2.amazonaws.com` titik akhir layanan untuk Amazon EC2.
- ID acara.
  - Mulai ID peristiwa - ID peristiwa Wawasan yang dicatat pada awal aktivitas yang tidak biasa.
  - End event ID - ID peristiwa Insights yang dicatat pada akhir aktivitas yang tidak biasa.
  - ID peristiwa bersama - Dalam peristiwa Wawasan, ID peristiwa Bersama adalah GUID yang dihasilkan oleh CloudTrail Wawasan untuk mengidentifikasi pasangan awal dan akhir peristiwa Wawasan secara unik. ID peristiwa bersama adalah umum antara peristiwa Wawasan awal dan akhir, dan membantu menciptakan korelasi antara kedua peristiwa tersebut untuk mengidentifikasi aktivitas yang tidak biasa secara unik.

3. Pilih tab Atribusi untuk melihat informasi tentang identitas pengguna, agen pengguna, dan peristiwa Insights rasio panggilan API, kode kesalahan yang berkorelasi dengan aktivitas dasar dan tidak biasa. Maksimal lima identitas pengguna, lima agen pengguna, dan lima kode kesalahan ditampilkan dalam tabel pada tab Atribusi, diurutkan berdasarkan rata-rata jumlah aktivitas, dalam urutan menurun dari tertinggi ke terendah. Untuk informasi selengkapnya tentang tab Atribusi, lihat Tab Atribusi dan CloudTrail Wawasan`insightDetails`elemen di panduan ini.

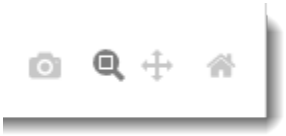
4. Pada tab CloudTrail peristiwa, lihat peristiwa terkait yang CloudTrail dianalisis untuk menentukan bahwa aktivitas yang tidak biasa terjadi. Secara default, filter sudah diterapkan untuk nama acara Insights, yang juga merupakan nama API terkait. Tab CloudTrail peristiwa menampilkan peristiwa CloudTrail manajemen yang terkait dengan API subjek yang terjadi antara waktu mulai (minus satu menit) dan waktu akhir (ditambah satu menit) dari peristiwa Insights.

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

   Untuk menampilkan semua CloudTrail peristiwa yang dicatat selama durasi acara Insights, dan tidak hanya untuk API terkait, matikan filter.
5. Pilih tab Catatan peristiwa Insights untuk melihat peristiwa awal dan akhir Wawasan dalam format JSON.
6. Memilih sumber Peristiwa yang ditautkan 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 di halaman detail peristiwa Wawasan dengan menggunakan bilah alat di sudut kanan atas.

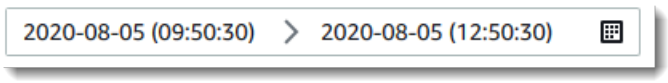


Dari kiri ke kanan, tombol perintah pada toolbar grafik melakukan hal berikut:

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

Ubah pengaturan rentang waktu grafik

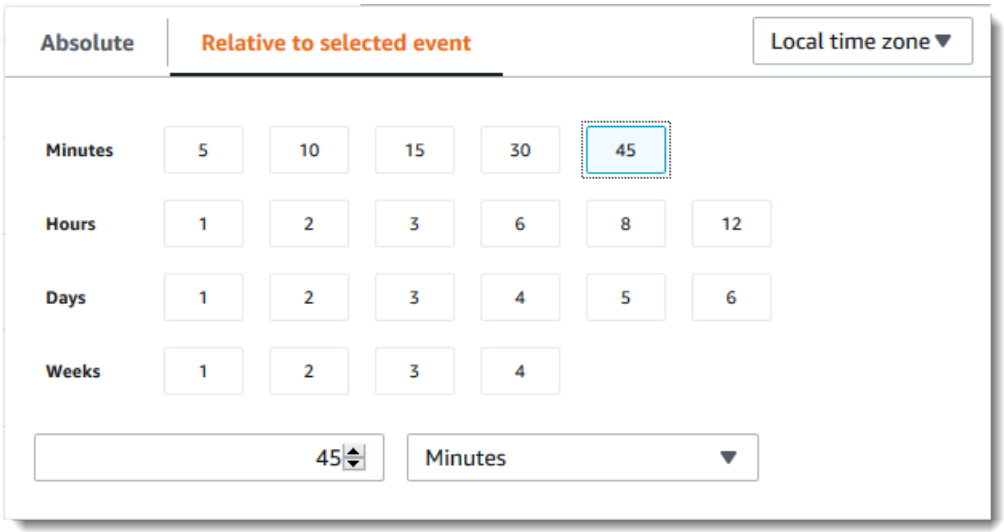
Anda dapat mengubah rentang waktu—durasi peristiwa yang dipilih yang ditampilkan pada sumbu x—yang ditampilkan dalam grafik dengan memilih pengaturan di sudut kanan atas grafik.



Rentang waktu default yang ditampilkan dalam grafik bergantung pada durasi acara Wawasan yang dipilih.

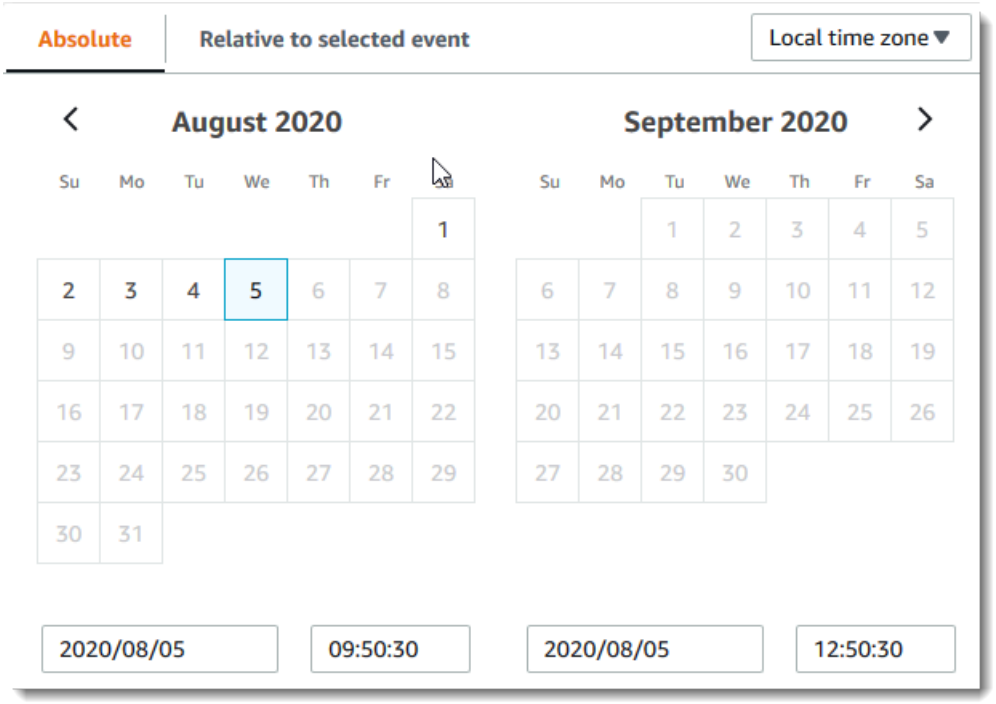
Durasi acara Insights	Rentang waktu default
Kurang dari 4 jam	3 jam (tiga jam)
Antara 4 dan 12 jam	12 jam (12 jam)
Antara 12 dan 24 jam	1d (satu hari)
Antara 24 dan 72 jam	3d (tiga hari)
Lebih dari 72 jam	1w (satu minggu)

Anda dapat memilih preset lima menit, 30 menit, satu jam, tiga jam, 12 jam, atau Custom. Gambar berikut menunjukkan Relatif terhadap periode waktu acara yang dipilih yang dapat Anda pilih di Pengaturan khusus. Periode waktu relatif adalah perkiraan periode waktu sekitar awal dan akhir acara Wawasan yang dipilih yang ditampilkan di halaman detail acara Wawasan.



Untuk menyesuaikan preset yang dipilih, tentukan nomor dan satuan waktu di kotak di bawah preset.

Untuk menentukan tanggal dan rentang waktu yang tepat, pilih tab Absolute. Jika Anda menetapkan tanggal dan rentang waktu absolut, waktu mulai dan akhir diperlukan. Untuk informasi tentang cara mengatur waktu, lihat the section called “Memfilter acara Wawasan” di topik ini.



Mengunduh acara Wawasan

Anda dapat mengunduh riwayat peristiwa Wawasan 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 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. Sebagai praktik keamanan terbaik, 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 tiga hari terakhir aktivitas.
2. Pilih Unduh acara, lalu pilih Unduh CSV atau Unduh 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 Anda selesai, buka file untuk melihat peristiwa yang Anda tentukan.
4. Untuk membatalkan unduhan Anda, pilih Batalkan unduhan. Jika Anda membatalkan unduhan sebelum selesai, file CSV atau JSON di komputer lokal Anda mungkin hanya berisi sebagian dari acara Anda.

Melihat acara CloudTrail Wawasan untuk jalur dengan AWS CLI

Anda dapat mencari acara CloudTrail Insights selama 90 hari terakhir dengan menjalankan aws cloudtrail lookup-events perintah. `lookup-events`Perintah memiliki opsi berikut:

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--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

- Untuk menjalankan AWS CLI perintah, Anda harus menginstal file AWS CLI. Untuk informasi selengkapnya, lihat Menginstal Antarmuka Baris AWS Perintah.
- 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 Mengonfigurasi Antarmuka Baris AWS Perintah.
- Untuk mencatat peristiwa Insights pada volume 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 melihat sepuluh 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": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "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
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
          "awsRegion": "us-east-1",
          "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
          "eventType": "AwsCloudTrailInsight",
          "recipientAccountId": "123456789012",
          "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
          "insightDetails": {
          "state": "End",
          "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
                    }
                  ]
                }
              ]
            }
          },
            "eventCategory": "Insight"
        }
    ]
}
```

Untuk penjelasan tentang bidang terkait pencarian di output, lihat Bidang keluaran pencarian di topik ini. Untuk penjelasan bidang dalam acara Wawasan, lihatCloudTrail isi rekaman.

Menentukan jumlah peristiwa Insights yang akan dikembalikan

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

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

Nilai default untuk<integer>, jika tidak ditentukan, adalah 10. Nilai yang mungkin adalah 1 hingga 50. Contoh berikut mengembalikan satu hasil.

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

Mencari acara Wawasan berdasarkan rentang waktu

Insights event 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 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
```

Menentukan halaman hasil berikutnya

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
```

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 lanjut, lihat Menghasilkan Parameter JSON CLI Skeleton dan CLI 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`.

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 Acara Logging Insights di panduan ini.

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, lihatBuat penyimpanan data acara untuk CloudTrail acara.

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 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.
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

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 (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 *myBucketName*, *eventDataStoremyAccountID, region, prefix, dan Id* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* adalah ID AWS akun yang digunakan untuk CloudTrail Lake, yang mungkin tidak sama dengan ID AWS akun untuk bucket S3.

Ganti *key-region*, *keyAccountID, 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:::myBucketName"
      ],
      "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:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/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 *eventDataStoremyAccountID, region, dan Id* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* adalah ID AWS akun 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.

Anda dapat menambahkan pernyataan berikut ke kebijakan bucket S3 untuk memberikan izin ini. Ganti *roLearn* dan *myBucketName*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:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

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 *roLearn*, *myBucketName*, *eventDataStoremyAccountID, region, dan Id* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* 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:::myBucketName/*"
    },
    "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, lihatBuat penyimpanan data acara untuk CloudTrail acara.

> **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 AWS Management Console 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, lihatRincian salinan acara.

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

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”
- Pengenal 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:

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/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:
>
> ```
> bucket_name/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
    Bucket_Name
        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 isi rekaman.

Mengunduh CloudTrail file log

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.

Misalnya, jika Anda menggunakan Mozilla Firefox, Anda juga dapat mengunduhJSONViewadd-on. Dengan JSONView, Anda dapat mengklik dua kali file.gz terkompresi di bucket Anda untuk membuka file log dalam format JSON.

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, lihatBekerja dengan Objek Amazon S3diPanduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Prosedur berikut menjelaskan cara mengunduh file log denganAWS Management Console.

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. PilihUnduhatauUnduh sebagaidan 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 seperti7-Zipuntuk 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 referensi acara log.

AWSbermitra dengan spesialis pihak ketiga dalam pencatatan dan analisis untuk memberikan solusi yang menggunakan CloudTrail keluaran. Untuk informasi selengkapnya, lihatAWSJaringan Mitra - AWS CloudTrailMitra.

> **Note**
>
> Anda juga dapat menggunakanSejarah kejadianfitur untuk mencari acara untuk membuat, memperbarui, dan menghapus aktivitas API selama 90 hari terakhir.
> Untuk informasi selengkapnya, lihat Bekerja dengan Riwayat CloudTrail Acara.

Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail

Anda dapat diberitahu ketika 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 mengonfigurasi CloudTrail 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 dapat mendapatkan pembaruan yang dikirim ke antrean Amazon Simple Queue Service (Amazon SQS), yang memungkinkan Anda untuk menangani notifikasi ini secara terprogram.

Topik

- Mengkonfigurasi CloudTrail untuk mengirim pemberitahuan

Mengkonfigurasi CloudTrail untuk mengirim pemberitahuan

Anda dapat mengonfigurasi jejak untuk menggunakan topik Amazon SNS. Anda dapat menggunakan CloudTrail konsol ataucreate-trail aws cloudtrailPerintah CLI untuk membuat topik. CloudTrail membuat topik Amazon SNS untuk Anda dan melampirkan kebijakan yang sesuai, sehingga CloudTrail memiliki izin untuk mempublikasikan ke topik itu.

Saat Anda membuat nama topik SNS, nama tersebut 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 yang berlaku untuk semua 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 pemberitahuan, berlangganan topik Amazon SNS atau topik yang CloudTrail menggunakan. Anda melakukan ini dengan konsol Amazon SNS atau perintah Amazon SNS CLI. Untuk informasi selengkapnya, lihatBerangganan topikdiPanduan Developer Amazon Simple Notification Service.

> **Note**
>
> CloudTrail mengirimkan pemberitahuan ketika file log ditulis ke ember 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, lihatBerangganan antrean ke topik Amazon SNSdiPanduan Pengembang Amazon Simple Queue Service Amazon Simple Queue Service.

Notifikasi Amazon SNS terdiri dari objek JSON yang menyertakan`Message`elapangan. The`Message`bidang daftar jalur lengkap ke file log, seperti yang ditunjukkan pada contoh berikut:

```
{
    "s3Bucket": "your-bucket-name","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": "your-bucket-name",
    "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 notifikasi melalui email, isi email terdiri dari isi`Message`lapangan. Untuk deskripsi lengkap tentang struktur JSON, lihatMengirim Pesan Amazon SNS ke Antrian Amazon SQSdiPanduan Developer Amazon Simple Notification Service. Hanya`Message`lapangan menunjukkan CloudTrail informasi. Bidang lainnya berisi informasi dari layanan Amazon SNS.

Jika Anda membuat jejak dengan CloudTrail API, Anda dapat menentukan topik Amazon SNS yang ada yang Anda inginkan CloudTrail untuk mengirim pemberitahuan ke 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 Amazon SNS dan berlangganan topik Amazon SNS dan berlangganan topik Amazon SNS dan berlangganan topik Amazon SNS dan berlangganan topikPanduan Developer Amazon Simple Notification Service.

Kiat untuk mengelola jalur

- Mulai 12 April 2019, jejak hanya dapat dilihat di Wilayah AWS tempat mereka mencatat peristiwa. Jika Anda membuat jejak yang mencatat peristiwa di semuaWilayah AWS, itu akan muncul di konsol Wilayah AWS di semua AWSpartisi tempat Anda bekerja. Jika Anda membuat jejak yang hanya mencatat peristiwa dalam satuWilayah AWS, Anda dapat melihat dan mengelolanya hanya di dalamnyaWilayah AWS.
- Untuk mengedit jejak dalam daftar, pilih nama jejak.
- Konfigurasikan setidaknya satu jejak yang berlaku untuk semua Wilayah sehingga Anda menerima file log dari semua Wilayah di AWS partisi tempat Anda bekerja.
- Untuk mencatat peristiwa dari Wilayah tertentu dan mengirimkan file log ke bucket S3 di Wilayah yang sama, Anda dapat memperbarui jejak untuk diterapkan ke satu Wilayah. Ini berguna jika Anda ingin memisahkan file log Anda. Misalnya, Anda mungkin ingin pengguna mengelola log mereka sendiri di Wilayah tertentu, atau Anda mungkin ingin memisahkan alarm CloudWatch Log berdasarkan Wilayah.

- Untuk mencatat peristiwa dari beberapa AWS akun dalam satu jejak, pertimbangkan untuk membuat organisasi AWS Organizations dan kemudian membuat jejak organisasi.
- Membuat beberapa jalur akan dikenakan biaya tambahan. Untuk informasi lebih lanjut tentang harga, lihat AWS CloudTrailHarga.

Mengelola biaya CloudTrail jejak

Sebagai praktik terbaik, kami sarankan menggunakan AWS layanan dan alat yang dapat membantu Anda mengelola CloudTrail biaya. Anda juga 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.

Alat untuk membantu mengelola biaya

AWS Anggaran, fitur AWS Billing and Cost Management, memungkinkan Anda mengatur anggaran khusus yang mengingatkan Anda ketika biaya atau penggunaan Anda melebihi (atau diperkirakan melebihi) jumlah yang dianggarkan Anda.

Saat Anda membuat beberapa jalur, membuat anggaran untuk CloudTrail menggunakan AWS Anggaran adalah praktik terbaik yang direkomendasikan, dan dapat membantu Anda melacak pengeluaran Anda. CloudTrail Anggaran berbasis biaya 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.

Setelah Anda membuat anggaran, Anda dapat menggunakan AWS Cost Explorer untuk melihat bagaimana CloudTrail biaya Anda mempengaruhi keseluruhan AWS tagihan Anda. Di AWS Cost Explorer, setelah menambahkan CloudTrail ke filter Layanan, Anda dapat membandingkan CloudTrail pengeluaran historis Anda dengan pengeluaran Anda saat ini month-to-date (MTD), menurut Wilayah dan akun. Fitur ini membantu Anda memantau dan mendeteksi biaya tak terduga dalam CloudTrail pengeluaran bulanan Anda. Fitur tambahan di Cost Explorer memungkinkan Anda membandingkan CloudTrail pengeluaran dengan pengeluaran bulanan di tingkat sumber daya tertentu, memberikan informasi tentang apa yang mungkin mendorong kenaikan atau penurunan biaya tagihan 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 Billing and Cost Management, 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 Anggaran dan Praktik Terbaik untuk AWS Anggaran.

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

Pengiriman pertama dari setiap acara manajemen untuk akun gratis. 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 berdasarkan`resources.type`,`eventName`,`resources.ARN`, dan `readOnly` bidang, sehingga Anda dapat mencatat hanya peristiwa data yang menarik. Untuk informasi selengkapnya tentang mengonfigurasi bidang ini, lihat AdvancedFieldSelector. Untuk informasi selengkapnya tentang membuat dan memperbarui jejak, lihat Membuat jejak atau Memperbarui jejak 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

- AWS CloudTrail Penetapan Harga
- Mengelola biaya Anda dengan AWS Budgets
- Memulai dengan Cost Explorer
- Bersiaplah untuk membuat jejak untuk organisasi Anda

Persyaratan penamaan

Bagian ini memberikan informasi tentang persyaratan penamaan untuk CloudTrail sumber daya, bucket Amazon S3, dan kunci KMS.

Topik

- CloudTrail persyaratan penamaan sumber
- Persyaratan bucket Amazon S3
- AWS KMSpersyaratan penamaan alias

CloudTrail persyaratan penamaan sumber

CloudTrail nama sumber harus memenuhi persyaratan sebagai 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 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 bucket Amazon S3

bucket Amazon S3 yang Anda gunakan untuk menyimpan CloudTrail file 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, lihatPeraturan penamaan bucketdiPanduan Pengguna Amazon Simple Storage.

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 bucket harus dimulai dengan huruf atau angka kecil.
- 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 untuk digunakan sebagai URL yang dapat diakses secara 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, lihatPembatasan dan batasan bucketdiPanduan Pengguna Amazon Simple Storage.

AWS KMSpersyaratan penamaan alias

Saat Anda membuatAWS 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 sebagai berikut:

- Antara 1 dan 256 karakter, inklusif
- Berisi karakter alfanumerik (A-Z, a-z, 0-9), tanda hubung (-), garis miring (/), dan garis bawah (_)
- Tidak dapat dimulai denganaws

Untuk informasi selengkapnya tentang Membuat Kunci dalam AWS Key Management ServicePanduan Developer.

Mengontrol izin pengguna untuk CloudTrail jalan setapak

AWS CloudTrailIntegrasi denganAWS Identity and Access Management(IAM) untuk membantu Anda mengontrol akses CloudTrail dan lainnyaAWSsumber daya yang CloudTrail membutuhkan. Topik Amazon S3 Simple Notification Service (Amazon SNS). Anda dapat menggunakan IAM untuk mengontrolAWSpengguna dapat membuat, mengkonfigurasi, atau menghapus CloudTrail melacak, memulai dan menghentikan logging, dan mengakses bucket yang berisi informasi log. Untuk mempelajari selengkapnya, lihat Identity and Access Management untuk AWS CloudTrail.

Topik berikut membantu Anda memahami izin, kebijakan, dan CloudTrail keamanan:

- Pemberian izin untuk administrasi CloudTrail
- Aturan penamaan Amazon S3
- Kebijakan bucket Amazon S3 untuk CloudTrail

- Contoh kebijakan bucket untuk jejak organisasi diMembuat jejak untuk organisasi dengan AWS Command Line Interface.
- Kebijakan topik Amazon SNS untuk CloudTrail
- Mengenkripsi file CloudTrail log dengan AWS KMS kunci (SSE-KMS)
- Izin yang diperlukan untuk menyalin peristiwa jejak
- Izin yang diperlukan untuk menetapkan administrator yang didelegasikan
- Kebijakan kunci KMS default dibuat dalam CloudTrail konsol
- Memberikan izin untuk melihat AWS Config informasi di konsol CloudTrail
- Berbagi file CloudTrail log antar AWS akun
- Izin yang diperlukan untuk membuat jejak organisasi
- Menggunakan peran IAM yang sudah ada sebelumnya untuk menambahkan pemantauan jejak organisasi ke Amazon CloudWatch Log

Menggunakan AWS CloudTrail dengan VPC endpoint antarmuka

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host sumber daya AWS Anda, Anda dapat membuat koneksi privat antara VPC dan 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 dalam jaringan virtual yang Anda tetapkan. Dengan VPC, Anda memiliki kendali terhadap pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan pintu masuk jaringan. Dengan VPC endpoint, perutean antara VPC dan layanan AWS ditangani oleh jaringan AWS, dan Anda dapat menggunakan kebijakan IAM untuk mengendalikan akses ke sumber daya layanan.

Untuk menghubungkan VPC Anda CloudTrail, Anda menentukan titik akhir VPC antarmuka untuk. CloudTrail Antarmuka titik akhir adalah antarmuka jaringan elastis dengan alamat IP privat yang berfungsi sebagai titik masuk untuk lalu lintas ditujukan untuk layanan AWS yang didukung. 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 lebih lanjut, lihat AWS PrivateLink.

Langkah-langkah berikut ditujukan untuk para pengguna Amazon VPC. Untuk informasi selengkapnya, lihat Memulai Amazon VPC di Panduan Pengguna Amazon VPC.

Ketersediaan

CloudTrail saat ini mendukung titik akhir VPC di Wilayah berikut: AWS

- AS Timur (Ohio)
- AS Timur (Virginia Utara)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Tokyo)
- (Canada (Central)
- Kanada Barat (Calgary)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Eropa (Milan)
- Eropa (Paris)

- Eropa (Spanyol)
- Eropa (Stockholm)
- Eropa (Zürich)
- Israel (Tel Aviv)
- Timur Tengah (Bahrain)
- Timur Tengah (UEA)
- Amerika Selatan (Sao Paulo)
- AWS GovCloud (AS-Timur)
- AWS GovCloud (AS-Barat)

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.

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.

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 Perilaku ini juga berlaku untuk jejak organisasi yang dibuat oleh akun manajemen atau administrator yang didelegasikan, dan untuk

jejak organisasi multi-wilayah yang kemudian dibuat di akun anggota organisasi. 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.

Pengguna memiliki opsi untuk menghapus jejak sebelum menutupnya Akun AWS, atau menghubungi AWS Supportuntuk meminta penghapusan jejak setelah ditutup. Akun AWS

Untuk informasi selengkapnya tentang menutup Akun AWS, lihat Menutup Akun AWS.

> **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).

Bekerja dengan file CloudTrail log

Anda dapat melakukan tugas yang lebih maju dengan CloudTrail file Anda.

- Buat beberapa jalur per Wilayah.
- 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 Anda 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.
- Peristiwa manajemen: Acara manajemen memberikan visibilitas ke dalam operasi manajemen yang dilakukan pada sumber daya di AWS akun Anda. Ini juga dikenal sebagai operasi pesawat 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 ditangkap oleh CloudTrail.

> **Note**
>
> Tidak semua AWS layanan mendukung CloudTrail acara. Untuk informasi selengkapnya tentang layanan yang didukung, lihatCloudTrail layanan dan integrasi yang didukung. Untuk detail spesifik tentang API apa yang dicatat untuk layanan tertentu, lihat dokumentasi layanan tersebutCloudTrail layanan dan integrasi yang didukung.

- Peristiwa Insights: 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 dibuat hanya untuk API manajemen. Untuk informasi selengkapnya, lihat Acara Logging Insights.

> **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

- Mengelola konsistensi data dalam CloudTrail
- Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log
- Menerima file CloudTrail log dari beberapa akun
- Berbagi file CloudTrail log antar AWS akun
- Memvalidasi CloudTrail integritas berkas log
- Menggunakan CloudTrail Perpustakaan Pengolahan

Buat beberapa jalur

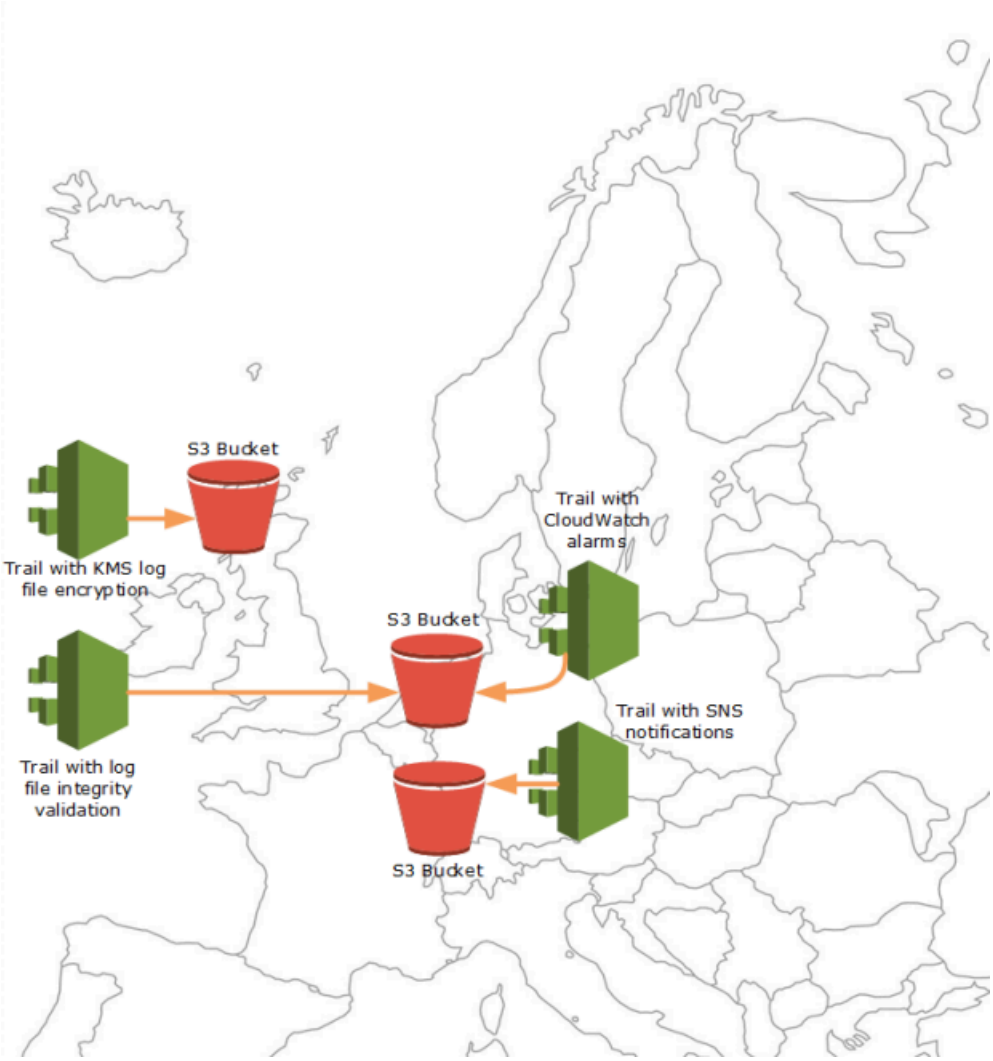
Anda dapat menggunakan CloudTrail log file untuk memecahkan masalah operasional atau keamanan diAWSakun. Anda dapat membuat jejak untuk pengguna yang berbeda, yang dapat membuat dan mengelola jalur mereka sendiri. Anda dapat mengonfigurasi jejak untuk mengirimkan file log ke bucket S3 terpisah atau bucket S3 bersama.

> **Note**
>
> Membuat beberapa jalur akan dikenakan biaya tambahan. Untuk informasi selengkapnya, lihat AWS CloudTrail Harga.

Misalnya, Anda mungkin memiliki pengguna berikut:

- Administrator keamanan akan membuat Wilayah Eropa (Irlandia) dan mengkonfigurasi enkripsi file log KMS. Jejak mengirimkan file log ke ember S3 di Wilayah Eropa (Irlandia) Wilayah Eropa (Irlandia) Wilayah Eropa (Irlandia).
- Auditor TI membuat jejak di Wilayah Eropa (Irlandia) dan mengonfigurasi validasi integritas file log untuk memastikan file log tidak berubah sejak saat itu CloudTrail mengantarkan mereka. Jejak ini dikonfigurasi untuk mengirimkan file log ke ember S3 di Wilayah Eropa (Frankfurt) Wilayah Eropa (Frankfurt)
- Pengembang membuat jejak di Wilayah Eropa (Frankfurt) dan mengkonfigurasi 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 Wilayah Eropa (Prancis) akan dikirim ke Wilayah Eropa (Eropa).

Gambar berikut mengilustrasikan contoh ini.



> **Note**
>
> Anda dapat membuat hingga lima jalur perWilayah AWSJejak yang mencatat aktivitas dari semua Wilayah dihitung sebagai satu jejak 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, lihatContoh: Membuat dan menerapkan kebijakan untuk tindakan pada jalur tertentu.

Untuk informasi selengkapnya tentang beberapa jalur, lihat sumber daya berikut:

- Bagaimana CloudTrail berperilaku regional dan global?
- CloudTrail pertanyaan umum

Acara manajemen logging

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 Harga AWS CloudTrail.

Daftar Isi

Acara manajemen

Acara manajemen memberikan visibilitas ke dalam 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 `AttachRolePolicy` API IAM)

- 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, ketika pengguna masuk ke akun Anda, CloudTrail mencatat `ConsoleLogin` peristiwa tersebut. Untuk informasi selengkapnya, lihat Peristiwa non-API 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.

Pencatatan acara manajemen dengan AWS Management Console

1. Masuk ke AWS Management Console dan buka CloudTrail konsol di https://console.aws.amazon.com/cloudtrail/.
2. Untuk memperbarui jejak, buka halaman Trails CloudTrail konsol dan pilih nama jejak.

   Untuk memperbarui penyimpanan data acara, buka halaman penyimpanan data acara CloudTrail konsol dan pilih nama penyimpanan data acara.
3. Untuk acara Manajemen, pilih Edit.
   - Pilih apakah Anda ingin penyimpanan data jejak atau acara mencatat peristiwa Baca, Menulis peristiwa, atau keduanya.
   - Pilih Kecualikan AWS KMS acara untuk memfilter AWS Key Management Service (AWS KMS) peristiwa dari jejak atau penyimpanan data acara 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 penyimpanan data jejak atau acara 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 KMStindakan sepertiEncrypt,Decrypt, dan GenerateDataKey biasanya menghasilkan volume besar (lebih dari 99%) peristiwa. Tindakan ini sekarang dicatat sebagai peristiwa Baca. Volume rendah, AWS KMS tindakan yang relevan sepertiDisable,Delete, dan ScheduleKey (yang biasanya menyumbang kurang dari 0,5% dari volume AWS KMS peristiwa) dicatat sebagai peristiwa Tulis.

Untuk mengecualikan peristiwa bervolume tinggi sepertiEncrypt,Decrypt, danGenerateDataKey, tetapi masih mencatat peristiwa yang relevan sepertiDisable, Delete danScheduleKey, 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 API dari jejak atau penyimpanan data peristiwa 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.

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

  Peristiwa hanya-baca mencakup operasi API yang membaca sumber daya Anda, tetapi tidak membuat perubahan. Misalnya, peristiwa hanya-baca mencakup operasi Amazon DescribeSecurityGroups EC2 DescribeSubnets dan API. Operasi ini hanya menampilkan informasi tentang sumber daya Amazon EC2 Anda dan tidak mengubah konfigurasi Anda.

- Menulis

Peristiwa khusus tulis mencakup operasi API yang mengubah (atau mungkin memodifikasi) sumber daya Anda. Misalnya, operasi Amazon EC2 `RunInstances` dan `TerminateInstances` API 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 `read-only-bucket` 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 `write-only-bucket` 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 ke. `read-only-bucket`
5. Operasi `TerminateInstances` API adalah acara khusus tulis dan cocok dengan pengaturan untuk jejak kedua. Jejak mencatat dan mengirimkan acara ke. `write-only-bucket`

Mencatat peristiwa dengan AWS Command Line Interface

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:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/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:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/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 dalam 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

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"
}
```

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"
}
```

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"
}
```

Mencatat peristiwa 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 Mengelola CloudTrail Danau dengan menggunakan AWS CLI dan Referensi AWS CloudTrail API.

Mengirim acara ke Amazon CloudWatch Logs

Untuk jejak, CloudTrail mendukung pengiriman data dan peristiwa manajemen ke CloudWatch Log. Saat Anda mengonfigurasi jejak untuk mengirim peristiwa ke grup CloudWatch log Log, hanya CloudTrail mengirimkan peristiwa yang Anda tentukan di jejak Anda. Misalnya, jika Anda mengonfigurasi jejak Anda hanya untuk mencatat peristiwa manajemen, jejak Anda hanya akan mengirimkan peristiwa manajemen ke grup CloudWatch log Log Anda. Lihat informasi yang lebih lengkap di Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Pencatatan peristiwa data

Secara default, jejak dan penyimpanan data peristiwa tidak mencatat peristiwa data. Biaya tambahan berlaku untuk peristiwa data. Untuk informasi selengkapnya, silakan lihat Harga AWS CloudTrail.

> **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 Acara dari AWS layanan di Panduan EventBridge Pengguna Amazon.

Daftar Isi

        - Catat semua peristiwa Amazon S3 untuk bucket Amazon S3 dengan menggunakan pemilih acara lanjutan
        - Log Amazon S3 pada AWS Outposts peristiwa dengan menggunakan pemilih 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 ember
        - Sertakan Amazon S3 pada acara AWS Outposts
- Mencatat peristiwa data untuk AWS Config kepatuhan
- Mencatat peristiwa data dengan AWS SDK
- Mengirim acara ke Amazon CloudWatch Logs

Peristiwa data

Peristiwa data memberikan visibilitas ke dalam operasi sumber daya yang dilakukan pada atau di dalam sumber daya. Ini juga dikenal sebagai operasi bidang data. Peristiwa data seringkali merupakan aktivitas volume tinggi.

Contoh peristiwa data meliputi:

- Aktivitas API tingkat objek Amazon S3 (misalnya, `GetObject`, `DeleteObject`, dan operasi `PutObject` API) pada bucket dan objek dalam bucket.
- 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 peristiwa data yang tersedia untuk jejak dan penyimpanan data peristiwa. Kolom tipe peristiwa data (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 bucket Amazon S3 dan objek bucket, fungsi Lambda, dan tabel DynamoDB (ditampilkan

dalam tiga baris pertama tabel). Anda hanya dapat menggunakan pemilih acara lanjutan untuk mencatat jenis peristiwa data yang ditampilkan di baris yang tersisa.

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

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon DynamoDB	Aktivitas API tingkat objek Amazon DynamoDB pada tabel (misalnya `PutItem`,,`DeleteItem` , dan operasi API). `UpdateItem` **Note** Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table` . Jika Anda menentukan `AWS::Dyna`	DynamoDB	`AWS::DynamoDB::Table`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	moDB::Table untukresources.type , itu akan mencatat kedua tabel DynamoDB dan DynamoDB stream peristiwa secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di eventName bidang.		
AWS Lambda	AWS Lambda aktivitas eksekusi fungsi (InvokeAPI).	Lambda	AWS::Lambda::Function

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon S3	Aktivitas API tingkat objek Amazon S3 (misalnya , `GetObject` `DeleteObject` , dan operasi `PutObject` API) pada bucket dan objek dalam bucket.	S3	`AWS::S3::Object`
AWS AppConfig	AWS AppConfig Aktivitas API untuk operasi konfigurasi seperti panggilan ke `StartConfiguration` `Session` dan`GetLatestConfiguration` .	AWS AppConfig	`AWS::AppConfig::Configuration`
AWS Pertukaran Data B2B	Aktivitas B2B Data Interchange API untuk operasi Transformer seperti panggilan ke dan. `GetTransformerJob` `StartTransformerJob`	Pertukaran Data B2B	`AWS::B2BI::Transformer`
Amazon Bedrock	Aktivitas Amazon Bedrock API pada alias agen.	Alias agen batuan dasar	`AWS::Bedrock::AgentAlias`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Aktivitas Amazon Bedrock API pada basis pengetahuan.	Basis pengetahuan batuan dasar	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront Aktivitas API pada a KeyValueStore.	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	AWS Cloud Map Aktivitas API pada namespace.	AWS Cloud Map namespace	`AWS::ServiceDiscovery::Namespace`
	AWS Cloud Map Aktivitas API pada layanan.	AWS Cloud Map layanan	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` aktivitas di saluran CloudTrail Danau yang digunakan untuk mencatat peristiwa dari luar AWS.	CloudTrail	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	Aktivitas Amazon CodeWhisperer API pada kustomisasi.	CodeWhisperer kustomisasi	`AWS::CodeWhisperer::Customization`
	Aktivitas Amazon CodeWhisperer API di profil.	CodeWhisperer	`AWS::CodeWhisperer::Profile`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon Cognito	Aktivitas API Amazon Cognito di kumpulan identitas Amazon Cognito.	Kolam Identitas Cognito	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	Aktivitas Amazon DynamoDB API di stream.	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	API langsung Amazon Elastic Block Store (EBS), seperti,`PutSnapshotBlock` , `GetSnapshotBlock` dan pada snapshot `ListChangedBlocks` Amazon EBS.	API langsung Amazon EBS	`AWS::EC2::Snapshot`
Amazon EMR	Aktivitas Amazon EMR API di ruang kerja log tulis di depan.	Ruang kerja log tulis ke depan EMR	`AWS::EMRWAL::Workspace`
Amazon FinSpace	Amazon FinSpaceAktivitas API di lingkungan.	FinSpace	`AWS::FinSpace::Environment`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS Glue	AWS Glue Aktivitas API pada tabel yang dibuat oleh Lake Formation. **Note** AWS Glue peristiwa data untuk tabel saat ini hanya didukung di wilayah berikut: • AS Timur (N. Virginia) • AS Timur (Ohio) • AS Barat (Oregon) • Eropa (Irlandia) • Wilayah Asia Pasifik (Tokyo)	Formasi Danau	`AWS::Glue::Table`
Amazon GuardDuty	Aktivitas Amazon GuardDuty API untuk detektor.	GuardDuty detektor	`AWS::GuardDuty::Detector`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS HealthImaging	AWS HealthImaging Aktivitas API pada penyimpanan data.	Toko data Pencitraan Medis	`AWS::MedicalImaging::Datastore`
AWS IoT	AWS IoT Aktivitas API pada sertifikat.	Sertifikat IoT	`AWS::IoT::Certificate`
	AWS IoT Aktivitas API pada berbagai hal.	Hal IoT	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	Aktivitas API Greengrass dari perangkat inti Greengrass pada versi komponen. **Note** Greengrass tidak mencatat peristiwa yang ditolak akses.	Versi komponen Greengrass IoT	`AWS::GreengrassV2::ComponentVersion`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Greengrass aktivitas API dari perangkat inti Greengrass pada penerapan. **Note** Greengrass tidak mencatat peristiwa yang ditolak akses.	Penyebaran Greengrass IoT	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	Aktivitas SiteWise API IoT pada aset.	Aset IoT SiteWise	`AWS::IoTSiteWise::Asset`
	Aktivitas SiteWise API IoT pada deret waktu.	Deret waktu IoT SiteWise	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	Aktivitas TwinMaker API IoT pada entitas.	Entitas IoT TwinMaker	`AWS::IoTTwinMaker::Entity`
	Aktivitas TwinMaker API IoT di ruang kerja.	Ruang kerja IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`
Peringkat Cerdas Amazon Kendra	Aktivitas API Peringkat Cerdas Amazon Kendra pada rencana eksekusi skor ulang.	Peringkat Kendra	`AWS::KendraRanking::ExecutionPlan`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Amazon Keyspaces (untuk Apache Cassandra)	Aktivitas API Amazon Keyspaces di atas meja.	Meja Cassandra	`AWS::Cassandra::Table`
Amazon Kinesis	Aktivitas API Amazon Kinesis pada aliran video, seperti panggilan ke dan. `GetMedia` `PutMedia`	Aliran video Kinesis	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	Aktivitas API Amazon Managed Blockchain di jaringan.	Jaringan Blockchain yang dikelola	`AWS::ManagedBlockchain::Network`
	Amazon Managed Blockchain JSON-RPC memanggil node Ethereum, seperti atau. `eth_getBalance` `eth_getBlockByNumber`	Blockchain yang Dikelola	`AWS::ManagedBlockchain::Node`
Grafik Amazon Neptunus	Aktivitas API data, misalnya kueri, algoritme , atau pencarian vektor, pada Grafik Neptunus.	Grafik Neptunus	`AWS::NeptuneGraph::Graph`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
AWS Private CA	AWS Private CA Konektor untuk aktivitas Active Directory API.	AWS Private CA Konektor untuk Active Directory	`AWS::PCAConnectorAD::Connector`
Amazon Q Bisnis	Aktivitas Amazon Q Business API pada aplikasi.	Aplikasi Amazon Q Business	`AWS::QBusiness::Application`
	Aktivitas Amazon Q Business API pada sumber data.	Sumber data Amazon Q Business	`AWS::QBusiness::DataSource`
	Aktivitas API Amazon Q Business pada indeks.	Amazon Q Indeks Bisnis	`AWS::QBusiness::Index`
	Aktivitas Amazon Q Business API pada pengalaman web.	Pengalaman web Amazon Q Bisnis	`AWS::QBusiness::WebExperience`
Amazon RDS	Aktivitas Amazon RDS API di Cluster DB.	API Data RDS - Kluster DB	`AWS::RDS::DBCluster`
Amazon S3	Aktivitas API Amazon S3 pada titik akses.	Titik Akses S3	`AWS::S3::AccessPoint`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Aktivitas API titik akses Objek Lambda Amazon S3, seperti panggilan ke dan. `CompleteMultipartUpload` `GetObject`	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 pada aktivitas API tingkat objek Outposts.	Outposts S3	`AWS::S3Outposts::Object`
Amazon SageMaker	SageMaker `InvokeEndpointWithResponseStream` Aktivitas Amazon di titik akhir.	SageMaker titik akhir	`AWS::SageMaker::Endpoint`
	Aktivitas SageMaker API Amazon di toko fitur.	SageMaker feature store	`AWS::SageMaker::FeatureGroup`
	Aktivitas Amazon SageMaker API pada komponen percobaan percobaan.	SageMaker komponen percobaan percobaan metrik	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	Operasi `Publish`API Amazon SNS pada titik akhir platform.	Titik akhir platform SNS	`AWS::SNS::PlatformEndpoint`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
	Operasi Amazon SNS `Publish`dan `PublishBatch` API pada topik.	Topik SNS	`AWS::SNS::Topic`
Amazon SQS	Aktivitas Amazon SQS API pada pesan.	SQS	`AWS::SQS::Queue`
Rantai Pasokan AWS	Rantai Pasokan AWS Aktivitas API pada sebuah instance.	Rantai Pasokan	`AWS::SCN::Instance`
Amazon SWF	Aktivitas API Amazon SWF di domain.	Domain SWF	`AWS::SWF::Domain`
AWS Systems Manager	Aktivitas API Systems Manager pada saluran kontrol.	Systems Manager	`AWS::SSMMessages::ControlChannel`
	Aktivitas API Systems Manager pada node terkelola.	Node terkelola Systems Manager	`AWS::SSM::ManagedNode`
Amazon Timestream	Aktivitas `Query`API Amazon Timestream pada database.	Database Timestream	`AWS::Timestream::Database`
	Aktivitas `Query`API Amazon Timestream pada tabel.	Tabel Timestream	`AWS::Timestream::Table`

AWS layanan	Deskripsi	Jenis peristiwa data (konsol)	nilai resources.type
Izin Terverifikasi Amazon	Aktivitas API Izin Terverifikasi Amazon di toko kebijakan.	Izin Terverifikasi Amazon	`AWS::VerifiedPermissions::PolicyStore`
Klien WorkSpaces Tipis Amazon	WorkSpaces Aktivitas API Klien Tipis di Perangkat.	Perangkat Klien Tipis	`AWS::ThinClient::Device`
	WorkSpaces Aktivitas API Klien Tipis di Lingkungan.	Lingkungan Klien Tipis	`AWS::ThinClient::Environment`
AWS X-Ray	Aktivitas X-Ray API pada jejak.	Jejak X-Ray	`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. Lihat informasi yang lebih lengkap di Membuat jejak dan Buat penyimpanan data acara untuk CloudTrail acara.

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.

Mencatat peristiwa data dengan AWS Management Console

Prosedur berikut menjelaskan cara memperbarui penyimpanan data peristiwa yang ada atau jejak untuk mencatat peristiwa data dengan menggunakan AWS Management Console. Untuk informasi tentang cara membuat penyimpanan data peristiwa untuk mencatat peristiwa data,

lihatBuat penyimpanan data acara untuk CloudTrail acara. Untuk informasi tentang cara membuat jejak untuk mencatat peristiwa data, lihatMembuat jejak di konsol.

Untuk jejak, langkah-langkah untuk mencatat peristiwa data berbeda berdasarkan apakah Anda menggunakan pemilih acara lanjutan atau pemilih acara dasar. Anda dapat mencatat peristiwa data untuk semua tipe peristiwa data menggunakan pemilih peristiwa lanjutan, tetapi Anda hanya dapat mencatat peristiwa data untuk bucket Amazon S3 dan objek bucket AWS Lambda , fungsi, dan tabel Amazon DynamoDB menggunakan pemilih peristiwa dasar.

Memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa data di AWS Management Console

Gunakan prosedur berikut untuk memperbarui penyimpanan data peristiwa yang ada untuk mencatat peristiwa data.

1. Masuk ke AWS Management Console 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 peristiwa Data, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data.
7. Pilih templat pemilih log. CloudTrail termasuk template standar yang mencatat semua peristiwa data untuk jenis sumber daya. Untuk membuat template pemilih log kustom, pilih Kustom.

   > **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 penyimpanan data acara. 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 penyimpanan data peristiwa 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 penyimpanan data peristiwa 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 penyimpanan data peristiwa 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 penyimpanan data acara. Jika Anda membuat penyimpanan data peristiwa untuk satu Wilayah, 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 penyimpanan data jejak atau peristiwa. 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.

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. Di Advanced event selectors, buat ekspresi untuk sumber daya spesifik tempat Anda ingin mencatat peristiwa data. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

    a. Pilih dari bidang berikut.

    - **`readOnly`**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Peristiwa data hanya-baca 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.
- **resources.ARN**- Anda dapat menggunakan operator apa pun denganresources.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

  Tabel berikut menunjukkan format ARN yang valid untuk masing-masing. resources.type

  > **Note**
  >
  > Anda tidak dapat menggunakan resources.ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

resources.type	Sumber Daya.arn
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /

resources.type	Sumber Daya.arn
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	Sumber Daya.arn
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	Sumber Daya.arn
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*

resources.type	Sumber Daya.arn
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*

resources.type	Sumber Daya.arn
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*

resources.type	Sumber Daya.arn
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	Sumber Daya.arn
AWS::SSM::ManagedNode	ARN harus berada dalam salah satu format berikut: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	Sumber Daya.arn
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table`. Jika Anda menentukan `AWS::DynamoDB::Table` untuk`resources.type`, itu akan mencatat kedua tabel DynamoDB dan DynamoDB stream peristiwa secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.

[2] Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok. Garis miring disengaja; jangan mengecualikannya.

[3] Untuk mencatat peristiwa pada semua objek di titik akses S3, kami sarankan Anda hanya menggunakan titik akses ARN, jangan sertakan jalur objek, dan gunakan `StartsWith` operator atau. `NotStartsWith`

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Tindakan, sumber daya, dan kunci kondisi di AWS Identity and Access Management Panduan Pengguna.

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, menyetel operator untuk tidak memulai, lalu menempelkan ARN bucket S3, atau menelusuri 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.

> **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.
> 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 penyimpanan data acara. Anda masih dapat mencatat semua fungsi dengan template pemilih yang telah ditentukan, 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 penyimpanan data peristiwa di konsol, dan kemudian menggunakan AWS CLI untuk mengonfigurasi pencatatan peristiwa data untuk fungsi Lambda tertentu. Untuk informasi selengkapnya, lihat Mencatat peristiwa data dengan AWS Command Line Interface.

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.

10. Untuk menambahkan tipe data lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 6 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk tipe peristiwa data.
11. Setelah meninjau dan memverifikasi pilihan, pilih Simpan perubahan.

Memperbarui jejak yang ada untuk mencatat peristiwa data dengan pemilih acara lanjutan di AWS Management Console

Dalam AWS Management Console, 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 dan tips tentang menggunakan penyeleksi acara tingkat lanjut, lihat Log peristiwa 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 peristiwa Data, pilih jenis sumber daya tempat Anda ingin mencatat peristiwa data.
5. Pilih templat pemilih log. CloudTrail termasuk template standar yang mencatat semua peristiwa data untuk jenis sumber daya. Untuk membuat template pemilih log kustom, pilih Kustom.

> **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. Di Advanced event selectors, buat ekspresi untuk sumber daya spesifik tempat Anda ingin mencatat peristiwa data. Anda dapat melewati langkah ini jika Anda menggunakan template log yang telah ditentukan.

   a. Pilih dari bidang berikut.

   - **readOnly**- `readOnly` dapat diatur untuk sama dengan nilai `true` atau`false`. Peristiwa data hanya-baca 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.
   - **resources.ARN**- Anda dapat menggunakan operator apa pun denganresources.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`

     Tabel berikut menunjukkan format ARN yang valid untuk masing-masing. `resources.type`

     > **Note**
     >
     > Anda tidak dapat menggunakan `resources.`ARN bidang untuk memfilter jenis sumber daya yang tidak memiliki ARN.

resources.type	Sumber Daya.arn
`AWS::DynamoDB::Table` [1]	`arn:`*`partition`*` :dynamodb : `*`region`*`:`*`account_ID`*` :table/`*`table_name`*

resources.type	Sumber Daya.arn
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*

resources.type	Sumber Daya.arn
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace: *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*

resources.type	Sumber Daya.arn
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*

resources.type	Sumber Daya.arn
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	Sumber Daya.arn
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	Sumber Daya.arn
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	Sumber Daya.arn
AWS::SSM::ManagedNode	ARN harus berada dalam salah satu format berikut: • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	Sumber Daya.arn
`AWS::VerifiedPermissions::PolicyStore`	`arn:partition :verifiedpermissions: region:account_ID :policy-store/ policy_store_ID`

[1] Untuk tabel dengan aliran diaktifkan, `resources` bidang dalam peristiwa data berisi keduanya `AWS::DynamoDB::Stream` dan`AWS::DynamoDB::Table`. Jika Anda menentukan `AWS::DynamoDB::Table` untuk`resources.type`, itu akan mencatat kedua tabel DynamoDB dan DynamoDB stream peristiwa secara default. Untuk mengecualikan peristiwa aliran, tambahkan filter di `eventName` bidang.

[2] Untuk mencatat semua peristiwa data untuk semua objek dalam bucket S3 tertentu, gunakan `StartsWith` operator, dan sertakan hanya ARN bucket sebagai nilai yang cocok. Garis miring disengaja; jangan mengecualikannya.

[3] Untuk mencatat peristiwa pada semua objek di titik akses S3, kami sarankan Anda hanya menggunakan titik akses ARN, jangan sertakan jalur objek, dan gunakan `StartsWith` operator atau. `NotStartsWith`

Untuk informasi selengkapnya tentang format ARN sumber daya peristiwa data, lihat Tindakan, sumber daya, dan kunci kondisi di AWS Identity and Access Management Panduan Pengguna.

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 jejak Anda, Anda dapat mengatur bidang ke Resources.arn, menyetel operator untuk tidak memulai, lalu menempelkan di ARN bucket S3, atau menelusuri 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.

> **Note**
>
> Anda dapat memiliki maksimum 500 nilai untuk semua penyeleksi di jalan setapak. 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.
> 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 mencatat semua fungsi dengan template pemilih yang telah ditentukan, 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, dan kemudian menggunakan AWS CLI untuk mengonfigurasi pencatatan peristiwa data untuk fungsi Lambda tertentu. Untuk informasi selengkapnya, lihat Mencatat peristiwa data dengan AWS Command Line Interface.

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.

8. Untuk menambahkan tipe data lain untuk mencatat peristiwa data, pilih Tambahkan tipe peristiwa data. Ulangi langkah 4 melalui langkah ini untuk mengonfigurasi pemilih acara lanjutan untuk tipe peristiwa data.
9. Setelah meninjau dan memverifikasi pilihan, pilih Simpan perubahan.

Perbarui jejak yang ada untuk mencatat peristiwa data dengan pemilih acara dasar di AWS Management Console

Gunakan prosedur berikut untuk memperbarui jejak yang ada untuk mencatat peristiwa data menggunakan pemilih acara dasar.

1. Masuk ke AWS Management Console 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, 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.

5. Untuk menambahkan tipe data 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, dan kemudian menggunakan put-event-selectors perintah AWS CLI dan untuk mengonfigurasi pencatatan peristiwa data untuk fungsi Lambda tertentu. Untuk informasi selengkapnya, lihat Mengelola jalur dengan AWS CLI.

7. Untuk menambahkan tipe data 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.

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 pencatatan semua peristiwa data untuk bucket S3 bernama bucket-1. Dalam contoh ini, CloudTrail pengguna menentukan awalan kosong, dan opsi untuk mencatat peristiwa data Baca dan Tulis.

1. Seorang pengguna mengunggah objek kebucket-1.
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 kebucket-2.
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 bernama ***bucket-3, 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:::bucket-3/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:::bucket-3/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:::bucket-3/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 informasi selengkapnya, lihat Bagaimana cara CloudTrail kerja.
> Untuk menghindari peristiwa data pencatatan untuk bucket Amazon S3 tempat Anda menerima file log jika mengonfigurasi jejak untuk mencatat semua peristiwa data Amazon S3 di akun AWS Anda, pertimbangkan untuk mengonfigurasi 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 akun lain AWS

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 akun AWS

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`owner-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 akun AWS

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 tersebut. 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.

Acara hanya-baca dan hanya 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 Amazon `DescribeSecurityGroups` EC2 `DescribeSubnets` dan API. 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 Amazon EC2 `RunInstances` dan `TerminateInstances` API 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 `read-only-bucket` 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 bernama `write-only-bucket` 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. `read-only-bucket`
5. Operasi `TerminateInstances` API adalah acara khusus tulis dan cocok dengan pengaturan untuk jejak kedua. Jejak mencatat dan mengirimkan acara ke. `write-only-bucket`

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 Untuk melihat apakah jejak Anda mencatat manajemen dan peristiwa data, jalankan `get-event-selectors`perintah.

> **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 acara lanjutan untuk memfilter berdasarkan nilai`eventName`,`resources.`ARN, dan `readOnly` bidang, sehingga Anda dapat mencatat hanya peristiwa data yang menarik. Untuk informasi selengkapnya tentang mengonfigurasi bidang ini, lihat AdvancedFieldSelector.

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

Perintah mengembalikan pengaturan default untuk jejak.

Topik

Log peristiwa 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 kombinasi bucket/awalan Amazon S3 kecuali untuk bucket bernama dan peristiwa data untuk fungsi bernama. `sample_bucket_name` 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:::sample_bucket_name/"] }
    ]
  },
  {
    "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:::sample_bucket_name/" ]
        },
      ]
    },
{
      "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:::bucket_name/"] }
            ]
        }
]'
```

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:::bucket_name/"
                    ]
                }
```

```
            ]
        }
    ]
}
```

Log Amazon S3 pada AWS Outposts peristiwa dengan menggunakan pemilih 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:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/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:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/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.

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 ember
- Sertakan Amazon S3 pada acara AWS Outposts

Sertakan semua acara Amazon S3 untuk ember

Contoh berikut menunjukkan cara membuat penyimpanan data peristiwa 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 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:::bucket_name/"] }
            ]
        }
]'
```

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:::bucket_name/"
                    ]
                },
                {
```

```
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

Sertakan Amazon S3 pada acara AWS Outposts

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"
}
```

Mencatat peristiwa data 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 Kerangka AWS Well-Architected Framework
- 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 Logging

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 Mengelola CloudTrail Danau dengan menggunakan AWS CLI dan Referensi AWS CloudTrail API.

Mengirim acara ke Amazon CloudWatch Logs

CloudTrail mendukung pengiriman peristiwa data ke CloudWatch Log. Saat Anda mengonfigurasi jejak untuk mengirim peristiwa ke grup CloudWatch log Log, hanya CloudTrail mengirimkan peristiwa yang Anda tentukan di jejak Anda. Misalnya, jika Anda mengonfigurasi jejak Anda untuk mencatat peristiwa data saja, jejak Anda hanya akan mengirimkan peristiwa data ke grup CloudWatch log Log Anda. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Acara Logging Insights

AWS CloudTrail Wawasan membantu AWS pengguna mengidentifikasi dan merespons aktivitas tidak biasa yang terkait dengan 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 volume

panggilan API dibuat untuk API `write` manajemen, dan peristiwa Insights tentang tingkat kesalahan API dibuat untuk keduanya `read` dan API `write` manajemen.

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

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.

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 Harga AWS CloudTrail.

Daftar Isi

    - Tab catatan acara wawasan
- Mengirim acara jejak ke Amazon CloudWatch Logs

Memahami penyampaian acara Wawasan

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 biasa akun.

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

Wawasan pengiriman acara untuk jalur

Jika Anda telah mengaktifkan peristiwa Insights di jejak dan CloudTrail mendeteksi aktivitas yang tidak biasa, kirimkan peristiwa CloudTrail Insights ke `/CloudTrail-Insight` folder di bucket S3 tujuan yang dipilih untuk jejak Anda. Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di jalur, diperlukan waktu hingga 36 jam CloudTrail untuk menyampaikan acara Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

Jika Anda menonaktifkan log peristiwa Insights di jejak lalu mengaktifkan kembali peristiwa Insights, atau menghentikan dan memulai ulang logging di jejak, diperlukan waktu hingga 36 jam CloudTrail untuk memulai ulang pengiriman peristiwa Wawasan, jika aktivitas yang tidak biasa terdeteksi.

Wawasan pengiriman acara untuk penyimpanan data acara

Jika Anda telah mengaktifkan peristiwa Insights di penyimpanan data peristiwa sumber, kirimkan peristiwa CloudTrail Insights ke penyimpanan data acara tujuan. Setelah Anda mengaktifkan CloudTrail Insights untuk pertama kalinya di penyimpanan data peristiwa sumber, diperlukan waktu hingga 7 hari CloudTrail untuk mengirimkan acara Insights pertama ke penyimpanan data acara tujuan, jika aktivitas yang tidak biasa terdeteksi.

Jika Anda menonaktifkan log peristiwa Insights di penyimpanan data peristiwa sumber dan kemudian mengaktifkan kembali peristiwa Insights, atau menghentikan dan memulai ulang konsumsi peristiwa di penyimpanan data peristiwa sumber, diperlukan waktu hingga 7 hari CloudTrail untuk memulai ulang pengiriman peristiwa Wawasan, jika aktivitas yang tidak biasa terdeteksi. 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 CloudTrailHarga.

Acara Logging Insights dengan AWS Management Console

Anda dapat mengaktifkan peristiwa Insights di penyimpanan data jejak atau peristiwa menggunakan konsol.

Topik

Mengaktifkan acara CloudTrail Insights di jalur yang ada

Gunakan prosedur berikut untuk mengaktifkan peristiwa CloudTrail Insights pada jejak yang ada. Secara default, peristiwa Insights tidak diaktifkan.

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

> **Note**
>
> Biaya tambahan berlaku untuk acara logging Insights. Untuk CloudTrail harga, lihat AWS CloudTrailHarga.

3. Di Jenis acara, pilih Acara Wawasan.
4. Dalam peristiwa Insights, di bagian Pilih jenis Wawasan, pilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Jejak Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Insights untuk rasio panggilan API. Jejak Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.
5. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Diperlukan waktu hingga 36 jam CloudTrail untuk menyampaikan peristiwa Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

Mengaktifkan peristiwa CloudTrail Wawasan pada penyimpanan data acara yang ada

Gunakan prosedur berikut untuk mengaktifkan peristiwa CloudTrail Insights pada penyimpanan data peristiwa yang ada. Secara default, peristiwa Insights tidak diaktifkan.

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 CloudTrailHarga.

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

1. Di panel navigasi kiri CloudTrail konsol, di bawah Danau, pilih Penyimpanan data acara.
2. Pilih nama penyimpanan data acara.
3. Di acara Manajemen, pilih Edit.
4. Pilih Aktifkan Wawasan.
5. Pilih penyimpanan data acara tujuan tempat CloudTrail akan mengirimkan 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 acara tujuan yang mencatat peristiwa Wawasan.
6. Di bagian Pilih jenis Wawasan, pilih tingkat panggilan API, tingkat kesalahan API, atau keduanya. Penyimpanan data peristiwa Anda harus mencatat peristiwa manajemen Tulis untuk mencatat peristiwa Wawasan untuk tingkat panggilan API. Penyimpanan data peristiwa Anda harus mencatat peristiwa manajemen Baca atau Tulis untuk mencatat peristiwa Wawasan untuk tingkat kesalahan API.
7. Pilih Simpan perubahan untuk menyimpan perubahan Anda.

Diperlukan waktu hingga 7 hari CloudTrail untuk menyampaikan peristiwa Wawasan pertama, jika aktivitas yang tidak biasa terdeteksi.

Acara Logging Insights dengan AWS Command Line Interface

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

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

Topik

Peristiwa Logging Insights untuk jejak menggunakan AWS CLI

Untuk melihat apakah jejak Anda mencatat peristiwa Insights, jalankan `get-insight-selectors` perintah.

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

Hasil berikut menunjukkan pengaturan default untuk jejak. Secara default, jejak tidak mencatat peristiwa Wawasan. Nilai `InsightType` atribut kosong, dan tidak ada pemilih acara Insight yang ditentukan, karena koleksi acara Insights tidak diaktifkan.

Jika Anda tidak menambahkan pemilih Insights, get-insight-selectors perintah akan menampilkan pesan galat berikut: “Terjadi kesalahan (InsightNotEnabledException) saat memanggil GetInsightSelectors operasi: *Nama* jejak tidak memiliki Wawasan diaktifkan. Edit pengaturan jejak untuk mengaktifkan Wawasan, lalu coba operasi lagi.”

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

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.

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

Hasil berikut menunjukkan pemilih peristiwa Insights yang dikonfigurasi untuk jejak.

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

Peristiwa Logging Insights 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 Wawasan.

Untuk melihat apakah peristiwa Insights diaktifkan di 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 Wawasan 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
```

Prosedur berikut menunjukkan 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.

   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 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. 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": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

Anda akan menggunakan ARN (atau akhiran ID ARN) dari respons sebagai nilai untuk 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, diperlukan waktu hingga 7 hari CloudTrail untuk menyampaikan acara Insights pertama, jika aktivitas yang tidak biasa terdeteksi.

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 CloudTrailHarga.

Mencatat peristiwa dengan AWS SDK

Jalankan GetInsightSelectorsoperasi untuk melihat apakah penyimpanan data jejak atau acara Anda mengaktifkan peristiwa Insights. Anda dapat mengonfigurasi jejak atau penyimpanan data peristiwa untuk mengaktifkan peristiwa Wawasan dengan operasi. PutInsightSelectors Untuk informasi lebih lanjut, lihat Referensi API AWS CloudTrail.

Informasi tambahan untuk jalan setapak

Bagian ini memberikan informasi tambahan yang khusus untuk jalur. Bagian ini menjelaskan cara Anda dapat melihat peristiwa untuk jejak langganan Anda dari halaman Wawasan di CloudTrail konsol dan cara mengirim peristiwa ini secara opsional ke Log untuk CloudWatch dipantau.

Topik

- Melihat peristiwa Wawasan untuk jejak di konsol
- Mengirim acara jejak ke Amazon CloudWatch Logs

Melihat peristiwa Wawasan untuk jejak di konsol

Untuk jalur, Anda juga dapat mengakses dan melihat peristiwa Wawasan di halaman Wawasan di konsol. CloudTrail Untuk informasi selengkapnya tentang cara mengakses dan melihat peristiwa Wawasan di konsol dan menggunakanAWS CLI, lihat Melihat acara CloudTrail Wawasan untuk jalur di panduan ini.

Gambar berikut menunjukkan contoh peristiwa Wawasan untuk sebuah jejak. Anda membuka halaman detail untuk acara Insights dengan memilih nama acara Insights dari halaman Dasbor atau Wawasan.

Jika Anda menonaktifkan CloudTrail Insights di jejak, atau menghentikan pencatatan pada jejak (yang menonaktifkan CloudTrail Insights), Anda mungkin menyimpan peristiwa Insights di bucket S3 tujuan, atau ditampilkan di halaman Insights konsol, tanggal tersebut dari waktu sebelumnya saat Anda mengaktifkan Insights.

Kolom filter

Kolom kiri mencantumkan peristiwa Insights yang terkait dengan API subjek, dan yang memiliki jenis peristiwa Insights yang sama. Kolom ini memungkinkan Anda memilih acara Wawasan tentang informasi selengkapnya yang Anda inginkan. Saat Anda memilih acara di kolom ini, acara disorot dalam grafik di tab Grafik wawasan. Secara default, CloudTrail menerapkan filter yang membatasi peristiwa yang ditampilkan di tab CloudTrailperistiwa dengan API tertentu yang dipanggil selama periode aktivitas tidak biasa yang memicu peristiwa Insights. Untuk menampilkan semua CloudTrail peristiwa yang disebut selama periode aktivitas yang tidak biasa, termasuk peristiwa yang tidak terkait dengan peristiwa Wawasan, matikan filter.

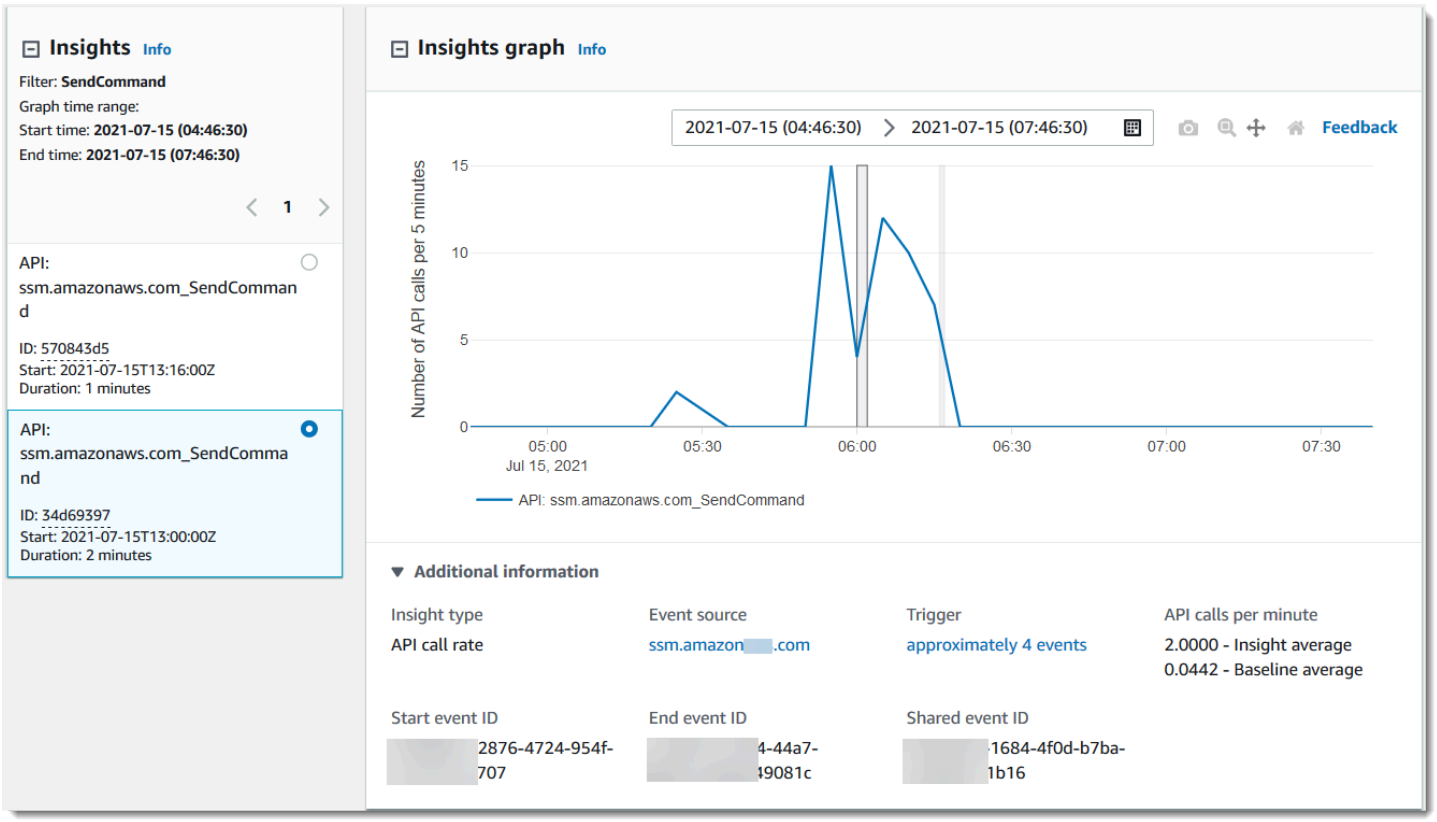
Tab grafik wawasan

Pada tab grafik Insights, halaman detail untuk peristiwa Insights menampilkan grafik volume panggilan API atau tingkat kesalahan yang terjadi selama periode waktu sebelum dan sesudah satu atau beberapa peristiwa Insights dicatat. Dalam grafik, peristiwa Insights disorot dengan bilah vertikal, dengan lebar bilah menunjukkan waktu mulai dan akhir acara Wawasan.

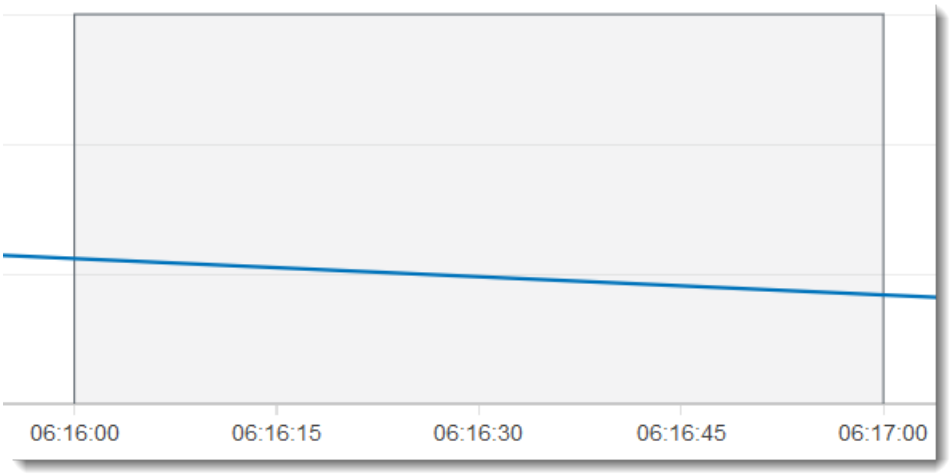
Dalam contoh ini, pita penyorotan vertikal menunjukkan jumlah panggilan AWS Systems Manager `SendCommand` API yang tidak biasa di akun. Di area yang disorot, karena jumlah `SendCommand` panggilan naik di atas rata-rata dasar akun sebesar 0,0442 panggilan per menit, CloudTrail mencatat peristiwa Wawasan ketika mendeteksi aktivitas yang tidak biasa. Acara Insights mencatat bahwa sebanyak 15 `SendCommand` panggilan dilakukan dalam periode lima menit antara pukul 5:50 dan

5:55 pagi. Ini adalah sekitar dua panggilan lagi ke API itu per menit daripada yang diharapkan untuk akun. Dalam contoh ini, rentang waktu grafik adalah tiga jam: 4:30 pagi. PDT pada 15 Juli 2021 hingga 7:30 pagi PDT pada 15 Juli 2021. Acara ini memiliki waktu mulai pukul 6:00 pagi. PDT pada 15 Juli 2021, dan waktu berakhir dua menit kemudian. Acara akhir Insights, tidak disorot, menunjukkan bahwa aktivitas yang tidak biasa berakhir sekitar pukul 6:16 pagi.

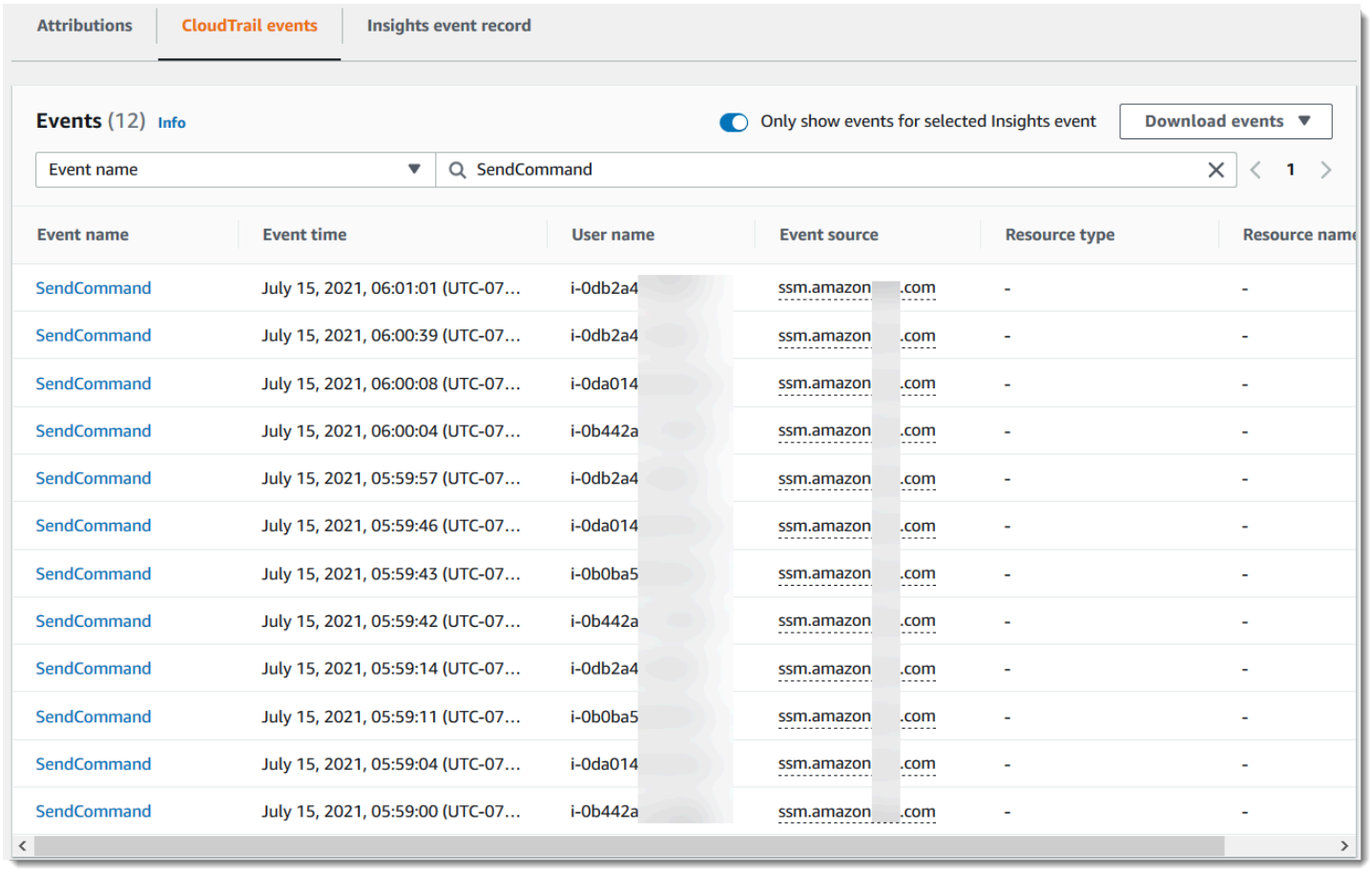
Garis dasar dihitung selama tujuh hari sebelum dimulainya acara Insights. Meskipun nilai durasi dasar — periode yang CloudTrail menganalisis aktivitas normal pada APIS — adalah sekitar tujuh hari, membulatkan durasi dasar menjadi satu hari bilangan CloudTrail bulat penuh, sehingga durasi dasar yang tepat dapat bervariasi.



Anda dapat menggunakan perintah Zoom pada bilah alat untuk memperbesar acara Wawasan akhir, yang menunjukkan waktu mulai dan berakhir. Dalam contoh ini, memilih Zoom, lalu menyeret kursor Zoom jarak yang sangat pendek ke salah satu tepi acara Insights yang disorot memperluas acara Insights dan menampilkan lebih banyak detail timeline.

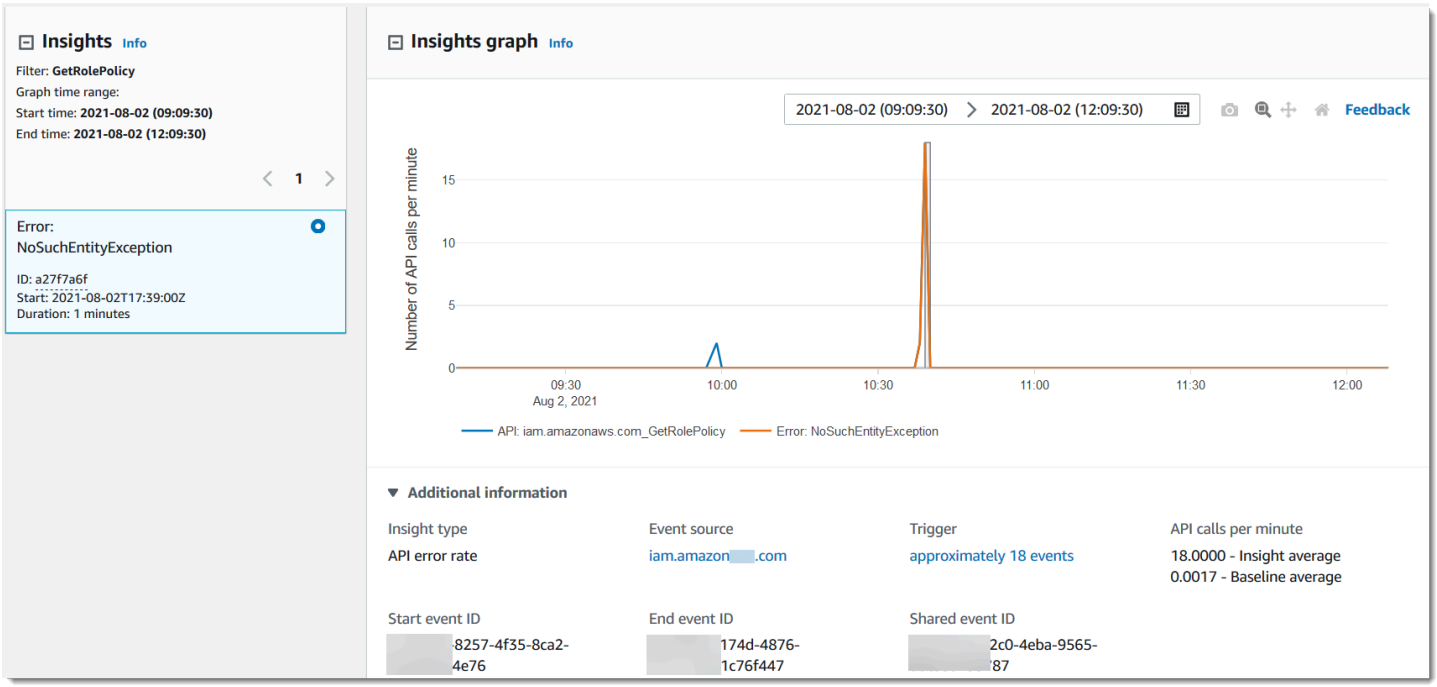


Untuk melihat CloudTrail peristiwa yang dianalisis untuk menentukan aktivitas yang tidak biasa, buka tab CloudTrail peristiwa. Dalam contoh ini, CloudTrail menganalisis 12 peristiwa, empat di antaranya memicu peristiwa Wawasan.



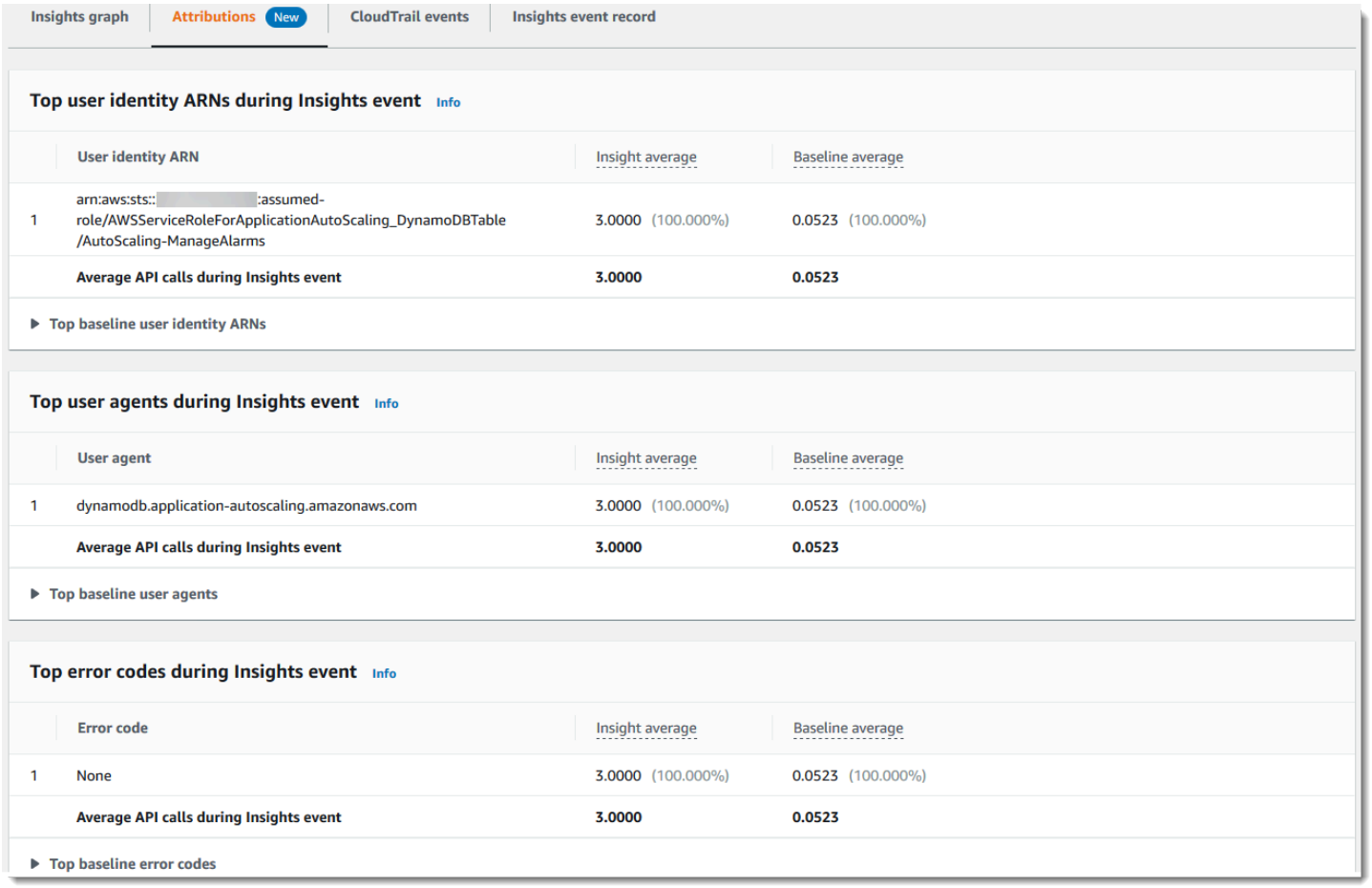
Gambar berikut menunjukkan tab grafik Insights untuk peristiwa Insights tingkat kesalahan API. Area yang disorot menunjukkan bahwa peristiwa Insights dicatat karena kejadian

`NoSuchEntityException` kesalahan pada panggilan API `GetRolePolicy` IAM naik di atas rata-rata dasar 0,0017 `NoSuchEntityException` kesalahan per menit pada panggilan API ini, rata-rata 18 kesalahan per menit selama periode wawasan. Jumlah CloudTrail peristiwa yang memicu peristiwa Insights cocok dengan rata-rata Wawasan 18 `NoSuchEntityException` kesalahan dalam satu menit, dalam contoh ini. Tidak seperti grafik laju panggilan API, tingkat kesalahan API menunjukkan dua baris, dalam warna yang kontras: garis yang mengukur panggilan ke API IAM,`GetRolePolicy`, yang menghasilkan jumlah kesalahan yang tidak biasa, dan garis yang mengukur kesalahan di mana aktivitas yang tidak biasa dicatat,. `NoSuchEntityException`

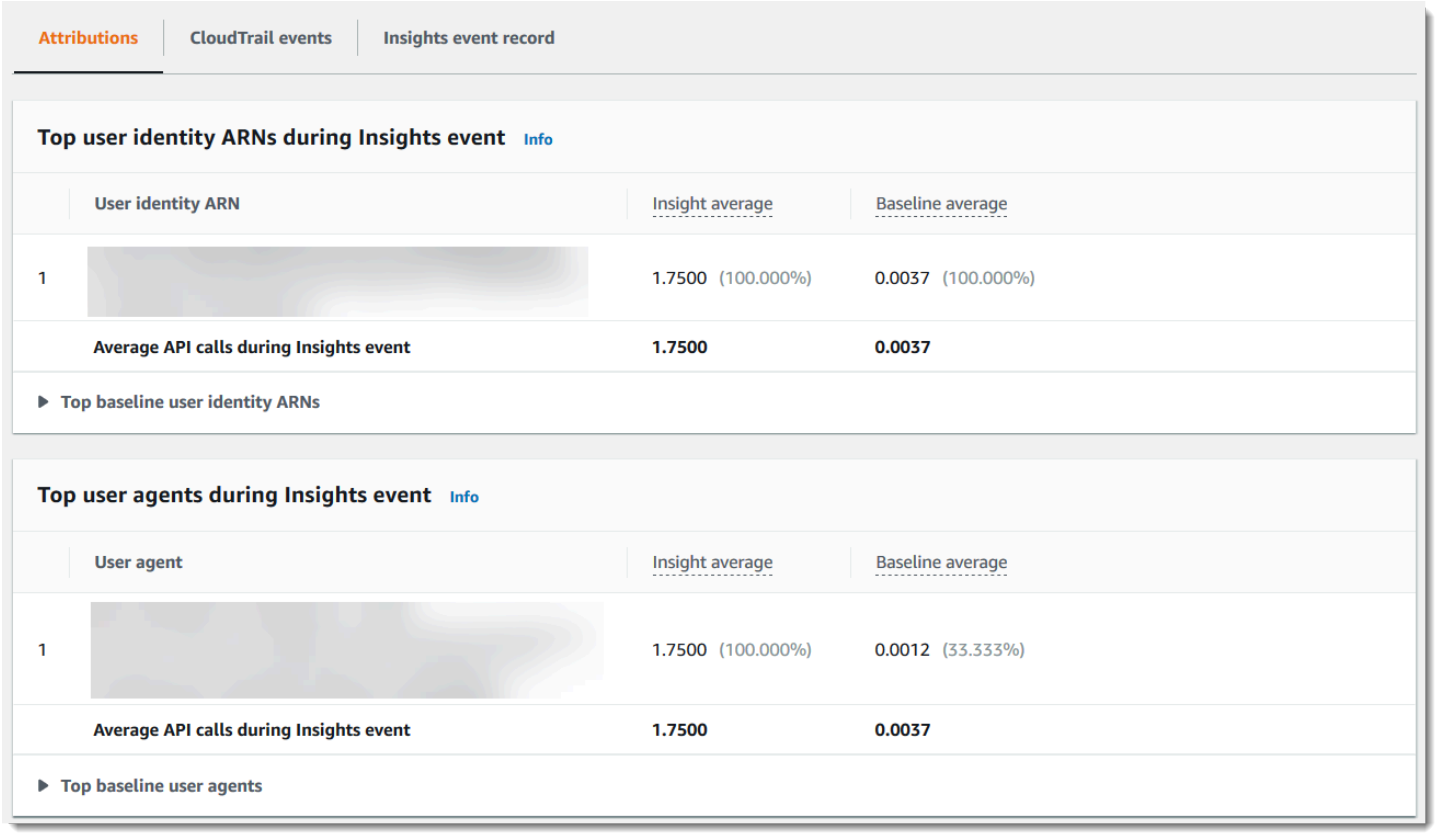


Tab Atribusi

Tab Atribusi menampilkan informasi berikut tentang peristiwa Wawasan. Informasi pada tab Atribusi dapat membantu Anda mengidentifikasi penyebab dan sumber aktivitas Wawasan. Perluas area dasar teratas untuk membandingkan identitas pengguna, agen pengguna, dan aktivitas kode kesalahan selama periode normal dengan yang dikaitkan selama aktivitas Wawasan. Di ARN identitas pengguna dasar teratas, Agen pengguna dasar teratas, dan kode kesalahan dasar teratas, hanya rata-rata baseline — rata-rata historis peristiwa untuk API yang dicatat oleh identitas pengguna, agen pengguna, atau yang menghasilkan kode kesalahan, kira-kira tujuh hari sebelum waktu mulai acara Wawasan — ditampilkan.



Tab Atribusi hanya menampilkan ARN identitas pengguna teratas dan agen pengguna teratas untuk peristiwa Insights tingkat kesalahan, seperti yang ditunjukkan pada gambar berikut. Kode kesalahan teratas tidak diperlukan untuk peristiwa Insights tingkat kesalahan.



- ARN identitas pengguna teratas - Tabel ini menampilkan hingga lima AWS pengguna teratas atau peran IAM (identitas pengguna) yang berkontribusi pada panggilan API selama aktivitas dan periode dasar yang tidak biasa, dalam urutan menurun menurut jumlah rata-rata panggilan API yang dikontribusikan. Persentase rata-rata sebagai total aktivitas yang berkontribusi pada aktivitas yang tidak biasa ditunjukkan dalam tanda kurung. Jika lebih dari lima ARN identitas pengguna berkontribusi pada aktivitas yang tidak biasa, aktivitas mereka diringkas dalam baris Lainnya.
- Agen pengguna teratas - Tabel ini menampilkan hingga lima AWS alat teratas yang dengannya identitas pengguna berkontribusi pada panggilan API selama aktivitas dan periode dasar yang tidak biasa, dalam urutan menurun menurut jumlah rata-rata panggilan API yang disumbangkan. Alat-alat ini termasuk AWS Management ConsoleAWS CLI,, atau AWS SDK. Misalnya, agen pengguna bernama `ec2.amazonaws.com` menunjukkan bahwa konsol Amazon EC2 adalah salah satu alat yang digunakan untuk memanggil API. Persentase rata-rata sebagai total aktivitas yang berkontribusi pada aktivitas yang tidak biasa ditunjukkan dalam tanda kurung. Jika lebih dari lima agen pengguna berkontribusi pada aktivitas yang tidak biasa, aktivitas mereka diringkas dalam baris Lain.
- Kode kesalahan teratas - Hanya ditampilkan untuk peristiwa Insights tingkat panggilan API. Tabel ini menampilkan hingga lima kode kesalahan teratas yang terjadi pada panggilan API selama

aktivitas dan periode dasar yang tidak biasa, dalam urutan menurun dari jumlah panggilan API terbesar hingga terkecil. Persentase rata-rata sebagai total aktivitas yang berkontribusi pada aktivitas yang tidak biasa ditunjukkan dalam tanda kurung. Jika lebih dari lima kode kesalahan terjadi selama aktivitas yang tidak biasa atau baseline, aktivitas mereka diringkas dalam baris Lain.

Nilai None sebagai salah satu dari lima nilai kode kesalahan teratas berarti bahwa persentase signifikan dari panggilan yang berkontribusi pada peristiwa Wawasan tidak menghasilkan kesalahan. Jika nilai kode kesalahan adalahNone, dan tidak ada kode kesalahan lain dalam tabel, nilai dalam rata-rata Insight dan kolom rata-rata Baseline sama dengan nilai untuk peristiwa Insights secara keseluruhan. Anda juga dapat melihat nilai tersebut ditampilkan dalam rata-rata Insight dan legenda rata-rata dasar pada tab Grafik Insights, di bawah panggilan API per menit.

Rata-rata dasar dan rata-rata Wawasan

Rata-rata dasar dan rata-rata Wawasan ditampilkan untuk identitas pengguna teratas, agen pengguna teratas, dan kode kesalahan teratas.

- Rata-rata dasar - Tingkat kejadian tipikal per menit pada API tempat peristiwa Insights dicatat, yang diukur dalam kira-kira tujuh hari sebelumnya, di Wilayah tertentu di akun Anda.
- Rata-rata wawasan - Tingkat panggilan atau kesalahan pada API ini yang memicu peristiwa Insights. Rata-rata CloudTrail Insights untuk acara mulai adalah tingkat panggilan atau error per menit pada API yang memicu peristiwa Insights. Biasanya, ini adalah menit pertama aktivitas yang tidak biasa. Rata-rata Insights untuk acara akhir adalah tingkat panggilan API atau error per menit selama durasi aktivitas yang tidak biasa, antara peristiwa Insights awal dan peristiwa Insights akhir.

CloudTrail tab acara

Pada tab CloudTrail peristiwa, lihat peristiwa terkait yang CloudTrail dianalisis untuk menentukan bahwa aktivitas yang tidak biasa terjadi. Secara default, filter sudah diterapkan untuk nama acara Insights, yang juga merupakan nama API terkait. Untuk menampilkan semua CloudTrail peristiwa yang dicatat selama periode aktivitas yang tidak biasa, matikan Hanya tampilkan acara untuk acara Wawasan yang dipilih. Tab CloudTrail peristiwa menampilkan peristiwa CloudTrail manajemen yang terkait dengan API subjek yang terjadi antara waktu mulai dan akhir acara Insights. Peristiwa ini membantu Anda melakukan analisis lebih dalam untuk menentukan kemungkinan penyebab peristiwa Insights, dan alasan aktivitas API dan tingkat kesalahan yang tidak biasa.

Tab catatan acara wawasan

Seperti CloudTrail acara apa pun, acara CloudTrail Insights adalah catatan dalam format JSON. Tab catatan peristiwa Insights menunjukkan struktur JSON dan konten peristiwa awal dan akhir Insights, kadang-kadang disebut payload peristiwa. Untuk informasi selengkapnya tentang bidang dan konten catatan acara Wawasan, lihat Kolom rekaman untuk acara Insights dan CloudTrail Wawasan`insightDetails`elemen dalam panduan ini.

Mengirim acara jejak ke Amazon CloudWatch Logs

CloudTrail mendukung pengiriman acara Wawasan untuk jejak ke CloudWatch Log. Saat mengonfigurasi jejak Anda untuk mengirim peristiwa Wawasan ke grup CloudWatch log Log, CloudTrail Wawasan hanya akan mengirimkan peristiwa yang Anda tentukan di jejak Anda. Misalnya, jika Anda mengonfigurasi jejak Anda ke manajemen log dan peristiwa Wawasan, jejak Anda akan mengirimkan peristiwa manajemen dan Wawasan ke grup CloudWatch log Log Anda. Untuk informasi selengkapnya, lihat Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Menerima file CloudTrail log dari beberapa Wilayah

Anda dapat mengonfigurasi CloudTrail untuk mengirimkan file log dari beberapa Wilayah ke satu bucket S3 untuk satu akun. Misalnya, Anda memiliki jejak di Wilayah Barat AS (Oregon) yang dikonfigurasi untuk mengirimkan file log ke bucket S3, dan grup CloudWatch log Log. Saat Anda mengubah jejak Wilayah Tunggal yang ada untuk mencatat semua Wilayah, CloudTrail mencatat peristiwa dari semua Wilayah yang ada dalam satu AWS partisi 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 jalur Multi-wilayah tidak harus berada di Wilayah asal jalur tersebut.

Untuk mencatat peristiwa di semua Wilayah di semua AWS partisi di akun Anda, buat jejak Multi-wilayah di setiap partisi.

Di konsol, secara default, Anda membuat jejak yang mencatat peristiwa Wilayah AWS di semua AWSpartisi tempat Anda bekerja. Ini adalah praktik terbaik yang direkomendasikan. Untuk mencatat peristiwa di satu Wilayah (tidak disarankan), gunakan AWS CLI. Untuk mengonfigurasi jejak wilayah Tunggal yang ada untuk masuk ke semua Wilayah, Anda harus menggunakan. AWS CLI

Untuk mengubah jejak yang ada sehingga berlaku untuk semua Wilayah, 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 berlaku untuk semua Wilayah, `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": "my-bucket"
}
```

> **Note**
>
> Saat Region baru diluncurkan di awspartisi, CloudTrail secara otomatis membuat jejak untuk Anda di Wilayah baru dengan pengaturan yang sama dengan jejak asli Anda.

Untuk informasi lebih lanjut, lihat sumber daya berikut:

- Bagaimana CloudTrail berperilaku regional dan global?
- CloudTrail FAQ

Mengelola konsistensi data dalam CloudTrail

CloudTrail menggunakan model komputasi terdistribusi yang disebutkonsistensi akhirnya. Setiap perubahan yang Anda buat untuk Anda CloudTrail konfigurasi (atau lainnyaAWSlayanan), termasuk tag yang digunakan dikontrol akses berbasis atribut (ABAC), membutuhkan waktu untuk menjadi terlihat dari semua titik akhir yang mungkin. Beberapa penundaan dihasilkan dari waktu yang diperlukan untuk mengirim data dari server ke server, dari zona replikasi ke zona replikasi, 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 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 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 acara, CloudTrail mengirimkan log ke bucket S3 atau penyimpanan data peristiwa berdasarkan konfigurasi terakhir yang diketahui hingga perubahan menyebar ke semua lokasi.

Untuk informasi lebih lanjut tentang bagaimana ini mempengaruhi orang lainLayanan AWS, lihat sumber daya berikut:

- Amazon DynamoDB:Apa model konsistensi DynamoDB?diDynamoDB FAM, danBaca konsistensidiPanduan Pengembang Amazon DynamoDB.
- Amazon EC2:Konsistensi akhirnyadiReferensi API Awan Elastis.
- EMR Amazon:Memastikan Konsistensi Saat Menggunakan Amazon S3 dan Amazon Elastic MapReduce untuk Alur Kerja ETLdiAWSBlog Data Besar.
- AWS Identity and Access Management(SAYA):Perubahan yang saya buat tidak selalu langsung terlihatdiPanduan Pengguna IAM.
- Pergeseran Merah Amazon:Mengelola konsistensi datadiPanduan Pengembang Basis Data Amazon Redshift.
- Amazon S3:Model konsistensi data Amazon S3diPanduan Pengguna Layanan Penyimpanan Sederhana.

Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log

Anda dapat mengonfigurasi CloudTrail bersama 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. Mendefinisikan CloudWatch Log filter metrik untuk mengevaluasi kejadian log, lalu mengevaluasi kejadian, frasa, atau nilai. Misalnya, Anda dapat memantau`ConsoleLogin`peristiwa.
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, lalu mengirimkan notifikasi 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, lihatAmazon CloudWatch Harga.

Untuk informasi selengkapnya tentang Wilayah tempat Anda dapat mengonfigurasi jejak Anda untuk mengirim log CloudWatch Log, lihatAmazon CloudWatch Log Wilayah dan KuotadiAWSReferensi Umum.

Topik

- Mengirim acara ke CloudWatch Log
- Menciptakan CloudWatch alarm untuk CloudTrail Peran: contoh
- Berhenti CloudTrail dari mengirim acara ke CloudWatch Log
- CloudWatch grup log dan log nama 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 untuk mencatat peristiwa data saja, jejak Anda hanya akan mengirimkan peristiwa data 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 CloudWatch Log Amazon di konsol CloudTrail .
- Jika Anda mengonfigurasi grup CloudWatch log Log menggunakanAWS 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 organisasi.
- Lampirkan kebijakan peran atau gunakan default.

Daftar Isi

Mengkonfigurasi pemantauan CloudWatch Log dengan konsol

Anda dapat menggunakan AWS Management Console 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 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 CloudWatch Log Amazon di konsol CloudTrail .

   > **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 yang berlaku untuk semua 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 yang berlaku untuk semua Wilayah mengirimkan file log dari semua Wilayah ke grup CloudWatch log Log yang Anda tentukan.

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 log nama aliran log untuk CloudTrail.
7. Jika Anda memilih 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 yang ada 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 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 isinya.

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
```

Menciptakan 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`.

```
{
  "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.

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

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 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 akun 111111111111 dan untuk jejak organisasi yang dibuat di AWS akun 111111111111 yang diterapkan ke organisasi dengan ID CloudTrail o-exampleorgid: AWS Organizations

```
{
    "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_*"
            ]
        }
    ]
}
```

Untuk informasi selengkapnya tentang jalur organisasi, lihatMembuat jejak untuk 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.

Menciptakan CloudWatch alarm untuk CloudTrail Peran: contoh

Topik ini menjelaskan cara mengonfigurasi alarm untuk CloudTrail peristiwa, dan termasuk contoh.

Topik

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.
- Tentukan atau buat peran IAM yang memberikan CloudTrail izin untuk membuatCloudWatch Aliran log log di grup log yang Anda tentukan dan kirimkan CloudTrail peristiwa ke aliran log itu. Menetapkan standar`CloudTrail_CloudWatchLogs_Role`melakukan ini untuk Anda.

Untuk informasi selengkapnya, lihat Mengirim acara ke CloudWatch Log. Contoh di bagian ini dilakukan di Amazon CloudWatch Konsol log. Untuk informasi selengkapnya tentang cara membuat filter dan alarm metrik, lihatMembuat metrik dari peristiwa log menggunakan filterdanMenetapkan Amazon CloudWatch alarmdiAmazon CloudWatch Panduan Pengguna.

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 CloudTrail log peristiwa, lihat bagian terkait JSONFilter dan sintaks poladiAmazon CloudWatch Panduan Pengguna Log.

Contoh perubahan konfigurasi grup keamanan

Ikuti prosedur ini untuk membuat Amazon CloudWatch alarm yang dipicu ketika perubahan konfigurasi terjadi pada grup keamanan.

Buat filter metrik

1. Menetapkan CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, padaLog, pilihMenetapkan log.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. DariFilter metrikatauTindakanmenu, pilihBuat filter metrik.
5. PadaTentukan polahalaman, diBuat pola filter, masukkan yang berikut untukPola filter.

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. DiPola uji, tinggalkan default. Pilih Selanjutnya.
7. PadaMenetapkan metrikhalaman, untukFilter nama, masukkan**SecurityGroupEvents**.
8. DiDetail metrik, nyalakanMenetapkan yang baru, dan kemudian masuk**CloudTrailMetrics**untukRuang nama metrik.
9. UntukNama metrik, ketik**SecurityGroupEventCount**.
10. UntukNilai metrik, ketik**1**.
11. MeninggalkanMenetapkan nilai defaultkosong
12. Pilih Selanjutnya.
13. PadaMemeriksa dan membuathalaman, tinjau pilihan Anda. PilihBuat filter metrikuntuk membuat filter, atau memilihSuntinguntuk kembali dan mengubah nilai.

Buat alarm

Setelah Anda membuat filter metrik, CloudWatch Halaman detail grup log log untuk Anda CloudTrail grup log jejak terbuka. Ikuti prosedur ini untuk membuat alarm.

1. PadaFilter metriktab, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. DiFilter metrikbar, pilihMenetapkan alarm.
2. UntukTentukan metrik dan kondisi, masukkan yang berikut.
   a. UntukGrafik, garis diatur pada**1**berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. UntukNama metrik, pertahankan nama metrik saat ini,**SecurityGroupEventCount**.
   c. UntukStatistik, pertahankan default,**Sum**.
   d. UntukPeriode, pertahankan default,**5 minutes**.
   e. DiKetentuan, untukJenis ambang, pilihStatis.
   f. UntukKapan pun***metric_name***adalah, pilihLebih Besar/Setara.
   g. Untuk nilai ambang, masukkan**1**.
   h. DiKonfigurasi tambahan, tinggalkan default. Pilih Selanjutnya.
3. PadaKonfigurasikan tindakanhalaman, pilihPemberitahuan, dan kemudian pilihDalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang 1 peristiwa perubahan dalam 5 menit dilintasi, danSecurityGroupEventCountberada di kondisi alarm.
   a. UntukKirim pemberitahuan ke topik SNS berikut, pilihBuat topik baru.

b. Masuk**SecurityGroupChanges_CloudWatch_Alarms_Topic**sebagai nama untuk topik Amazon SNS yang baru.

c. DiEndpoint 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 Selanjutnya.
5. PadaTambahkan nama dan deskripsihalaman, masukkan nama yang ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan**Security group configuration changes**untuk nama, dan**Raises alarms if security group configuration changes occur**untuk deskripsi. Pilih Selanjutnya.
6. PadaPratinjau dan buathalaman, tinjau pilihan Anda. PilihSuntinguntuk membuat perubahan, atau memilihMenetapkan alarmuntuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch membukaAlarmhalaman AlarmTindakankolom menunjukkanKonfirmasi yang tertundasampai semua penerima email pada topik SNS telah mengkonfirmasi bahwa mereka ingin berlangganan pemberitahuan SNS.

ContohAWS Management Consolekegagalan masuk

Ikuti prosedur ini untuk membuat Amazon CloudWatch alarm yang dipicu ketika ada tiga atau lebihAWS Management Consolekegagalan masuk selama periode lima menit.

Buat filter metrik

1. Menetapkan CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, padaLog, pilihMenetapkan log.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. DariFilter metrikatauTindakanmenu, pilihBuat filter metrik.
5. PadaTentukan polahalaman, diBuat pola filter, masukkan yang berikut untukPola filter.

```
{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
```

6. DiPola uji, tinggalkan default. Pilih Selanjutnya.

7. PadaMenetapkan metrikhalaman, untukFilter nama, masukkan**`ConsoleSignInFailures`**.
8. DiDetail metrik, nyalakanMenetapkan yang baru, dan kemudian masuk**`CloudTrailMetrics`**untukRuang nama metrik.
9. UntukNama metrik, ketik**`ConsoleSigninFailureCount`**.
10. UntukNilai metrik, ketik**`1`**.
11. MeninggalkanNilai defaultkosong
12. Pilih Selanjutnya.
13. PadaMemeriksa dan membuathalaman, tinjau pilihan Anda. PilihBuat filter metrikuntuk membuat filter, atau memilihSuntinguntuk kembali dan mengubah nilai.

Buat alarm

Setelah Anda membuat filter metrik, CloudWatch Halaman detail grup log log untuk Anda CloudTrailgrup log jejak terbuka. Ikuti prosedur ini untuk membuat alarm.

1. PadaFilter metriktab, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. DalamFilter metrikbar, pilihMenetapkan alarm.
2. PadaMenetapkan Alarmhalaman, diTentukan metrik dan kondisi, masukkan yang berikut.
   a. UntukGrafik, garis diatur pada**`3`**berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. UntukNama metrik, pertahankan nama metrik saat ini,**`ConsoleSigninFailureCount`**.
   c. UntukStatistik, pertahankan default,**`Sum`**.
   d. UntukPeriode, pertahankan default,**`5 minutes`**.
   e. DiKetentuan, untukJenis ambang, pilihStatis.
   f. UntukKapan pun***`metric_name`***adalah, pilihLebih Besar/Setara.
   g. Untuk nilai ambang, masukkan**`3`**.
   h. DiKonfigurasi tambahan, tinggalkan default. Pilih Selanjutnya.
3. PadaKonfigurasikan tindakanhalaman, untukPemberitahuan, pilihDalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang 3 peristiwa perubahan dalam 5 menit dilintasi, danConsoleSigninFailureCountberada di kondisi alarm.
   a. UntukKirim pemberitahuan ke topik SNS berikut, pilihBuat topik baru.

b. Masuk**`ConsoleSignInFailures_CloudWatch_Alarms_Topic`**sebagai nama untuk topik Amazon SNS yang baru.

c. DiEndpoint 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 Selanjutnya.
5. PadaTambahkan nama dan deskripsihalaman, masukkan nama yang ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan**`Console sign-in failures`**untuk nama, dan**`Raises alarms if more than 3 console sign-in failures occur in 5 minutes`**untuk deskripsi. Pilih Selanjutnya.
6. PadaPratinjau dan buathalaman, tinjau pilihan Anda. PilihSuntinguntuk membuat perubahan, atau memilihMenetapkan alarmuntuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch membukaAlarmhalaman AlarmTindakankolom menunjukkanKonfirmasi yang tertundasampai semua penerima email pada topik SNS telah mengkonfirmasi bahwa mereka ingin berlangganan pemberitahuan SNS.

Contoh: Perubahan kebijakan IAM

Ikuti prosedur ini untuk membuat Amazon CloudWatch alarm yang dipicu saat panggilan API dibuat untuk mengubah kebijakan IAM.

Buat filter metrik

1. Menetapkan CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, pilih Log.
3. Dalam daftar grup log, pilih grup log yang Anda buat untuk jejak Anda.
4. PilihTindakan, dan kemudian pilihBuat filter metrik.
5. PadaTentukan polahalaman, diBuat pola filter, masukkan yang berikut untukPola 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. DiPola uji, tinggalkan default. Pilih Selanjutnya.
7. PadaTetapkan metrikhalaman, untukFilter nama, masukkan**`IAMPolicyChanges`**.
8. DiDetail metrik, nyalakanMenetapkan yang baru, dan kemudian masuk**`CloudTrailMetrics`**untukRuang nama metrik.
9. UntukNama metrik, ketik**`IAMPolicyEventCount`**.
10. UntukNilai metrik, ketik**`1`**.
11. MeninggalkanNilai defaultkosong
12. Pilih Selanjutnya.
13. PadaMemeriksa dan membuathalaman, tinjau pilihan Anda. PilihBuat filter metrikuntuk membuat filter, atau memilihSuntinguntuk kembali dan mengubah nilai.

Buat alarm

Setelah Anda membuat filter metrik, CloudWatch Halaman detail grup log log untuk Anda CloudTrailgrup log jejak terbuka. Ikuti prosedur ini untuk membuat alarm.

1. PadaFilter metriktab, temukan filter metrik yang Anda buatthe section called “Buat filter metrik”. Isi kotak centang untuk filter metrik. DalamFilter metrikbar, pilihMenetapkan alarm.
2. PadaMenetapkan Alarmhalaman, diTentukan metrik dan kondisi, masukkan yang berikut.
   a. UntukGrafik, garis diatur pada**`1`**berdasarkan pengaturan lain yang Anda buat saat membuat alarm.
   b. UntukNama metrik, pertahankan nama metrik saat ini,**`IAMPolicyEventCount`**.
   c. UntukStatistik, pertahankan default,**`Sum`**.
   d. UntukPeriode, pertahankan default,**`5 minutes`**.
   e. DiKetentuan, untukJenis ambang, pilihStatis.
   f. UntukKapanpun***`metric_name`***adalah, pilihLebih Besar/Setara.
   g. Untuk nilai ambang, masukkan**`1`**.
   h. DiKonfigurasi tambahan, tinggalkan default. Pilih Selanjutnya.
   i.

3. PadaKonfigurasikan tindakanhalaman, untukPemberitahuan, pilihDalam alarm, yang menunjukkan bahwa tindakan diambil ketika ambang 1 peristiwa perubahan dalam 5 menit dilintasi, danIAMPolicyEventCountberada di kondisi alarm.

   a. UntukKirim pemberitahuan ke topik SNS berikut, pilihBuat topik baru.

   b. Masuk**`IAM_Policy_Changes_CloudWatch_Alarms_Topic`**sebagai nama untuk topik Amazon SNS yang baru.

   c. DiEndpoint 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 Selanjutnya.

5. PadaTambahkan nama dan deskripsihalaman, masukkan nama yang ramah untuk alarm, dan deskripsi. Untuk contoh ini, masukkan**`IAM Policy Changes`**untuk nama, dan**`Raises alarms if IAM policy changes occur`**untuk deskripsi. Pilih Selanjutnya.

6. PadaPratinjau dan buathalaman, tinjau pilihan Anda. PilihSuntinguntuk membuat perubahan, atau memilihMenetapkan alarmuntuk membuat alarm.

   Setelah Anda membuat alarm, CloudWatch membukaAlarmhalaman AlarmTindakankolom menunjukkanKonfirmasi yang tertundasampai semua penerima email pada topik SNS telah mengkonfirmasi bahwa mereka ingin berlangganan pemberitahuan SNS.

Mengkonfigurasi notifikasi untuk CloudWatch Alarm log

Anda dapat mengkonfigurasi CloudWatch Log untuk mengirim pemberitahuan setiap kali alarm dipicu CloudTrail. Melakukannya memungkinkan Anda merespons dengan cepat peristiwa operasional penting yang terekam CloudTrailperistiwa dan terdeteksi oleh CloudWatch Log. CloudWatch menggunakan Amazon Simple Notification Service (SNS) untuk mengirim email. Untuk informasi selengkapnya, lihatMengatur Amazon SNSdiCloudWatch Panduan Pengembang.

Berhenti CloudTrail dari mengirim acara ke CloudWatch Log

Anda dapat berhenti mengirimAWS CloudTrailacara ke Amazon CloudWatch Log dengan memperbarui jejak untuk menonaktifkan CloudWatch Pengaturan log.

Berhenti mengirim acara ke CloudWatch Log (konsol)

Untuk berhenti mengirim CloudTrail peristiwa untuk CloudWatch Log

1. Masuk keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilih Jejak.
3. Pilih nama jejak yang ingin Anda nonaktifkan CloudWatch Integrasi log.
4. DiCloudWatch Log, pilihSunting.
5. Hapus Diaktifkan kotak centang.
6. Pilih Save changes (Simpan perubahan).

Berhenti mengirim acara ke CloudWatch Log (CLI)

Anda dapat menghapus CloudWatch Log grup log sebagai titik akhir pengiriman dengan menjalankanupdate-trailperintah. Perintah berikut membersihkan grup log dan peran dari konfigurasi jejak dengan mengganti nilai untuk grup log ARN dan CloudWatch Log peran 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 log nama aliran log untuk CloudTrail

Amazon CloudWatch akan menampilkan grup log yang Anda buat 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. Sebagai contoh, **`CloudTrail/logs`**.

Ikuti panduan berikut saat menamai grup log:

- Nama grup log terdiri dari nama yang unik dalam suatu daerah untukAkun 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).

Kapan CloudTrail membuat aliran log untuk grup log, itu menamai aliran log sesuai dengan format berikut:*Account_ID*_CloudTrail_*trail_region*.

> **Note**
>
> Jika volume CloudTrail log berukuran besar, beberapa aliran log dapat dibuat untuk mengirimkan data log ke grup log Anda. Ketika ada beberapa aliran log, CloudTrail nama setiap log terdiri dari format berikut:*Account_ID*_CloudTrail_*trail_region*_*nomor*.

Untuk informasi lebih lanjut tentang CloudWatch grup log, lihatBekerja dengan grup log dan log streamdiAmazon CloudWatch Panduan Pengguna logdanCreateLogGroupdiAmazon CloudWatch Referensi API log.

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 AWS Service (AWS Management Console) atau Membuat Peran (CLI dan API).

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`.)

> **Note**
>
> Pencegahan wakil yang bingung tidak berlaku untuk kebijakan peran untuk pemantauan CloudWatch Log. Kebijakan peran tidak mendukung penggunaan `aws:SourceArn` dan`aws:SourceAccount`.

```
{
```

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID: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:accountID: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 izin yang diperlukan untuk membuat aliran log Log di grup CloudWatch log yang Anda tentukan sebagai nilai log_group_name, dan untuk mengirimkan CloudTrail peristiwa ke aliran log tersebut untuk kedua jejak di akun 11111111111111 dan untuk jejak organisasi yang dibuat di AWS akun 11111111111111 yang diterapkan ke organisasi dengan ID CloudTrail o-exampleorgid: AWS Organizations*

```
{
    "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 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 ID akun 111111111111, 222222222222, 333333333333, dan 4444444444444444, dan Anda ingin mengonfigurasi untuk mengirimkan file log dari keempat akun ini ke bucket 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 di 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 memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasikanAWS KMSkebijakan utama untuk CloudTrail.

Menyunting ID akun pemilik bucket 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 bahkan jika 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:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

Berikut ini adalah perilaku saat ini.

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

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 pada bucket tujuan Anda untuk memberikan CloudTrail izin untuk menulis file log dari setiap akun yang ditentukan.

> **Note**
>
> Untuk alasan keamanan, pengguna yang tidak sah tidak dapat membuat jejak yang mencakup `AWSLogs/` sebagai `S3KeyPrefix` parameter.

Untuk memodifikasi izin bucket sehingga file dapat diterima dari beberapa akun

1. Masuk ke AWS Management Console menggunakan akun yang memiliki ember (111111111111 dalam contoh ini) dan buka konsol Amazon S3.
2. Pilih ember di mana CloudTrail mengirimkan file log Anda dan kemudian memilih Izin.
3. Untuk Kebijakan bucket, pilih Sunting.
4. Ubah kebijakan yang ada untuk menambahkan baris untuk setiap akun tambahan yang file lognya ingin dikirim ke bucket ini. Lihat kebijakan contoh berikut dan perhatikan kebijakan contoh berikut `Resource` baris yang menentukan ID akun kedua. Sebagai praktik keamanan terbaik, tambahkan `aws:SourceArn` kunci kondisi ke kebijakan bucket S3. Ini membantu mencegah akses akses tidak sah ke bucket S3 Anda. Jika Anda memiliki jalur yang ada, pastikan untuk menambahkan satu atau lebih kunci kondisi.

   > **Note**
   >
   > Sebuah AWS ID akun adalah nomor dua belas digit, termasuk angka nol di depan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "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:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
          "arn:aws:s3:::myBucketName/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 antarmuka baris perintah untuk membuat jejak di AWS akun tambahan dan menggabungkan file log mereka ke satu bucket Amazon S3.

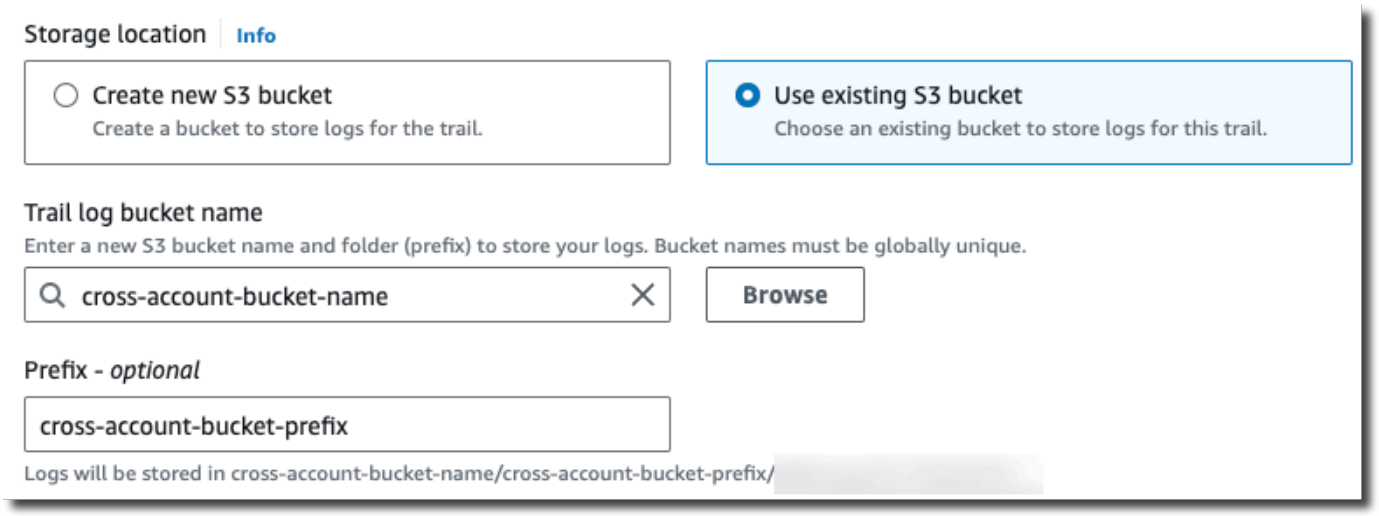
Menggunakan konsol untuk membuat jejak di akun tambahan AWS

Anda dapat menggunakan CloudTrail konsol untuk membuat jejak di akun tambahan.

1. Masuk AWS Management Console dengan akun yang ingin Anda buat jejaknya. Ikuti langkah-langkah Membuat jejak di 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 di akun tambahan AWS

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 Panduan AWS Command Line Interface Pengguna.

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 menggunakanAWS 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 my-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": "MyBucketBelongingToAccount111111111111"
}
```

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 (ACL). Secara default, Kepemilikan

Objek disetel ke setelan diberlakukan pemilik Bucket dan semua ACL dinonaktifkan. Saat ACL 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 Sumber Daya AWS Anda ke 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

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`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id: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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

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:

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id: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.

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

```
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

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 kredensil 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.

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

```
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
    }
  ]
}
```

Untuk menyunting kebijakan yang dikelola pelanggan (konsol)

1. Masuk ke AWS Management Console 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 langkah 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 membuat perubahan atau memilih Berikutnya di editor Visual, IAM mungkin merestrukturisasi kebijakan Anda untuk mengoptimalkannya untuk 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 Sumber Daya AWS Anda ke 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. Kredensil 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 kredensyal 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 lainAkun AWS, hapus peran yang Anda buat untuk akun itu. Untuk selengkapnya tentang cara menghapus peran, lihat Menghapus peran atau profil instance.

Memvalidasi CloudTrail integritas berkas log

Untuk menentukan apakah file log diubah, dihapus, atau tidak berubah setelahnya CloudTrail mengirimkannya, Anda dapat menggunakan CloudTrail validasi integritas file 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 log file tanpa deteksi. Anda dapat menggunakanAWS CLIuntuk memvalidasi file di lokasi di mana CloudTrail mengantarkan mereka.

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. The CloudTrail Proses validasi integritas file log juga memberi tahu Anda jika 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 membuat 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 berkas intisari menggunakan kunci pribadi dari sebuah key public dan private key pair. Setelah pengiriman, Anda dapat menggunakan kunci publik untuk memvalidasi file digest. CloudTrail menggunakan pasangan kunci yang berbeda untuk masing-masingWilayah AWS.

File intisari dikirimkan ke bucket Amazon S3 yang sama dengan jejak Anda. CloudTrail berkas log. Jika berkas 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 ember 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 berkas intisari, lihatCloudTrail digest struktur berkas.

Menyimpan log dan mencerna file

Anda dapat menyimpan CloudTrail log file dan mencerna file di Amazon S3 atau S3 Glacier dengan aman, tahan lama dan murah untuk jangka waktu yang tidak terbatas. Untuk meningkatkan keamanan file intisari yang disimpan di Amazon S3, Anda dapat menggunakanAmazon S3 MFA Hapus.

Mengaktifkan validasi dan memvalidasi file

Untuk mengaktifkan validasi integritas file log, Anda dapat menggunakanAWS Management Console,AWS CLI, atau CloudTrail API. Mengaktifkan validasi integritas file log memungkinkan CloudTrail untuk mengirimkan berkas log intisari ke bucket Amazon S3 Anda, tetapi tidak memvalidasi berkas log digest ke bucket Amazon S3 Anda, tetapi tidak memvalidasi berkas log. Untuk informasi selengkapnya, lihat Mengaktifkan validasi integritas file log untuk CloudTrail.

Untuk memvalidasi integritas CloudTrail file log, Anda dapat menggunakanAWS CLIatau buat solusi Anda sendiri. TheAWS CLIakan memvalidasi file di lokasi di mana CloudTrail mengantarkan mereka. 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 menggunakanAWS CLI, lihatMemvalidasi CloudTrail integritas file log denganAWS CLI. Untuk informasi tentang pengembangan implementasi kustom CloudTrail validasi file log, lihatImplementasi kustom validasi integritas file CloudTrail log.

Mengaktifkan validasi integritas file log untuk CloudTrail

Anda dapat mengaktifkan validasi integritas file log dengan menggunakanAWS Management Console,AWSAntarmuka Baris Perintah (AWS CLI), atau CloudTrail API. CloudTrail mulai mengirimkan file digest dalam waktu sekitar satu jam.

AWS Management Console

Untuk mengaktifkan validasi integritas file log dengan CloudTrail konsol, pilihyauntukAktifkan validasi file logopsi saat Anda membuat atau memperbarui jejak. Secara default, fitur ini dinonaktifkan untuk jalur baru. Untuk informasi selengkapnya, lihat Membuat dan memperbarui jejak dengan konsol.

AWS CLI

Untuk mengaktifkan validasi integritas file log denganAWS CLI, gunakan`--enable-log-file-validation`opsi dengan`buat-jejak`atau`perbaruan-jejak`perintah. Untuk menonaktifkan validasi integritas file log, gunakan`--no-enable-log-file-validation`opsi.

Contoh

Berikut ini`update-trail`perintah mengaktifkan 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, atur`EnableLogFileValidation`minta parameter untuk`true`saat menelepon`CreateTrail`atau`UpdateTrail`.

Untuk informasi selengkapnya, lihatCreateTraildanUpdateTraildiAWS CloudTrailReferensi API.

Memvalidasi CloudTrail integritas file log denganAWS CLI

Untuk memvalidasi log denganAWS Command Line Interface, gunakan CloudTrail `validate-logs`perintah. Perintah menggunakan file intiser yang dikirimkan ke bucket Amazon S3. Untuk informasi tentang file digest, lihatCloudTrail digest struktur berkas.

TheAWS CLImemungkinkan Anda mendeteksi jenis perubahan berikut:

- Modifikasi atau penghapusan CloudTrail file log
- Modifikasi atau penghapusan CloudTrail mencerna file
- Modifikasi atau penghapusan kedua hal di atas

> **Note**
>
> TheAWS CLIhanya memvalidasi 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 denganAWS CLI, kondisi berikut harus dipenuhi:

- Konektivitas online keAWS.
- Anda harus memiliki akses baca ke bucket Amazon S3 yang berisi biner dan log.
- File intisari dan log tidak boleh dipindahkan dari lokasi Amazon S3 asli di mana CloudTrail mengantarkan mereka.

> **Note**
>
> File log yang telah diunduh ke disk lokal tidak dapat divalidasi denganAWS CLI. Untuk panduan tentang membuat alat Anda sendiri untuk validasi, lihatImplementasi kustom validasi integritas file CloudTrail log.

validasi-log

Sintaksis

Berikut 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 <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> The`validate-logs`perintah khusus Wilayah. Anda harus menentukan`--region`opsi global untuk memvalidasi log untuk log tertentuWilayah AWS.

Opsi

Berikut ini adalah opsi baris perintah untuk`validate-logs`. The`--trail-arn`dan`--start-time`opsi diperlukan. The`--account-id`opsi 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. Untuk informasi selengkapnya, lihat Memeriksa apakah file tertentu telah dikirimkan oleh CloudTrail.

`--s3-bucket`

Secara opsional menentukan bucket Amazon S3 tempat file diger disimpan. Jika nama bucket tidak ditentukan,AWS CLIakan mengambilnya dengan meneleponDescribeTrails().

`--s3-prefix`

Secara opsional menentukan awalan Amazon S3 tempat file intisari disimpan. Jika tidak ditentukan,AWS CLIakan 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 Amazon Resource Name (ARN) dari trail yang akan divalidasi. Format jejak ARN berikut.

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> Untuk mendapatkan jejak ARN untuk jalan setapak, 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`**

The`validate-logs`perintah dimulai dengan memvalidasi file digest 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`, validasi-log akan memverifikasi itu`p1 == df1.digestS3Bucket + '/' + df1.digestS3Object`.

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 intisari berakhir. Jika file intisari hilang atau tidak valid, rentang waktu yang tidak dapat divalidasi ditunjukkan dalam output.

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:

```
<Digest file | Log file> <S3 path> <Validation Message>
```

Tabel berikut menjelaskan pesan validasi untuk file log dan digest.

Jenis File	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 intiser 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.

Jenis File	Pesan Validasi	Deskripsi
`Digest file`	`INVALID: public key not found for fingerprint` *`sidik jari`*	Kunci publik yang sesuai dengan sidik jari yang direkam dalam file intisari tidak ditemukan. File digest tidak dapat divalidasi.
`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` *`sidik jari`*	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 berikut`validate-logs`perintah menggunakan`--verbose`menandai 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://example-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://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-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://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-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://example-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://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-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://example-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://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-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
```

Tidak bertele-tele

Contoh berikut`validate-logs`Perintah 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://example-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

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
```

Memeriksa apakah file tertentu telah dikirimkan oleh CloudTrail

Untuk memeriksa apakah file tertentu di bucket Anda telah dikirimkan oleh CloudTrail, lari`validate-logs`dalam mode verbose untuk periode waktu yang menyertakan file. Jika file muncul di output`validate-logs`, maka file tersebut dikirimkan oleh CloudTrail.

CloudTrail digest struktur berkas

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.

Digest lokasi berkas

File digest dikirim ke lokasi bucket Amazon S3 yang mengikuti sintaks ini.

```
s3://s3-bucket-name/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://s3-bucket-name/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
> ```

Contoh isi file digest

Contoh file digest berikut berisi informasi untuk CloudTrail log.

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "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": "S3-bucket-name",
  "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": "S3-bucket-name",
      "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 digest:

`awsAccountId`

TheAWSID 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 dikirim 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 dikirim 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 digest saat ini dikirim.

`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 saat jejak 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 digest sebelumnya dikirim.

`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 intisari dengan menggunakanAWS CLIatau CloudTrail API. 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 intisari, lihatAWS CLI `list-public-keys`perintah atau CloudTrail `ListPublicKeys`API.

> **Note**
>
> CloudTrail menggunakan pasangan kunci pribadi/publik 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 berkas log.

`logFiles.s3Object`

Kunci objek Amazon S3 dari berkas 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.

Mulai file digest

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 digest yang direkam selama satu jam saat aktivitas API tidak 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": "example-bucket-name",
```

```
  "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": "example-bucket-name",
  "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 digest 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`

Digest file digest

Fakta bahwa setiap file intisari berisi referensi ke file intisari sebelumnya memungkinkan “rantai” yang memungkinkan alat validasi sepertiAWS CLIuntuk 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**
>
> Ketika Anda menonaktifkan validasi integritas berkas log, rantai file digest akan rusak setelah satu jam. CloudTrail tidak akan membuat file digest untuk berkas log yang dikirim selama periode saat validasi integritas berkas 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 saat Anda berhenti CloudTrail log atau hapus jejak.

Jika logging dihentikan atau jejak dihapus, CloudTrail akan mengirimkan file intisari akhir. File intisari ini dapat berisi informasi untuk semua file log yang tersisa yang mencakup peristiwa hingga`StopLogging`acara.

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 menerapkan solusi validasi Anda sendiri. Untuk informasi selengkapnya tentang file digest, lihatCloudTrail digest struktur berkas.

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 Get`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 kunci pribadi/publik 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 menggunakanAWS 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	Penjelasan
`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. Jenis: 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
S3-bucket-name/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.s3Object` 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 adalah agnostik online/offline; 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"));
            }
        }
    }
}
```

Menggunakan CloudTrail Perpustakaan Pengolahan

The CloudTrail Processing Library adalah perpustakaan Java yang menyediakan cara mudah untuk memprosesAWS CloudTraillog. Anda memberikan detail konfigurasi tentang CloudTrail SQS antrian dan menulis kode untuk memproses peristiwa. The CloudTrail Perpustakaan Pemrosesan melakukan sisanya. Ini polling antrian Amazon SQS Anda, membaca dan mem-parsing pesan antrian, download CloudTrail log file, mem-parsing peristiwa dalam file log, dan meneruskan peristiwa ke kode Anda sebagai objek Java.

The CloudTrail Perpustakaan 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 CloudTrail Memproses Perpustakaan untuk diproses CloudTrail log dalam 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 yang dapat Anda gunakan sebagai basis untuk proyek Anda sendiri.

Topik

Persyaratan minimum

Untuk menggunakan CloudTrail Pustaka Pemrosesan, Anda harus memiliki yang berikut:

- AWS SDK for Java1.11.830
- Jawa 1.8 (Jawa SE 8)

Pengolahan CloudTrail log

Untuk memproses CloudTrail log di aplikasi Java Anda:

1. Menambahkan CloudTrail Memproses Perpustakaan untuk proyek Anda
2. Mengkonfigurasi CloudTrail Perpustakaan Pengolahan
3. Menerapkan prosesor acara
4. Membuat instantiasi dan menjalankan pelaksana pemrosesan

Menambahkan CloudTrail Memproses Perpustakaan untuk proyek Anda

Untuk menggunakan CloudTrail Processing Library, tambahkan ke classpath proyek Java Anda.

Daftar Isi

Menambahkan perpustakaan ke proyek Apache Ant

Untuk menambahkan CloudTrail Memproses Perpustakaan ke proyek Apache Ant

1. Unduh atau kloning CloudTrail Memproses kode sumber Perpustakaan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Bangun file.jar dari sumber seperti yang dijelaskan dalamREADME:

```
mvn clean install -Dgpg.skip=true
```

3. Salin file.jar yang dihasilkan ke proyek Anda dan tambahkan ke proyek Andabuild.xmlberkas. Misalnya:

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Menambahkan perpustakaan ke proyek Apache Maven

The CloudTrail Pustaka Pemrosesan tersedia untukApache. Anda dapat menambahkannya ke proyek Anda dengan menulis satu ketergantungan di proyek Andapom.xmlberkas.

Untuk menambahkan CloudTrail Memproses Perpustakaan ke proyek Maven

- Buka proyek Maven Andapom.xmlfile dan menambahkan 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 CloudTrail Memproses Perpustakaan ke proyek Eclipse

1. Unduh atau kloning CloudTrail Memproses kode sumber Perpustakaan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Bangun file.jar dari sumber seperti yang dijelaskan dalamREADME:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. Salin yang dibangun aws-cloudtrail-processing-library-1.6.1.jar ke direktori di proyek Anda (biasanya`lib`).
4. Klik kanan nama proyek Anda di EclipsePenjelajah Proyek, pilihMembangun Jalur, dan kemudian pilihKonfigurasikan
5. DiJalur Bangun Javajendela, pilihPerpustakaantab.
6. PilihTambahkan JAR...dan arahkan ke jalur tempat Anda menyalin aws-cloudtrail-processing-library-1.6.1.jar.
7. PilihOKEuntuk menyelesaikan menambahkan`.jar`ke proyek Anda.

Menambahkan pustaka ke proyek IntelliJ

Untuk menambahkan CloudTrail Memproses Perpustakaan ke proyek IntelliJ

1. Unduh atau kloning CloudTrail Memproses kode sumber Perpustakaan dari GitHub:
   - https://github.com/aws/aws-cloudtrail-processing-library
2. Bangun file.jar dari sumber seperti yang dijelaskan dalamREADME:

   ```
   mvn clean install -Dgpg.skip=true
   ```
3. DariBerkas, pilihStruktur Proyek.
4. PilihModuldan kemudian memilihDependensi.
5. Pilih+ JARS atau Direktoridan kemudian pergi ke jalan di mana Anda membangun`aws-cloudtrail-processing-library-1.6.1.jar`.
6. PilihTerapkandan kemudian memilihOKEuntuk menyelesaikan menambahkan`.jar`ke proyek Anda.

Mengkonfigurasi CloudTrail Perpustakaan Pengolahan

Anda dapat mengonfigurasi CloudTrail Memproses Pustaka 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 berikut diperlukan:

- `sqsUrl`— Menyediakan URL untuk menarik CloudTrailpemberitahuan. Jika Anda tidak menentukan nilai ini,`AWSCloudTrailProcessingExecutor`melempar sebuah`IllegalStateException`.
- `accessKey`— Pengidentifikasi unik untuk akun Anda, seperti AKIAIOSFODNN7EXAMPLE.
- `secretKey`— Pengidentifikasi unik untuk akun Anda, seperti wjalrxutnfemi/K7mDeng/bPxRfiCY EXAMPLEKEY.

The`accessKey`dan`secretKey`parameter memberikan Anda`AWS`kredensyal ke perpustakaan sehingga perpustakaan dapat mengaksesAWSatas nama Anda.

Default untuk parameter lain diatur oleh perpustakaan. Untuk informasi lebih lanjut, lihatAWS CloudTrailReferensi Perpustakaan Pengolahan.

Membuat ClientConfiguration

Alih-alih mengatur opsi di properti classpath, Anda dapat memberikan opsi ke`AWSCloudTrailProcessingExecutor`dengan menginisialisasi dan mengatur 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 CloudTrail data 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 sebuah`EventsProcessor`, Anda menerapkan`process()`panggilan balik yang`AWSCloudTrailProcessingExecutor`digunakan untuk mengirim Anda CloudTrail peristiwa. Acara disediakan dalam daftar`CloudTrailClientEvent`benda.

The`CloudTrailClientEvent`objek menyediakan`CloudTrailEvent`dan`CloudTrailEventMetadata`yang dapat Anda gunakan untuk membaca CloudTrail informasi acara dan pengiriman.

Contoh sederhana ini mencetak informasi acara untuk setiap peristiwa yang diteruskan ke`SampleEventsProcessor`. Dalam implementasi Anda sendiri, Anda dapat memproses log sesuai keinginan Anda. The`AWSCloudTrailProcessingExecutor`terus mengirim acara ke`EventsProcessor`selama ada acara untuk dikirim dan masih berjalan.

Membuat instantiasi dan menjalankan pelaksana pemrosesan

Setelah Anda menulis`EventsProcessor`dan menetapkan nilai konfigurasi untuk CloudTrail Pustaka Pemrosesan (baik dalam file properti atau dengan menggunakan`ClientConfiguration`class), Anda dapat menggunakan elemen-elemen ini untuk menginisialisasi dan menggunakan`AWSCloudTrailProcessingExecutor`.

Untuk menggunakan**`AWSCloudTrailProcessingExecutor`**untuk memproses CloudTrail acara

1. Instantiasi`AWSCloudTrailProcessingExecutor.Builder`objek.`Builder`konstruktor mengambil sebuah`EventsProcessor`objek dan nama file properti classpath.
2. Panggil`Builder`ini`build()`metode pabrik untuk mengkonfigurasi dan mendapatkan`AWSCloudTrailProcessingExecutor`objek.
3. Gunakan`AWSCloudTrailProcessingExecutor`ini`start()`dan`stop()`metode untuk memulai dan mengakhiri CloudTrail pemrosesan 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

Secara default, semua log di bucket S3 antrian Amazon SQS Anda dan semua peristiwa yang dikandungnya dikirim ke Anda`EventsProcessor`. The CloudTrail Pustaka Pemrosesan menyediakan antarmuka opsional yang dapat Anda terapkan untuk memfilter sumber yang digunakan untuk mendapatkan CloudTrail log dan untuk memfilter kejadian 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`CloudTrailSource`objek. Untuk menjaga agar acara dari sumber tidak diproses, kembalikan`false`dari`filterSource()`.

The CloudTrail Perpustakaan Pemrosesan memanggil`filterSource()`metode setelah jajak pendapat pustaka untuk log pada antrian 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 a CloudTrailAcara dikirim ke Anda`EventsProcessor`.`EventFilter`mendeklarasikan metode callback tunggal,`filterEvent()`, yang menerima`CloudTrailEvent`objek. Agar acara tidak diproses, kembalikan`false`dari`filterEvent()`.

The CloudTrail Perpustakaan Pemrosesan memanggil`filterEvent()`metode setelah jajak pendapat pustaka untuk log pada antrian 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 sendiri`EventFilter`, maka`DefaultEventFilter`digunakan, yang memungkinkan semua acara diproses (selalu kembali`true`).

Memproses peristiwa data

Kapan CloudTrail memproses peristiwa data, mempertahankan angka dalam format aslinya, apakah itu bilangan bulat (`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 menjaga 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 CloudTrail peristiwa data, dan memungkinkan keduanya`int`dan`float`nomor yang diformat. Untuk hasil terbaik, gunakan versi 1.4.0 atau yang lebih tinggi CloudTrail Perpustakaan Pemrosesan.

Contoh cuplikan berikut menunjukkan`float`nomor yang diformat,`2.0`, untuk`desiredCount`parameter di`responseParameters`blok dari 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`int`nomor yang diformat,2, untuk`desiredCount`parameter di`ResponseParameters`blok dari 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 CloudTrail Memproses kemajuan Perpustakaan.`ProgressReporter`menyatakan dua metode:`reportStart()`dan`reportEnd()`, yang disebut pada awal dan akhir operasi berikut:

- Pesan polling dari Amazon SQS
- Mengurai pesan dari Amazon SQS
- Memproses sumber Amazon SQS CloudTrail log
- Menghapus pesan dari Amazon SQS
- Mengunduh CloudTrail file log
- Memproses CloudTrail file log

Kedua metode tersebut menerima`ProgressStatus`objek yang berisi informasi tentang operasi yang dilakukan. The`progressState`Anggota memegang anggota`ProgressState`enumerasi yang mengidentifikasi operasi saat ini. Anggota ini dapat memuat informasi tambahan di`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 menerapkan sendiri`ProgressReporter`, maka`DefaultExceptionHandler`, yang mencetak nama status yang sedang dijalankan, digunakan sebagai gantinya.

Menangani kesalahan

The`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 passed-in`ProcessingLibraryException`in`getStatus()`metode untuk mengetahui operasi apa yang dijalankan ketika pengecualian terjadi dan mendapatkan informasi tambahan tentang status operasi.`ProcessingLibraryException`berasal dari standar Java`Exception`kelas, 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`Parameter adalah`true`, CloudTrail Pustaka 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 CloudTrail file log. Karena Anda tidak memiliki izin yang diperlukan,`AmazonServiceException`dilemparkan. The CloudTrail Pustaka Pemrosesan membungkus ini dalam a`CallBackException`.
> 3. The`DefaultExceptionHandler`mencatat ini sebagai kesalahan, tetapi tidak mengidentifikasi akar penyebabnya, yaitu Anda tidak memiliki izin yang diperlukan. The CloudTrail Pustaka Pemrosesan menganggap ini sebagai kesalahan pemrosesan dan menghapus pesan, meskipun pesan tersebut menyertakan pesan yang valid CloudTrail file log.
>
> Jika ingin filter`SourceFilter`, verifikasi bahwa Anda`ExceptionHandler`dapat membedakan pengecualian layanan dari kesalahan pemrosesan.

Sumber daya tambahan

Untuk informasi lebih lanjut tentang CloudTrail Pustaka Pemrosesan, lihat berikut ini:

- CloudTrail Perpustakaan Pengolahan GitHub proyek, yang meliputisampelkode yang menunjukkan bagaimana menerapkan CloudTrail Memproses aplikasi Perpustakaan.
- CloudTrail Memproses Perpustakaan Java Package Dokumentasi.

Pengaturan

Anda dapat menggunakan halaman Pengaturan di CloudTrail konsol untuk mengonfigurasi dan meninjau CloudTrail pengaturan.

Untuk mengakses halaman Pengaturan

1. Masuk ke AWS Management Console 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 organisasiSaat Anda menggunakan CloudTrail dengan AWS Organizations organisasi, Anda dapat menetapkan akun apa pun di dalam organisasi untuk bertindak sebagai administrator yang CloudTrail didelegasikan untuk mengelola jejak organisasi dan penyimpanan data acara atas nama organisasi.
- Saluran terkait layanan— AWS layanan dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWSLayanan yang membuat saluran terkait layanan mengonfigurasi penyeleksi peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semuaWilayah AWS, atau satu saluran. Wilayah AWS

Administrator yang didelegasikan 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 AWS CloudTrail.

> **Note**
>
> Saat Anda menambahkan administrator yang didelegasikan menggunakan operasi AWS Organizations CLI atau API, peran terkait layanan tidak akan dibuat jika tidak ada. Peran terkait layanan hanya dibuat saat Anda melakukan panggilan dari akun manajemen langsung ke CloudTrail layanan, seperti saat Anda menambahkan administrator yang didelegasikan atau membuat jejak organisasi atau penyimpanan data peristiwa menggunakan CloudTrail konsol, AWS CLI atau API. CloudTrail

Perhatikan faktor-faktor berikut yang menentukan cara 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
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
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

Kemampuan	Akun manajemen	Akun administrator yang didelegasikan	Akun anggota
Salin peristiwa jejak ke penyimpanan data acara organisasi.	Ya	Tidak	Tidak
Jalankan kueri pada penyimpanan data acara organisasi.	Ya	Ya	Tidak
Lihat dasbor Danau untuk penyimpanan data acara organisasi.	Ya	Ya	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": "*"
}
```

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 AWS Management Console 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.

   Setelah menambahkan administrator yang didelegasikan, Anda hanya perlu menggunakan akun manajemen organisasi untuk mengubah atau menghapus akun administrator yang didelegasikan.

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 AWS Management Console 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.

Saluran terkait layanan

AWSlayanan dapat membuat saluran terkait layanan untuk menerima CloudTrail acara atas nama Anda. AWSLayanan yang membuat saluran terkait layanan mengonfigurasi penyeleksi peristiwa lanjutan untuk saluran dan menentukan apakah saluran tersebut berlaku untuk semuaWilayah AWS, atau satu saluran. Wilayah AWS

Topik

- Melihat saluran terkait layanan dengan menggunakan konsol
- Melihat saluran terkait layanan dengan menggunakanAWS 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.
- Semua wilayah - Nilainya adalah `Yes` jika saluran dikonfigurasi untuk semuaWilayah AWS.
- AWSlayanan - 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 menggunakanAWS CLI

MenggunakanAWS CLI, Anda dapat melihat informasi tentang apa pun CloudTrail saluran terkait layanan yang dibuat olehAWSlayanan.

Topik

- Dapatkan CloudTrail saluran terkait layanan
- Daftar semua CloudTrail saluran terkait layanan
- AWSacara layanan di saluran terkait layanan

Dapatkan CloudTrail saluran terkait layanan

Berikut ini contoh:AWS CLIperintah mengembalikan informasi tentang tertentu CloudTrail saluran terkait layanan, termasuk nama tujuanAWSlayanan, setiap 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`memewakili namaAWSlayanan yang menciptakan 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 CloudTrail saluran terkait layanan

Berikut ini contoh:AWS CLIperintah mengembalikan informasi tentang semua CloudTrail saluran 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 dari yang Anda tentukan`--max-results`nilai, jalankan perintah lagi menambahkan yang dikembalikan`NextToken`nilai untuk mendapatkan halaman berikutnya dari hasil.

```
aws cloudtrail list-channels
```

Berikut ini adalah contoh respons. Dalam contoh ini,`AWS_service_name`memewakili namaAWSlayanan yang menciptakan saluran.

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWSacara layanan di saluran terkait layanan

TheAWSlayanan yang mengelola saluran terkait layanan dapat memulai tindakan pada saluran terkait layanan (misalnya, membuat atau memperbarui saluran terkait layanan). CloudTrail mencatat tindakan ini sebagaiAWSacara layanan, dan menyampaikan peristiwa ini keRiwayat acara, dan setiap jejak aktif dan penyimpanan data acara yang dikonfigurasi untuk acara manajemen. Untuk acara-acara ini,`eventType`Bidang adalah`AwsServiceEvent`.

Berikut ini adalah contoh entri berkas log dariAWSacara 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"
}
```

Keamanan di AWS CloudTrail

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

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di dalam AWS Cloud. AWS juga memberi layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di AWS CloudTrail, lihat Cakupan Layanan Menurut Program Kepatuhan AWS.
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan CloudTrail. Topik berikut akan membantu Anda cara mengkonfigurasi CloudTrail untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan yang lainAWSmembantu Anda memantau dan mengamankan CloudTrail sumber daya.

Topik

Perlindungan data di AWS CloudTrail

Model tanggung jawab bersama AWS diterapkan untuk perlindungan data AWS CloudTrail. Sebagaimana dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data. Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan CloudTrail atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Secara default, file log CloudTrail peristiwa dienkripsi menggunakan enkripsi sisi server Amazon S3 (SSE). Anda juga dapat memilih untuk mengenkripsi file log Anda 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 dengan AWS KMS kunci (SSE-KMS)
- Kebijakan bucket Amazon S3 untuk CloudTrail
- Memvalidasi CloudTrail integritas berkas 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 Melindungi 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 sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. CloudTrail IAM adalah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara kerja AWS CloudTrail dengan IAM
- Contoh kebijakan berbasis identitas untuk AWS CloudTrail
- AWS CloudTrailcontoh 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 identitas dan akses AWS CloudTrail
- Menggunakan peran terkait layanan untuk AWS CloudTrail
- Kebijakan terkelola AWS untuk AWS CloudTrail

Audiens

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

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

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

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

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda untuk masuk ke AWS menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. Pengguna AWS IAM Identity Center Pengguna (Pusat Identitas IAM), autentikasi Single Sign-On perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas gabungan, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

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

Jika Anda mengakses AWS secara terprogram, AWS memberikan Kit Pengembangan Perangkat Lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang cara menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan API AWS dalam Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS dalam Panduan Pengguna IAM.

Pengguna root Akun AWS

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

Identitas terfederasi

Praktik terbaiknya adalah mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran ini memberikan kredensial sementara.

Untuk pengelolaan akses terpusat, sebaiknya Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apa yang dimaksud Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya andalkan kredensial temporer, dan bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, sebaiknya rotasikan kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan kumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

Peran IAM

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

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas gabungan, Anda dapat membuat peran dan menentukan izin untuk peran tersebut. Saat identitas terfederasi diautentikasi, identitas tersebut dikaitkan dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi sekumpulan izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengaitkan izin yang ditetapkan ke peran dalam IAM. Untuk informasi tentang rangkaian izin, lihat Rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) dengan akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat menyertakan kebijakan secara langsung ke sumber daya (bukan menggunakan peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Contoh, ketika Anda melakukan panggilan dalam layanan, umumnya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Saat menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan

oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

- Peran IAM – Peran layanan adalah peran IAM yang diambil layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran terkait layanan – Peran terkait layanan adalah tipe peran layanan yang terkait dengan Layanan AWS. Layanan tersebut dapat mengambil peran untuk melakukan sebuah tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial sementara untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan API AWS CLI atau AWS. Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan peran AWS ke instans EC2 dan menyediakannya bagi semua aplikasinya, Anda dapat membuat profil instans yang dilampirkan ke instans tersebut. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

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

Mengelola akses menggunakan kebijakan

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, pengguna root, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan

isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses terhadap apa. Artinya, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk operasi. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau API AWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

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

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. 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 yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang

dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Daftar kontrol akses (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Developer Layanan Penyimpanan Ringkas Amazon.

Tipe kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda berdasarkan tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan di mana Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan secara eksplisit terhadap salah satu kebijakan ini akan mengesampingkan izin tersebut. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola beberapa akun Akun AWS yang dimiliki bisnis Anda secara terpusat. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda teruskan sebagai parameter saat Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit di salah satu kebijakan ini akan membatalkan izin tersebut. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Jika beberapa jenis kebijakan diberlakukan untuk satu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan untuk mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

Cara kerja AWS CloudTrail dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses CloudTrail, pelajari fitur IAM yang tersedia untuk digunakan. CloudTrail

Fitur IAM yang dapat Anda gunakan dengan AWS CloudTrail

Fitur IAM	CloudTrail dukungan
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Parsial
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Tidak
ACL	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya

Fitur IAM	CloudTrail dukungan
Sesi akses teruskan (FAS)	Ya
Peran layanan	Ya
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara CloudTrail dan AWS layanan lain bekerja dengan sebagian besar fitur IAM, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk CloudTrail

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan pengguna dan peran, di sumber daya mana, dan dengan ketentuan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta ketentuan terkait jenis tindakan yang diizinkan atau ditolak. Anda tidak dapat menentukan pengguna utama dalam kebijakan berbasis identitas karena kebijakan ini berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat digunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk CloudTrail

Untuk melihat contoh kebijakan CloudTrail berbasis identitas, lihat. Contoh kebijakan berbasis identitas untuk AWS CloudTrail

Kebijakan berbasis sumber daya dalam CloudTrail

Mendukung kebijakan berbasis sumber daya	Parsial

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan tersebut, kebijakan ini menentukan jenis tindakan yang dapat dilakukan oleh pengguna utama tertentu di sumber daya tersebut dan apa ketentuannya. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama lintas akun ke kebijakan berbasis sumber daya bagian dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada di Akun AWS yang berbeda, administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas tersebut. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, kebijakan berbasis identitas lainnya tidak diperlukan. Untuk informasi selengkapnya, lihat Perbedaan peran IAM dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

CloudTrail mendukung kebijakan berbasis sumber daya pada saluran yang digunakan untuk integrasi CloudTrail Lake dengan sumber acara di luar. AWS Kebijakan berbasis sumber daya untuk saluran menentukan entitas utama mana (akun, pengguna, peran, dan pengguna gabungan) yang dapat dipanggil `PutAuditEvents` di 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.

Contoh-contoh

Untuk melihat contoh kebijakan CloudTrail berbasis sumber daya, lihat. AWS CloudTrailcontoh kebijakan berbasis sumber daya

Tindakan kebijakan untuk CloudTrail

Mendukung tindakan kebijakan	Ya

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

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

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

Untuk melihat daftar CloudTrail tindakan, lihat Tindakan yang Ditentukan oleh AWS CloudTrail dalam Referensi Otorisasi Layanan.

Tindakan kebijakan CloudTrail menggunakan awalan berikut sebelum tindakan:

```
cloudtrail
```

Misalnya, untuk memberikan izin kepada seseorang untuk mencantumkan tag untuk jejak dengan operasi `ListTags` API, Anda menyertakan `cloudtrail:ListTags` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. CloudTrail mendefinisikan serangkaian tindakannya sendiri yang menggambarkan 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 JSON AWS untuk menentukan siapa yang memiliki akses ke apa. Yaitu, pengguna utama mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

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

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

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

Untuk melihat daftar jenis CloudTrail sumber daya dan ARNnya, lihat Sumber Daya yang Ditentukan oleh AWS CloudTrail dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang Ditentukan oleh AWS CloudTrail.

Di CloudTrail, ada tiga jenis sumber daya: jalur, penyimpanan data acara, 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 berlaku untuk kebijakan tersebut. CloudTrail Saat ini tidak mendukung jenis sumber daya lain, yang kadang-kadang disebut sebagai subsumber daya.

Sumber daya CloudTrail jejak memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

Sumber daya penyimpanan data CloudTrail acara memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

Sumber daya CloudTrail saluran memiliki ARN berikut:

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

Untuk informasi lebih lanjut tentang format ARN, lihat Amazon Resource Name (ARN) dan Namespace Layanan AWS.

Misalnya, untuk 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 jejak milik akun tertentu di dalamnyaWilayah 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, jadi 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 spesifik layanan	Tidak

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

Elemen `Condition` (atau blok `Condition`) memungkinkan Anda menentukan kondisi di mana suatu pernyataan akan diterapkan. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi kondisional yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam satu pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya dengan menggunakan operasi `AND` logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

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

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

CloudTrail tidak mendefinisikan kunci kondisinya sendiri, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci syarat global AWS, lihat Kunci Konteks Syarat Global AWS dalam Panduan Pengguna IAM.

Untuk melihat daftar kunci CloudTrail kondisi, lihat Condition Keys untuk AWS CloudTrail dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana yang dapat Anda gunakan kunci syarat, lihat Tindakan yang Ditentukan oleh AWS CloudTrail.

ACL di CloudTrail

Mendukung ACL	Tidak

Daftar kontrol akses (ACL) mengontrol pengguna utama (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL sama dengan kebijakan berbasis sumber daya, meskipun tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan CloudTrail

Mendukung ABAC (tanda dalam kebijakan)	Parsial

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Di AWS, atribut ini disebut tag. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tanda ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tanda milik pengguna utama cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna dalam situasi di mana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tanda di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `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 hanya untuk beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial terkait langkah-langkah penyiapan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Meskipun Anda dapat melampirkan tag ke CloudTrail sumber daya, CloudTrail hanya mendukung pengendalian akses ke penyimpanan dan saluran data acara CloudTrail Lake berdasarkan tag. Anda tidak dapat mengontrol akses ke jalur berdasarkan tag.

Anda dapat melampirkan tag ke CloudTrail sumber daya atau meneruskan tag dalam permintaan CloudTrail. Untuk informasi selengkapnya tentang penandaan CloudTrail sumber daya, lihat Membuat jejak danMembuat, memperbarui, dan mengelola jalur dengan AWS Command Line Interface.

Menggunakan kredensyal sementara dengan CloudTrail

Mendukung kredensial sementara	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensial sementara. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial sementara, lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan membuat kredensial sementara secara otomatis saat masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang cara beralih peran, lihat Beralih peran (konsol) di Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan AWS CLI atau AWS API. Anda kemudian dapat menggunakan kredensial sementara untuk mengakses AWS. AWS menyarankan Anda membuat kredensial sementara secara dinamis, alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Teruskan sesi akses untuk CloudTrail

Mendukung sesi akses maju (FAS)	Ya

Jika menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Jika menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian dilanjutkan oleh tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya diajukan saat layanan menerima permintaan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Meneruskan sesi akses.

Peran layanan untuk CloudTrail

Mendukung peran layanan	Ya

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

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak CloudTrail fungsionalitas. Edit peran layanan hanya jika CloudTrail memberikan panduan untuk melakukannya.

Peran terkait layanan untuk CloudTrail

Mendukung peran yang terkait layanan	Ya

Peran yang terkait layanan adalah jenis peran layanan yang terkait dengan Layanan AWS. Layanan ini dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. 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 peran CloudTrail terkait layanan, lihat. Menggunakan peran terkait layanan untuk AWS CloudTrail

Contoh kebijakan berbasis identitas untuk AWS CloudTrail

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi CloudTrail sumber daya. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau API AWS. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat menjalankan peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM dalam 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 dalam Referensi 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 konsol CloudTrail
- Izinkan para pengguna untuk melihat izin mereka sendiri
- Memberikan izin khusus untuk pengguna CloudTrail

Praktik terbaik kebijakan

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

- Mulai menggunakan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Sebaiknya Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di 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 melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.

- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – 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 Analizer Akses IAM di Panduan Pengguna IAM.
- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di 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 Timur AS (Ohio) (Wilayah asalnya) Akun AWS dengan ID *`123456789012`*.

```
{
  "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 bernama My-First-Trail.

```
{
  "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 pada CloudTrail jejak.

Misalnya, Anda tidak ingin pengguna grup pengembang perusahaan Anda memulai atau menghentikan pencatatan pada jejak tertentu. Namun, Anda mungkin ingin memberi mereka izin untuk melakukan `DescribeTrails` dan `GetTrailStatus` tindakan di jalan setapak. Anda ingin pengguna grup pengembang melakukan `StartLogging` atau `StopLogging` tindakan 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 `StartLogging` dan `StopLogging` tindakan untuk jejak ARN yang Anda tentukan. Dalam contoh berikut, jejak ARN adalah. `arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail`

```
{
    "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, `DescribeTrails` dan `GetTrailStatus` tindakan diizinkan pada semua CloudTrail sumber daya:

```
{
    "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 mendapatkan pengecualian yang ditolak akses. Pengguna grup pengembang dapat memulai dan berhenti masuk pada jalur yang mereka buat dan kelola.

Contoh berikut menunjukkan bahwa grup pengembang dikonfigurasi dalam AWS CLI profil bernama`devgroup`. Pertama, pengguna `devgroup` menjalankan `describe-trails` perintah.

```
$ aws --profile devgroup cloudtrail describe-trails
```

Perintah berhasil diselesaikan dengan output berikut:

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "myS3bucket ",
            "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 berhasil diselesaikan 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 di jalur 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 akses ditolak pengecualian, 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 dengan `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 panggung tida`kalpha`,, `betagamma`, atau`prod`.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

Menggunakan konsol CloudTrail

Untuk mengakses konsol AWS CloudTrail tersebut, Anda harus memiliki rangkaian izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang CloudTrail sumber daya di AndaAkun 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 memberikan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. Sebaliknya, izinkan akses hanya ke tindakan yang cocok dengan operasi API yang coba dilakukan.

Pemberian izin untuk administrasi CloudTrail

Untuk mengizinkan peran IAM atau pengguna mengelola CloudTrail sumber daya, seperti jejak, penyimpanan data peristiwa, atau saluran, Anda harus memberikan izin eksplisit untuk melakukan tindakan yang terkait dengan tugas. CloudTrail Dalam kebanyakan situasi, Anda dapat menggunakan kebijakan AWS terkelola yang berisi izin yang telah ditentukan sebelumnya.

> **Note**
>
> Izin yang Anda berikan kepada pengguna untuk melakukan tugas CloudTrail administrasi tidak sama dengan izin yang CloudTrail diperlukan 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, Anda CloudTrail juga memerlukan peran yang dapat diasumsikan untuk mengirimkan peristiwa ke grup CloudWatch log Amazon Logs. Anda harus membuat peran yang CloudTrail menggunakan. Lihat informasi yang lebih lengkap di Memberikan izin untuk melihat dan mengonfigurasi informasi CloudWatch Log Amazon di konsol CloudTrail dan Mengirim acara ke CloudWatch Log.

Kebijakan AWS terkelola berikut tersedia untuk CloudTrail:

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

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

> **Note**
>
> AWSCloudTrail_FullAccessKebijakan ini tidak dimaksudkan untuk dibagikan secara luas di seluruh AndaAkun 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 ke administrator akun. Anda harus mengontrol dan memantau penggunaan kebijakan ini dengan cermat.

- AWSCloudTrail_ReadOnlyAccess— Kebijakan ini memberikan izin untuk melihat CloudTrail konsol, termasuk peristiwa terbaru dan riwayat acara. Kebijakan ini juga memungkinkan Anda untuk melihat jejak 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, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti petunjuk dalam Buat set izin dalam Panduan Pengguna AWS IAM Identity Center.

- Pengguna yang dikelola di IAM melalui penyedia identitas:

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

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di 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 Menyiapkan dengan IAM dan Manajemen akses untuk AWS sumber daya di Panduan Pengguna IAM.

Anda tidak perlu memperbolehkan izin konsol minimum bagi pengguna yang hanya melakukan panggilan ke AWS CLI atau AWS API. Alih-alih, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

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

```
{
    "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 pengguna CloudTrail

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 khusus 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

Akses hanya-baca

Contoh berikut menunjukkan kebijakan yang memberikan akses hanya-baca ke jejak. CloudTrail Ini setara dengan kebijakan yang dikelola AWSCloudTrail_ReadOnlyAccess. Ini memberi pengguna izin untuk melihat informasi jejak, tetapi tidak untuk membuat atau memperbarui jejak.

```
{
    "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 dilakukan pengguna. `Resource`Elemen mencantumkan AWS 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 oleh `cloudtrail:` untuk menunjukkan bahwa mereka merujuk CloudTrail pada 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 hanya-baca tidak memberikan izin pengguna untuk`CreateTrail`,, `UpdateTrail``StartLogging`, dan `StopLogging` tindakan. Pengguna dengan kebijakan ini tidak diizinkan untuk membuat jejak, memperbarui jejak, atau mengaktifkan dan menonaktifkan log. 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 danAWS Lambda, mengelola file di bucket Amazon S3, mengelola CloudWatch cara Log CloudTrail 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 akun AndaAWS. Pengguna dengan peran ini atau akses yang setara memiliki kemampuan untuk menonaktifkan atau mengkonfigurasi ulang fungsi audit yang paling sensitif dan penting di akun merekaAWS. Untuk alasan ini, kebijakan ini harus diterapkan hanya untuk administrator akun, dan penggunaan kebijakan ini harus dikontrol dan dipantau secara ketat.

```
{
    "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:::aws-cloudtrail-logs*"
            ]
        },
        {
            "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 di konsol CloudTrail

Anda dapat melihat informasi peristiwa di CloudTrail konsol, termasuk sumber daya yang terkait dengan peristiwa tersebut. Untuk sumber daya ini, Anda dapat memilih AWS Config ikon untuk melihat garis waktu sumber daya tersebut di AWS Config konsol. Lampirkan kebijakan ini ke pengguna Anda untuk memberi mereka akses hanya-bacaAWS Config. Kebijakan tidak memberi mereka izin untuk mengubah setelanAWS Config.

```
{
```

```
    "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 CloudWatch Log Amazon di konsol CloudTrail

Anda dapat melihat dan mengonfigurasi pengiriman peristiwa ke CloudWatch Log di CloudTrail konsol jika Anda memiliki izin yang memadai. 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 ini tidak memberi mereka izin di dalam CloudTrail atau di CloudWatch Log secara langsung, tetapi memberikan izin yang diperlukan untuk membuat dan mengonfigurasi peran yang CloudTrail akan diambil agar berhasil mengirimkan peristiwa ke grup Log Anda CloudWatch .

```
{
    "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 Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.

Informasi tambahan

Untuk mempelajari lebih lanjut tentang menggunakan IAM untuk memberikan identitas, seperti pengguna dan peran, akses ke sumber daya di akun Anda, lihat Memulai dan Mengelola akses untuk AWS sumber daya di Panduan Pengguna IAM.

AWS CloudTrailcontoh kebijakan berbasis sumber daya

CloudTrail mendukung kebijakan izin berbasis sumber daya untuk CloudTrail saluran yang digunakan untuk integrasi Lake. CloudTrail Untuk informasi selengkapnya tentang membuat integrasi dengan CloudTrail Lake, lihatBuat integrasi dengan sumber acara di luar AWS.

Informasi yang diperlukan untuk kebijakan ditentukan oleh jenis integrasi.

- Untuk integrasi arah, CloudTrail kebijakan harus berisi 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 kebijakan tersebut.
- Untuk integrasi solusi, Anda harus menentukan setidaknya satu Akun AWS ID sebagai prinsipal, dan secara opsional dapat memasukkan ID eksternal untuk mencegah wakil yang bingung.

Berikut ini adalah persyaratan untuk kebijakan berbasis 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.

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:rootarn:aws:iam::444455556666:root`, dan memanggil PutAuditEventsAPI di saluran `arn:aws:iam::123456789012:root` dengan ARN. CloudTrail `arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b`

```
{
    "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 terhadap wakil bingung. Masalah deputi yang bingung adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa 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, seperti frasa sandi atau nomor akun.

Contoh memberikan izin kepada prinsipal dengan ARN `arn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root`, dan memanggil PutAuditEventsAPI pada sumber daya CloudTrail saluran jika panggilan `arn:aws:iam::123456789012:root` ke `PutAuditEvents` API menyertakan nilai ID eksternal yang ditentukan dalam kebijakan.

```
{
    "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": "uniquePartnerExternalID"
                }
            }
```

```
        }
    ]
}
```

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 Command Line Interface.

Untuk mengirimkan file log 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:

- SID yang diizinkan
- 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 trail (atau array trail ARN) yang menggunakan bucket untuk menyimpan log. Pastikan untuk menambahkan kunci `aws:SourceArn` kondisi ke kebijakan bucket S3 untuk jalur yang ada.

Kebijakan berikut memungkinkan CloudTrail untuk menulis file log ke bucket dari yang didukung Wilayah AWS. Ganti *`myBucketName`*, *`[optionalPrefix]/`*, *`myAccountID`*, *`region`*, dan *`trailName`* dengan nilai yang sesuai untuk konfigurasi Anda.

Kebijakan bucket S3

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "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:::myBucketName/[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

- Kesalahan konfigurasi kebijakan Amazon S3 yang umum
- Mengubah awalan untuk bucket yang sudah 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 *myOrganizationBucket*, yang dimiliki oleh akun manajemen organisasi. Ganti *myOrganizationBucket*, *region*, *ManagementAccountID, trailName, dan O-OrganizationId* dengan 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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "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:::myOrganizationBucket/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:::myOrganizationBucket/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.

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 ID CloudTrail akun 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 ARN ID akun 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 *`myBucketName`*, *`[optionalPrefix]/`*, *`myAccountID`*, *`region`*, dan *`trailName`* dengan nilai yang sesuai untuk konfigurasi Anda.

Example Contoh kebijakan bucket dengan nama utama layanan

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
```

```
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "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:::myBucketName/[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 sudah 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 *awalan file log/* sesuai kebutuhan.

```
"Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::myBucketName/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 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 (AWSakun 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:

- SID yang diizinkan
- 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 didukungWilayah AWS. Ganti *myBucketName*, *myAccountID*, dan *myQueryRunningRegion* dengan nilai yang sesuai untuk konfigurasi Anda. *MyAccountID* 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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
```

```
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

Daftar Isi

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 pengiriman 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:

- SID yang diizinkan.
- 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 pemberitahuan SNS.

Kebijakan topik SNS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId: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

```
{
    "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

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 array ARN jejak yang menggunakan 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 Anda menambahkan kunci kondisi ke kebijakan topik SNS Anda, dapatkan nama topik SNS dari pengaturan jejak Anda di CloudTrail konsol.

Kunci `aws:SourceAccount` kondisi juga didukung, tetapi tidak disarankan.

Untuk menambahkan kunci **`aws:SourceArn`** kondisi ke kebijakan topik SNS

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

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 ID CloudTrail akun untuk setiap Wilayah. Kebijakan ini memberikan CloudTrail izin untuk mengirim notifikasi hanya untuk Wilayah yang ditentukan.

Kebijakan topik berikut memungkinkan CloudTrail untuk mengirim pemberitahuan hanya untuk sembilan Wilayah yang ditentukan:

Example kebijakan topik dengan ID akun

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

Kebijakan ini menggunakan izin berdasarkan ID CloudTrail akun individual. Untuk mengirimkan log untuk Wilayah baru, Anda harus memperbarui kebijakan secara manual untuk menyertakan ID CloudTrail akun untuk Wilayah tersebut. Misalnya, karena CloudTrail menambahkan dukungan untuk Wilayah Timur AS (Ohio), Anda harus memperbarui kebijakan untuk menambahkan ID akun ARN untuk Wilayah tersebut:. `"arn:aws:iam::475085895292:root"`

Sebagai praktik terbaik, perbarui kebijakan untuk menggunakan izin dengan kepala CloudTrail layanan. Untuk melakukan ini, ganti ARN ID akun dengan nama utama layanan:`"cloudtrail.amazonaws.com"`.

Ini memberikan CloudTrail izin untuk mengirim pemberitahuan untuk Wilayah saat ini dan yang baru. Berikut ini adalah versi terbaru dari kebijakan sebelumnya:

Example kebijakan topik dengan nama utama layanan

```
{
    "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 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`

Sumber daya tambahan

Untuk informasi selengkapnya tentang topik SNS dan berlangganannya, lihat Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Pemecahan masalah identitas dan akses AWS CloudTrail

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

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

Jika AWS Management Console memberi tahu bahwa Anda tidak diberi otorisasi untuk melakukan tindakan, 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 CloudTrail terkelola yang sesuai (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 IAM atau peran yang memiliki kebijakan AWSCloudTrail_FullAccessterkelola atau izin yang setara, dan Anda tidak dapat mengonfigurasi atau integrasi CloudWatch Log AWS Config Amazon dengan jejak, Anda mungkin kehilangan izin yang diperlukan untuk integrasi dengan layanan tersebut. Lihat informasi yang lebih lengkap di Memberikan izin untuk melihat AWS Config informasi di konsol CloudTrail dan Memberikan izin untuk melihat dan mengonfigurasi informasi CloudWatch Log Amazon di konsol CloudTrail .

Saya tidak berwenang untuk melakukan `iam:PassRole`

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

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

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

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses CloudTrail sumber daya saya

Anda dapat membuat peran dan berbagi CloudTrail informasi di antara beberapaAkun AWS. Untuk informasi selengkapnya, lihat Berbagi file CloudTrail log antar AWS akun.

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna 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 pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah CloudTrail mendukung fitur-fitur ini, lihatCara kerja AWS CloudTrail dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Saya tidak berwenang untuk melakukan **`iam:PassRole`**

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

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

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

Saya mendapatkan **`NoManagementAccountSLRExistsException`** pengecualian ketika saya mencoba membuat jejak organisasi atau penyimpanan data acara

`NoManagementAccountSLRExistsException`Pengecualian dilemparkan ketika akun manajemen tidak memiliki peran terkait layanan. Saat Anda menambahkan administrator yang didelegasikan menggunakan operasi AWS Organizations AWS CLI atau API, peran yang ditautkan layanan tidak akan dibuat jika tidak ada.

Bila Anda menggunakan akun manajemen organisasi untuk menambahkan administrator yang didelegasikan atau membuat jejak organisasi atau penyimpanan data peristiwa di CloudTrail konsol, atau dengan menggunakan AWS CLI atau CloudTrail API, CloudTrail secara otomatis membuat peran terkait layanan untuk akun manajemen Anda jika belum ada.

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 atau. Untuk informasi selengkapnya tentang membuat jejak organisasiMembuat jejak untuk organisasi Anda di konsol, lihatMembuat jejak untuk organisasi dengan AWS Command Line Interface, dan CreateTrail(API).

Menggunakan peran terkait layanan untuk AWS CloudTrail

AWS CloudTrail menggunakan AWS Identity and Access Management (IAM) peran tertaut layanan. Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. CloudTrail Peran terkait layanan telah ditentukan sebelumnya oleh CloudTrail dan menyertakan semua izin yang diperlukan layanan untuk memanggil orang lain Layanan AWS 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, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran tertaut 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 AWSServiceRoleForCloudTrail terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `cloudtrail.amazonaws.com`

Peran ini digunakan untuk mendukung pembuatan dan pengelolaan jalur CloudTrail organisasi dan penyimpanan data acara organisasi CloudTrail Danau di CloudTrail. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi.

CloudTrailServiceRolePolicyKebijakan yang dilampirkan pada peran 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 entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran tertaut layanan. Untuk informasi selengkapnya, silakan lihat Izin Peran Tertaut Layanan di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk CloudTrail

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda membuat jejak organisasi atau penyimpanan data peristiwa organisasi, atau menambahkan administrator yang didelegasikan di CloudTrail konsol, atau dengan menggunakan operasi AWS CLI atau API, akan CloudTrail membuat peran terkait layanan untuk Anda jika belum ada.

Jika Anda menghapus peran terkait layanan ini, dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. Saat Anda membuat jejak organisasi atau penyimpanan data peristiwa organisasi, atau menambahkan administrator yang didelegasikan, CloudTrail buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk CloudTrail

CloudTrail tidak memungkinkan Anda untuk mengedit peran AWSServiceRoleForCloudTrail terkait layanan. Setelah membuat peran tertaut 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, silakan lihat Menyunting peran tertaut layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk CloudTrail

Anda tidak perlu menghapus AWSServiceRoleForCloudTrail peran secara manual. Jika Akun AWS dihapus dari organisasi Organizations, AWSServiceRoleForCloudTrail peran tersebut secara otomatis dihapus dari ituAkun 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 API AWS untuk menghapus secara manual peran yang terhubung dengan layanan. 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.
- Perbarui penyimpanan data acara sehingga tidak lagi menjadi penyimpanan data acara organisasi. Untuk informasi selengkapnya, lihat Memperbarui penyimpanan data acara.
- Hapus jejak. Untuk informasi selengkapnya, lihat Menghapus jejak.
- Hapus penyimpanan data acara. Untuk informasi selengkapnya, lihat Hapus penyimpanan data acara.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForCloudTrail. Untuk informasi selengkapnya, lihat Menghapus peran tertaut 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 lebih lanjut, lihat Layanan AWStitik akhir di. Referensi Umum AWS

Kebijakan terkelola AWS untuk AWS CloudTrail

Menambahkan izin ke para pengguna, grup, dan peran lebih mudah dilakukan dengan menggunakan kebijakan terkelola AWS dibandingkan dengan menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan terkelola pelanggan IAM yang hanya menyediakan izin sesuai kebutuhan tim Anda. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS

terkelola. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di akun Akun AWS Anda. Untuk informasi lebih lanjut tentang kebijakan terkelola AWS, lihat kebijakan terkelola AWS di Panduan Pengguna IAM.

Layanan AWS mempertahankan dan memperbarui kebijakan-kebijakan terkelola AWS. Anda tidak dapat mengubah izin yang ada dalam kebijakan-kebijakan yang dikelola AWS. 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 yang ada di kebijakan yang dikelola AWS, sehingga pembaruan-pembaruan yang terjadi pada kebijakan tidak akan membuat izin yang ada rusak.

Selain itu, AWS mendukung kebijakan-kebijakan terkelola untuk fungsi tugas yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccessAWSterkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin hanya-baca untuk operasi dan sumber daya yang baru. Untuk melihat daftar dan deskripsi dari kebijakan-kebijakan fungsi tugas, lihat kebijakan terkelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Kebijakan terkelola AWS: **`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.

Kebijakan terkelola AWS: **`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.

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	Tanggal
`CloudTrailServiceRolePolicy` — Permbaruan ke kebijakan yang sudah 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` – Permbaruan ke kebijakan yang sudah 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
CloudTrail mulai melacak perubahan	CloudTrail mulai melacak perubahan untuk kebijakan yang AWS dikelola.	6 Juni 2022

Validasi kepatuhan untuk AWS CloudTrail

Auditor pihak ketiga melakukan penilaian pada keamanan dan kepatuhan AWS CloudTrail sebagai bagian dari beberapa program kepatuhan AWS. Ini mencakup SOC, PCI, FedRAMP, HIPAA, dan sebagainya.

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan khusus, lihat Layanan AWS di Scope oleh Program Program Kepatuhan yang Anda minati. Untuk informasi umum, silakan lihat Program Kepatuhan AWS .

Anda bisa 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, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah-langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Merancang Keamanan dan Kepatuhan HIPAA di Amazon Web Services – Laporan resmi ini menjelaskan cara perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

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

- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Panduan Kepatuhan Pelanggan AWS – Pahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan kontrol keamanan di banyak kerangka kerja (termasuk National Institute of Standards and Technology (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).

- Mengevaluasi Sumber Daya dengan Aturan di Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- AWS Security Hub – Layanan AWS ini memberikan pandangan komprehensif tentang status keamanan Anda di dadlam AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda dan untuk memeriksa kepatuhan terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- AWS Audit Manager – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan bagaimana Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

Ketahanan di AWS CloudTrail

Infrastruktur global AWS dibangun di sekitar Wilayah dan Availability Zone AWS. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah dan terisolasi secara fisik, yang terhubung dengan jaringan yang memiliki latensi rendah, throughput tinggi, dan sangat berkelebihan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara Availability Zone tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, menoleransi kegagalan, dan dapat diskalakan dibandingkan satu atau beberapa infrastruktur pusat data tradisional. 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 Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur Global AWS.

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 menerapkan jejak ke semua AWS Wilayah, CloudTrail buat jalur dengan konfigurasi identik di semua partisi lain Wilayah AWS di AWSpartisi tempat Anda bekerja. Saat AWS menambahkan Wilayah baru, konfigurasi jejak itu secara otomatis dibuat di Wilayah baru.

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 dalam AWS CloudTrail

Sebagai layanan yang dikelola,AWS CloudTraildilindungi olehAWSkeamanan jaringan global. Untuk informasi tentangAWSLayanan keamanan dan bagaimanaAWSmelindungi infrastruktur, lihatAWSKeamanan Cloud. Untuk mendesain AndaAWSlingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihatPerlindungan InfrastrukturdiPilar KeamananAWSKerangka Kerja yang Diarsiteksikan dengan Baik.

Anda menggunakanAWSpanggilan API yang dipublikasikan untuk mengakses CloudTrail melalui jaringan. Klien harus mendukung hal-hal berikut:

- Transport Layer Secrecy (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- suite cipher dengan Perfect Forward Secrecy (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Praktik terbaik keamanan berikut juga membahas keamanan infrastruktur di CloudTrail:

- Pertimbangkan titik akhir VPC Amazon untuk akses jejak.
- Pertimbangkan titik akhir VPC Amazon untuk akses bucket Amazon S3. Untuk informasi selengkapnya, lihatContoh Kebijakan ember untuk Titik Akhir VPC untuk Amazon S3.
- Identifikasi dan audit semua bucket Amazon S3 yang berisi CloudTrail file log. Pertimbangkan untuk menggunakan tag untuk membantu mengidentifikasi kedua CloudTrail jalur dan ember Amazon S3 yang berisi CloudTrailfile log. Anda kemudian dapat menggunakan grup sumber daya untuk CloudTrail sumber daya. Untuk informasi selengkapnya, lihat AWS Resource Groups.

Pencegahan Deputi Bingung Lintas Layanan

Masalah deputi yang membingungkan adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. DiAWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (disebut layanan). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini,AWSmenyediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Kami merekomendasikan menggunakan`aws:SourceArn`dan`aws:SourceAccount`kunci konteks kondisi global dalam kebijakan sumber daya untuk membatasi izin yangAWS CloudTrailmemberikan layanan lain ke sumber daya. Gunakan`aws:SourceArn`jika Anda hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan. Gunakan`aws:SourceAccount`jika Anda ingin mengizinkan sumber daya apa pun di akun itu dikaitkan dengan penggunaan lintas layanan.

Cara paling efektif untuk melindungi dari masalah wakil yang membingungkan adalah dengan menggunakan`aws:SourceArn`kunci konteks kondisi global dengan ARN penuh sumber daya. Jika Anda tidak mengetahui ARN lengkap sumber daya atau jika Anda menentukan beberapa sumber daya, gunakan`aws:SourceArn`kunci kondisi konteks global dengan wildcard (`*`) untuk bagian ARN yang tidak diketahui. Sebagai contoh, `"arn:aws:cloudtrail:*:`*AccountID*`:trail/*"`. Ketika Anda menyertakan wildcard, Anda juga harus menggunakan wildcard, Anda juga harus menggunakan wildcard, Anda juga harus menggunakan.`StringLike`operator kondisi.

Nilai dari`aws:SourceArn`harus ARN dari jejak, penyimpanan data acara, atau saluran yang menggunakan sumber daya.

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan`aws:SourceArn`dan`aws:SourceAccount`kunci konteks kondisi global di 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

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.

Terapkan jalur ke semua Wilayah AWS

Untuk mendapatkan catatan lengkap peristiwa yang diambil oleh identitas IAM, atau layanan di AWS akun Anda, setiap jejak harus dikonfigurasi untuk mencatat peristiwa di semua Wilayah AWS. Dengan mencatat peristiwa di semua Wilayah AWS, Anda memastikan bahwa semua peristiwa yang terjadi di AWS akun Anda dicatat, terlepas dari AWS Wilayah mana peristiwa itu terjadi. Ini termasuk mencatat peristiwa layanan global, yang dicatat ke AWS Wilayah khusus untuk layanan tersebut. Saat Anda membuat jejak yang berlaku untuk semua Wilayah, CloudTrail merekam peristiwa di setiap Wilayah dan mengirimkan file log CloudTrail peristiwa ke bucket S3 yang Anda tentukan. Jika

AWS Wilayah ditambahkan setelah Anda membuat jejak yang berlaku untuk semua Wilayah, Wilayah baru tersebut secara otomatis disertakan, dan peristiwa di Wilayah tersebut dicatat. Ini adalah opsi default saat Anda membuat jejak di CloudTrail konsol.

Berikut ini adalah beberapa langkah yang dapat Anda ambil:

- Buat jejak untuk AWS akun Anda.
- Perbarui jejak yang ada untuk mencatat peristiwa di semua Wilayah AWS.
- 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 dan/atau peristiwa data) yang ingin Anda pantau.

Misalnya, Anda dapat memantau keamanan kunci dan peristiwa manajemen terkait jaringan, seperti peristiwa login yang gagal AWS Management Console.

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 AWS Security Hub

Pantau penggunaan Anda CloudTrail karena berkaitan dengan praktik terbaik keamanan dengan menggunakan AWS Security Hub. Security Hub menggunakan kontrol keamanan detektif untuk mengevaluasi konfigurasi sumber daya dan standar keamanan guna membantu Anda mematuhi berbagai kerangka kerja kepatuhan. Untuk informasi selengkapnya tentang penggunaan Security Hub guna mengevaluasi CloudTrail sumber daya, lihat AWS CloudTrail kontrol di Panduan AWS Security Hub 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 Anda untuk secara khusus mengizinkan enkripsi AES256, seperti yang ditunjukkan pada contoh baris kebijakan berikut.
>
> ```
> "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 keamanan terbaik, sebaiknya tambahkan kunci kondisi `aws:SourceArn` (atau opsional`aws:SourceAccount`) ke pernyataan CloudTrail kebijakan. 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 Command Line Interface
- 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 dengan AWS KMS kunci (SSE-KMS)

Secara default, file log yang dikirimkan CloudTrail ke bucket Anda dienkripsi dengan menggunakan enkripsi sisi server dengan kunci KMS (SSE-KMS). Jika Anda tidak mengaktifkan enkripsi SSE-KMS, log Anda dienkripsi menggunakan enkripsi SSE-S3.

> **Note**
>
> Mengaktifkan enkripsi sisi server mengenkripsi file log tetapi bukan file digest dengan SSE-KMS. File Digest dienkripsi dengan kunci enkripsi yang dikelola Amazon S3 (SSE-S3). 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 kunci KMS, juga dikenal sebagai kunci. AWS KMS key Anda melampirkan kebijakan ke kunci yang menentukan pengguna mana yang dapat menggunakan kunci untuk mengenkripsi dan mendekripsi CloudTrail file log. Dekripsi mulus melalui S3. Ketika pengguna resmi dari kunci membaca file CloudTrail log, S3 mengelola dekripsi, dan pengguna yang berwenang dapat membaca file log dalam bentuk yang tidak terenkripsi.

Pendekatan ini memiliki keuntungan sebagai berikut:

- Anda dapat membuat dan mengelola kunci enkripsi kunci KMS sendiri.
- Anda dapat menggunakan satu kunci KMS untuk mengenkripsi dan mendekripsi file log untuk beberapa akun di semua Wilayah.
- Anda memiliki kendali atas siapa yang dapat menggunakan kunci Anda untuk mengenkripsi dan mendekripsi CloudTrail file log. 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, izin berikut diperlukan:
  - Pengguna harus memiliki izin baca S3 untuk bucket yang berisi file log.
  - Pengguna juga harus memiliki kebijakan atau peran yang diterapkan yang memungkinkan izin dekripsi oleh kebijakan kunci KMS.
- Karena S3 secara otomatis mendekripsi file log untuk permintaan dari pengguna yang berwenang untuk menggunakan kunci KMS, enkripsi SSE-KMS untuk file CloudTrail log 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 Anda. Misalnya, jika file log 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.

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 AWS Management Console, 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 Region yang sama dengan bucket S3 yang menerima file log 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.

- Untuk informasi tentang apa yang harus disertakan dalam kebijakan, lihatKonfigurasikanAWS KMSkebijakan utama untuk CloudTrail.

  > **Warning**
  >
  > Pastikan untuk menyertakan izin dekripsi dalam kebijakan untuk semua pengguna yang perlu membaca file log. 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 jejak Anda untuk menggunakan kunci KMS yang kebijakannya Anda modifikasi. CloudTrail

   - Untuk memperbarui konfigurasi jejak Anda menggunakan CloudTrail konsol, lihatMemperbarui sumber daya untuk menggunakan kunci KMS Anda.
   - Untuk memperbarui konfigurasi jejak Anda dengan menggunakan AWS CLI, lihatMengaktifkan dan menonaktifkan CloudTrail enkripsi file log denganAWS 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 membuatAWS KMS keydenganAWSKeyManagementServicePowerUserkebijakan.

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. PilihIzin, dan kemudian pilihLampirkan Kebijakan.
4. CariAWSKeyManagementServicePowerUser, pilih kebijakan, dan kemudian pilihLampirkan kebijakan.

   Pengguna sekarang memiliki izin untuk membuat kunci KMS. Jika Anda ingin membuat kebijakan khusus untuk pengguna Anda, lihatMembuat Kebijakan yang Dikelola oleh PelanggandiPanduan Pengguna IAM.

KonfigurasikanAWS KMSkebijakan utama untuk CloudTrail

Anda dapat membuatAWS KMS keydalam tiga cara:

- The CloudTrail konsol
- TheAWSKonsol manajemen
- TheAWS CLI

> **Note**
>
> Jika Anda membuat kunci KMS di CloudTrail konsol, CloudTrail menambahkan kebijakan kunci KMS yang diperlukan untuk Anda. Ketika Anda tidak perlu menambahkan pernyataan kebijakan tersebut. Lihat Kebijakan kunci KMS default dibuat dalam CloudTrail konsol.

Jika Anda membuat kunci KMS diAWSManajemen atauAWS CLI, Anda harus menambahkan bagian kebijakan ke kunci sehingga Anda dapat menggunakannya dengan CloudTrail. Kebijakan tersebut harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log dan penyimpanan data peristiwa, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk yang tidak terenkripsi.

Lihat sumber daya berikut:

- Untuk membuat kunci KMS denganAWS CLI, lihatbuat-kunci.
- Untuk mengedit kebijakan kunci KMS untuk CloudTrail, lihatMengedit kebijakan kuncidiAWS Key Management ServicePanduan Pengembang.

- Untuk detail teknis tentang caranya CloudTrail menggunakanAWS KMS, lihatBagaimanaAWS CloudTrailMenggunakanAWS KMSdiAWS Key Management ServicePanduan Pengembang.

Bagian kebijakan kunci KMS yang diperlukan untuk digunakan CloudTrail

Jika Anda membuat kunci KMS denganAWSKonsol manajemen atauAWS CLI, maka Anda harus, setidaknya, menambahkan pernyataan berikut ke kebijakan kunci KMS Anda agar dapat bekerja dengannya CloudTrail.

Topik

- Elemen kebijakan kunci KMS yang diperlukan untuk jalur
- Diperlukan elemen kebijakan kunci KMS untuk penyimpanan data acara

Elemen kebijakan kunci KMS yang diperlukan untuk jalur

1. Aktifkan CloudTrail izin log enkripsi. Lihat Memberikan izin enkripsi.
2. Aktifkan CloudTrail izin dekripsi log. Lihat Memberikan izin dekripsi. Ketika Anda menggunakan ember S3 yang ada dengan Kunci Ember S3, `kms:Decrypt` izin diperlukan untuk membuat atau memperbarui jejak dengan enkripsi SSE-KMS diaktifkan.
3. Aktifkan CloudTrail untuk menggambarkan properti kunci KMS. Lihat Aktifkan CloudTrail untuk menggambarkan properti kunci KMS.

Sebagai praktik keamanan terbaik, tambahkan `aws:SourceArn` kunci kondisi kebijakan kunci KMS. Kunci kondisi global IAM `aws:SourceArn` membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu. Nilai dari `aws:SourceArn` selalu merupakan jejak ARN (atau array trail ARN) yang menggunakan kunci KMS. Ketika Anda menambahkan `aws:SourceArn` kunci kondisi untuk kebijakan kunci KMS untuk jalur yang ada.

The `aws:SourceAccount` kunci kondisi juga didukung, tetapi tidak disarankan. Nilai dari `aws:SourceAccount` adalah ID akun pemilik jejak, atau untuk jalur organisasi, ID akun manajemen.

> **Important**
>
> Ketika Anda menambahkan bagian baru ke kebijakan kunci KMS Anda, jangan mengubah bagian apa pun yang ada dalam kebijakan tersebut.

Jika enkripsi diaktifkan pada jejak, dan kunci KMS dinonaktifkan, atau kebijakan kunci KMS tidak dikonfigurasi dengan benar CloudTrail, CloudTrail tidak dapat mengirimkan log.

Diperlukan elemen kebijakan kunci KMS untuk penyimpanan data acara

1. Aktifkan CloudTrail izin log enkripsi. Lihat Memberikan izin enkripsi.
2. Aktifkan CloudTrail izin dekripsi log. Lihat Memberikan izin dekripsi.
3. Berikan izin kepada pengguna dan peran untuk mengenkripsi dan mendekripsi data penyimpanan data peristiwa dengan kunci KMS.

   Saat Anda membuat penyimpanan data acara dan mengenkripsi dengan kunci KMS, atau menjalankan kueri pada penyimpanan data acara 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 dapat dikelola oleh pengguna yang menjalankan operasi (seperti kueri) di penyimpanan data acara.
4. Aktifkan CloudTrail untuk menggambarkan properti kunci KMS. Lihat Aktifkan CloudTrail untuk menggambarkan properti kunci KMS.

The`aws:SourceArn`dan`aws:SourceAccount`kunci kondisi tidak didukung dalam kebijakan kunci KMS untuk penyimpanan data peristiwa.

Important

Ketika Anda menambahkan bagian baru ke kebijakan kunci KMS Anda, jangan mengubah bagian apa pun yang ada dalam kebijakan tersebut.
Jika enkripsi diaktifkan pada penyimpanan data peristiwa, dan kunci KMS dinonaktifkan atau dihapus, atau kebijakan kunci KMS tidak dikonfigurasi dengan benar CloudTrail, CloudTrailtidak dapat mengirimkan acara ke penyimpanan data acara Anda.

Memberikan izin enkripsi

Example Izinkan CloudTrail untuk mengenkripsi log atas nama akun tertentu

CloudTrail memerlukan izin eksplisit untuk menggunakan kunci KMS untuk mengenkripsi log atas nama akun tertentu. Untuk menentukan akun, tambahkan pernyataan wajib berikut ke kebijakan

kunci KMS Anda dan ganti*akun-id*,*daerah*, dan*Nama jejak*dengan nilai yang sesuai untuk konfigurasi Anda. Anda dapat menambahkan ID akun tambahan ke`EncryptionContext`bagian untuk mengaktifkan akun-akun tersebut untuk digunakan CloudTrail untuk menggunakan kunci KMS Anda untuk mengenkripsi file log.

Sebagai praktik keamanan terbaik, tambahkan`aws:SourceArn`kunci kondisi kebijakan kunci KMS untuk jejak tersebut. Kunci kondisi global IAM`aws:SourceArn`membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu.

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "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/*"
         }
    }
}
```

Kebijakan untuk kunci KMS yang digunakan untuk mengenkripsi CloudTrail
Log penyimpanan data peristiwa danau tidak dapat menggunakan kunci kondisi`aws:SourceArn`atau`aws:SourceAccount`. Berikut ini adalah contoh kebijakan kunci KMS untuk penyimpanan data peristiwa.

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
```

```
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

Contoh pernyataan kebijakan berikut menggambarkan bagaimana akun lain dapat menggunakan kunci KMS Anda untuk mengenkripsi CloudTrail log.

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 mengenkripsi dengan kunci Anda ke CloudTrail EncryptionContext. Hal ini membatasi CloudTrail untuk menggunakan kunci Anda untuk mengenkripsi log hanya untuk akun yang Anda tentukan. Saat Anda memberikan root akun*222222222222*izin untuk mengenkripsi log, itu mendelegasikan izin ke administrator akun untuk mengenkripsi izin yang diperlukan untuk pengguna lain di akun itu. Administrator akun melakukan ini dengan mengubah kebijakan yang terkait dengan pengguna IAM tersebut.

Sebagai praktik keamanan terbaik, tambahkan`aws:SourceArn`kunci kondisi kebijakan kunci KMS. Kunci kondisi global IAM`aws:SourceArn`membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur yang ditentukan. Kondisi ini tidak didukung dalam kebijakan kunci KMS untuk penyimpanan data peristiwa.

Pernyataan kebijakan kunci KMS:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "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 lebih lanjut tentang mengedit kebijakan kunci KMS untuk digunakan dengan CloudTrail, lihatMengedit kebijakan utamadiAWS Key Management ServicePanduan Pengembang.

Memberikan izin dekripsi

Sebelum Anda 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 dekripsi tidak dapat membaca log terenkripsi. Ketika Anda menggunakan ember S3 yang ada dengan Kunci Ember S3,`kms:Decrypt`izin diperlukan untuk membuat atau memperbarui jejak dengan enkripsi SSE-KMS diaktifkan.

Aktifkan CloudTrail izin dekripsi log

Pengguna kunci Anda harus diberikan 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, ubah`Principal`bagian untuk menambahkan baris untuk setiap prinsipal yang ingin Anda dekripsi dengan menggunakan kunci KMS Anda.

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "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 kebijakan contoh yang diperlukan untuk mengizinkan kebijakan tersebut. CloudTrail kepala layanan untuk mendekripsi log jejak.

```
{
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

Kebijakan dekripsi untuk kunci KMS yang digunakan dengan CloudTrail Penyimpanan data acara danau mirip dengan yang berikut ini. ARN pengguna atau peran ditentukan sebagai nilai untuk`Principal`perlu mendekripsi izin untuk membuat atau memperbarui penyimpanan data acara, menjalankan kueri, atau mendapatkan hasil kueri.

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

Berikut ini adalah kebijakan contoh yang diperlukan untuk mengizinkan kebijakan tersebut. CloudTrail prinsip layanan untuk mendekripsi log penyimpanan data peristiwa.

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "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, ember S3, dan pengguna IAM Bob ada di akun*111111111111*.
- Anda memberikan izin Bob pengguna IAM untuk mendekripsi CloudTrail log dalam ember S3.

Dalam kebijakan utama, Anda mengaktifkan CloudTrail log dekripsi izin untuk pengguna IAM Bob.

Pernyataan kebijakan kunci KMS:

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "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, tetapi bukan log penyimpanan data peristiwa. Perubahan yang diperlukan pada kebijakan utama 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 IAM atau peran di akun lain untuk 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 S3 bucket ada di akun*222222222222*.

Ketika itu, 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 kunci KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Pernyataan kebijakan pengguna IAM Alice:

```
{
  "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 ember S3 Anda ada dalam akun Anda*111111111111*.
- Pengguna yang membaca log dari bucket Anda ada di akun*222222222222*.

Untuk mengaktifkan skenario ini, Anda mengaktifkan izin dekripsi untuk peran IAMCloudTrailReadRoledi akun Anda, dan kemudian berikan izin akun lain untuk mengambil peran itu.

Pernyataan kebijakan kunci KMS:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111: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:

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

```
   {
     "Sid": "Allow CloudTrail access",
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::222222222222:root"
     },
     "Action": "sts:AssumeRole"
    }
  ]
 }
```

Untuk informasi tentang mengedit kebijakan kunci KMS untuk digunakan dengan CloudTrail, lihatMengedit kebijakan kuncidiAWS Key Management ServicePanduan Pengembang.

Aktifkan CloudTrail untuk menggambarkan properti kunci KMS

CloudTrail membutuhkan kemampuan untuk menggambarkan sifat-sifat kunci KMS. Untuk mengaktifkan fungsi ini, tambahkan pernyataan wajib berikut sebagaimana adanya ke kebijakan kunci KMS Anda. Pernyataan ini tidak memberikan CloudTrail izin apa pun di luar izin lain yang Anda tentukan.

Sebagai praktik keamanan terbaik, tambahkan`aws:SourceArn`kunci kondisi kebijakan kunci KMS. Kunci kondisi global IAM`aws:SourceArn`membantu memastikan bahwa CloudTrail menggunakan kunci KMS hanya untuk jalur atau jalur tertentu.

```
{
  "Sid": "Allow CloudTrail access",
  "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, lihatMengedit kebijakan kuncidiAWS Key Management ServicePanduan Pengembang.

Kebijakan kunci KMS default dibuat dalam CloudTrail konsol

Ketika Anda membuat sebuahAWS KMS keydi CloudTrail konsol, kebijakan berikut secara otomatis dibuat untuk Anda. Kebijakan ini mengizinkan izin ini:

- MemungkinkanAkun AWS(root) izin untuk kunci KMS.
- Memungkinkan CloudTrail untuk mengenkripsi file log di bawah kunci KMS dan menjelaskan kunci KMS.
- Memungkinkan semua pengguna di akun yang ditentukan untuk mendekripsi file log.
- 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 standar untuk CloudTrail Toko data acara danau
- Kebijakan kunci KMS standar untuk jalur

Kebijakan kunci KMS standar untuk CloudTrail Toko data acara danau

Berikut ini adalah kebijakan default yang dibuat untukAWS KMS keyyang Anda gunakan dengan penyimpanan data acara di CloudTrail Danau.

```
{
      "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::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

Kebijakan kunci KMS standar untuk jalur

Berikut ini adalah kebijakan default yang dibuat untukAWS KMS keyyang Anda gunakan dengan jejak.

> **Note**
>
> Kebijakan tersebut mencakup pernyataan untuk mengizinkan lintas akun mendekripsi file log dengan kunci KMS.

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id: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:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id: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": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
```

```
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

Memperbarui sumber daya untuk menggunakan kunci KMS Anda

DiAWS CloudTrailkonsol, memperbarui jejak atau penyimpanan data acara untuk menggunakanAWS Key Management Servicekunci. Sadarilah bahwa menggunakan kunci KMS Anda sendiri adaAWS KMSbiaya untuk enkripsi dan dekripsi. Untuk informasi selengkapnya, lihat AWS Key Management Service Harga.

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 menggunakanAWS KMS keyyang Anda modifikasi untuk CloudTrail, selesaikan langkah-langkah berikut di CloudTrail konsol.

> **Note**
>
> Memperbarui jejak dengan prosedur berikut mengenkripsi file log tetapi bukan file intisari dengan SSE-KMS. File Digest dienkripsi dengan Kunci enkripsi yang dikelola Amazon S3 (SSE-S3).
> Jika Anda menggunakan bucket S3 yang ada dengan bucket Kunci bucket S3, CloudTrail harus diizinkan izin dalam kebijakan kunci untuk menggunakanAWS KMStindakan `GenerateDataKey` dan `DescribeKey`. Jika `cloudtrail.amazonaws.com` tidak diberikan izin tersebut dalam kebijakan utama, Anda tidak dapat membuat atau memperbarui jejak.

Untuk memperbarui jejak menggunakanAWS CLI, lihatMengaktifkan dan menonaktifkan CloudTrail enkripsi file log denganAWS CLI.

Untuk memperbarui jejak untuk menggunakan kunci KMS Anda

1. Masuk keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. PilihJalan setapakdan kemudian pilih nama jejak.
3. DiRincian umum, pilihSunting.
4. UntukFile log enkripsi SSE-KMS, pilihDiaktifkanjika Anda ingin mengenkripsi file log Anda menggunakan enkripsi SSE-KMS alih-alih enkripsi SSE-S3. Defaultnya adalahDiaktifkan. Jika Anda tidak mengaktifkan enkripsi SSE-KMS, log Anda dienkripsi menggunakan enkripsi SSE-S3. Untuk informasi lebih lanjut tentang enkripsi SSE-KMS, lihatMenggunakan enkripsi sisi server denganAWS Key Management Service(SSE-KMS). Untuk informasi lebih lanjut tentang enkripsi SSE-S3, lihatMenggunakan Kunci Enkripsi Sisi Server dengan Kunci Enkripsi Terkelola Amazon S3 (SSE-S3).

   Pilihyang adauntuk memperbarui jejak Anda denganAWS KMS key. Pilih kunci KMS yang ada di Wilayah yang sama dengan bucket S3 yang ada di bucket S3 yang Anda tentukan. 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. Kebijakan utama harus memungkinkan CloudTrail untuk menggunakan kunci untuk mengenkripsi file log Anda, dan memungkinkan pengguna yang Anda tentukan untuk membaca file log dalam bentuk yang tidak terenkripsi. Untuk informasi tentang mengedit kebijakan kunci secara manual, lihatKonfigurasikanAWS KMSkebijakan utama untuk CloudTrail.

   DiAWS KMSAlias, 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.

   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 ada di antara format berikut:

- Nama Alias:`alias/MyAliasName`
- Alias ARN:`arn:aws:kms:region:123456789012:alias/MyAliasName`
- Kunci ARN:`arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-12345678901`
- ID kunci unik secara global:`12345678-1234-1234-1234-123456789012`

5. PilihPerbarui 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, lihatKunci utama: Efek pada kunci KMS AndadiAWS Key Management ServicePanduan Pengembang.

Memperbarui penyimpanan data acara untuk menggunakan kunci KMS

Untuk memperbarui toko data acara untuk menggunakanAWS KMS keyyang Anda modifikasi untuk CloudTrail, selesaikan langkah-langkah berikut di CloudTrail konsol.

Untuk memperbarui penyimpanan data acara dengan menggunakanAWS CLI, lihatPerbarui penyimpanan data acara dengan AWS CLI.

> **Important**
>
> Menonaktifkan atau menghapus kunci KMS, atau menghapus CloudTrail izin pada kunci, mencegah CloudTrail dari menelan peristiwa ke penyimpanan data peristiwa, dan mencegah pengguna melakukan kueri data di penyimpanan data acara 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 keAWS Management Consoledan buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. Di panel navigasi, pilihPenyimpanan data acaradiDanau. Pilih penyimpanan data acara untuk diperbarui.
3. DiRincian umum, pilihSunting.
4. UntukEnkripsi, jika belum diaktifkan, pilihGunakan saya sendiriAWS KMS keyuntuk mengenkripsi file log Anda dengan kunci KMS Anda sendiri.

   Pilihyang adauntuk memperbarui penyimpanan data acara Anda dengan kunci KMS Anda. Pilih kunci KMS yang ada di Wilayah yang sama dengan toko data acara. Kunci dari akun lain tidak didukung.

   DiMasukAWS KMSAlias, tentukan alias yang Anda ubah kebijakan untuk digunakan CloudTrail, dalam formatalias/*MyAliasName*. Untuk informasi selengkapnya, lihat Memperbarui sumber daya untuk menggunakan kunci KMS Anda.

   Anda dapat memilih alias, atau menggunakan ID kunci yang unik secara global. Nilai dapat ada di antara format berikut:

   - Nama Alias:`alias/`*`MyAliasName`*
   - Alias ARN:`arn:aws:kms:`*`region`*`:123456789012:alias/`*`MyAliasName`*
   - Kunci ARN:`arn:aws:kms:`*`region`*`:123456789012:key/12345678-1234-1234-1234-12345678901`
   - ID kunci unik secara global:`12345678-1234-1234-1234-123456789012`
5. Pilih Save changes (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, lihatKunci utama: Efek pada kunci KMS AndadiAWS Key Management ServicePanduan Pengembang.

Mengaktifkan dan menonaktifkan CloudTrail enkripsi file log denganAWS CLI

Topik ini menjelaskan cara mengaktifkan dan menonaktifkan enkripsi file log SSE-. CloudTrail dengan menggunakanAWS CLI. Untuk informasi latar belakang, lihat Mengenkripsi file CloudTrail log dengan AWS KMS kunci (SSE-KMS).

Topik

Mengaktifkan CloudTrail enkripsi file log dengan menggunakanAWS CLI

Aktifkan enkripsi file log untuk jejak

1. Buat kunci denganAWS CLI. Kunci yang Anda buat harus berada di Wilayah yang sama dengan bucket S3. CloudTrail file log. Untuk langkah ini, Anda menggunakanAWS KMS create-keyperintah.
2. Dapatkan kebijakan kunci yang ada sehingga Anda dapat memodifikasinya untuk digunakan CloudTrail. Anda dapat mengambil kebijakan kunci denganAWS KMS get-key-policyperintah.
3. Tambahkan bagian yang diperlukan ke kebijakan kunci. CloudTrail dapat mengenkripsi dan pengguna dapat mendekripsi file log Anda. 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, lihatKonfigurasikanAWS KMSkebijakan utama untuk CloudTrail.
4. Lampirkan file kebijakan JSON yang dimodifikasi ke kunci dengan menggunakanAWS KMS put-key-policyperintah.
5. Jalankan CloudTrail `create-trail`atau`update-trail`perintah dengan`--kms-key-id`parameter. Perintah ini memungkinkan enkripsi log.

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

The `--kms-key-id` parameter menentukan kunci yang kebijakannya Anda dimodifikasi 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 contoh responsnya:

```
{
    "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": "my-bucket-name"
}
```

Kehadiran `KmsKeyId` elemen menunjukkan bahwa enkripsi file log telah diaktifkan. File log terenkripsi akan muncul di bucket Anda dalam waktu sekitar 5 menit.

Aktifkan enkripsi file log untuk penyimpanan data acara

1. Buat kunci dengan AWS CLI. Kunci yang Anda buat harus berada di Wilayah yang sama dengan data. Untuk langkah ini, jalankan AWS KMS create-key perintah.
2. Dapatkan kebijakan kunci yang ada untuk diedit untuk digunakan CloudTrail. Anda bisa mendapatkan kebijakan kunci dengan menjalankan AWS KMS get-key-policy perintah.
3. Tambahkan bagian yang diperlukan ke kebijakan kunci. CloudTrail dapat mengenkripsi dan pengguna dapat mendekripsi file log Anda. 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, lihat Konfigurasikan AWS KMS kebijakan utama untuk CloudTrail.

4. Lampirkan file kebijakan JSON yang telah diedit ke kunci dengan menjalankanAWS KMS put-key-policyperintah.
5. Jalankan CloudTrail `create-event-data-store`atau`update-event-data-store`perintah, dan tambahkan`--kms-key-id`parameter. Perintah ini memungkinkan enkripsi log.

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

The`--kms-key-id`parameter menentukan kunci yang kebijakannya Anda dimodifikasi CloudTrail. Ini bisa menjadi 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 contoh responsnya:

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

KehadiranKmsKeyIdelemen menunjukkan bahwa enkripsi file log telah diaktifkan. File log terenkripsi akan muncul di penyimpanan data acara Anda dalam waktu sekitar 5 menit.

Menonaktifkan CloudTrail enkripsi file log dengan menggunakanAWS CLI

Untuk berhenti mengenkripsi log di jalan setapak, jalankanupdate-traildan berikan string kosong kekms-key-idParameter:

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

Berikut contoh responsnya:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

Tidak adanyaKmsKeyIdnilai menunjukkan bahwa enkripsi file log tidak lagi diaktifkan.

> **Important**
>
> Anda tidak dapat menghentikan enkripsi file log pada penyimpanan data peristiwa.

CloudTrail referensi acara log

CloudTrail Log adalah catatan dalam format 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.

Contoh berikut menunjukkan catatan log tunggal dari suatu peristiwa. 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 bernama`myTrail`.


```
{
    "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"
}
```


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, lihat[CloudTrail Wawasan`insightDetails`elemen](#).


```
{
        "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"
}
```

Topik berikut mencantumkan bidang data yang CloudTrail menangkap untuk setiap panggilan AWS API dan peristiwa login.

Topik

CloudTrail isi rekaman

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).

CloudTrail memotong bidang jika isi bidang melebihi ukuran bidang maksimum. Jika bidang terpotong, `omitted` hadir dengan nilai. `true`

`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 1.10.

`eventVersion`Nilainya adalah versi mayor dan minor dalam bentuk *`major_version`*. *`minor_version`*. Misalnya, Anda dapat memiliki `eventVersion` nilai`1.09`, di mana `1` adalah versi utama, dan `09` 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. 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 greater-than-or-equal -to pada versi minor. Tidak ada angka nol terkemuka dalam versi minor. Anda dapat menafsirkan *`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`. Sebagai contoh:

- AWS 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 biasanya`AWS Internal/#`, di mana `#` adalah nomor yang digunakan untuk tujuan internal.

Sejak: 1.0

Opsional: Salah

`userAgent`

Agen melalui mana permintaan dibuat, seperti AWS Management Console, AWS layanan, AWS SDK atau. AWS CLI Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong. Berikut ini adalah contoh nilai:

- `lambda.amazonaws.com`Permintaan itu dibuat dengan AWS Lambda.
- `aws-sdk-java`Permintaan dibuat dengan AWS SDK for Java.
- `aws-sdk-ruby`Permintaan dibuat dengan AWS SDK for 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, bidang ini biasanya`AWS Internal/#`, di mana `#` adalah 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.

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 pengecualian. Sebagai contoh, lihat Kode kesalahan dan contoh log pesan. Bidang ini memiliki ukuran maksimum 1 KB; konten yang melebihi batas itu terpotong.

> **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; konten yang melebihi batas itu terpotong.

Sejak: 1.0

Opsional: Salah

`responseElements`

Elemen respons untuk tindakan yang membuat perubahan (membuat, memperbarui, atau menghapus tindakan). Jika tindakan tidak mengubah status (misalnya, permintaan untuk mendapatkan atau daftar objek), elemen ini dihilangkan. Tindakan ini didokumentasikan dalam dokumentasi referensi API untuk AWS layanan yang sesuai. Bidang ini memiliki ukuran maksimum 100 KB; konten yang melebihi batas itu terpotong.

`responseElements`Nilai ini berguna untuk membantu Anda melacak permintaan dengan AWS Support. Keduanya `x-amz-request-id` dan `x-amz-id-2` berisi informasi yang membantu Anda melacak permintaan AWS Support. Nilai ini sama dengan nilai yang dikembalikan layanan sebagai respons terhadap permintaan yang memulai peristiwa, 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; konten yang melebihi batas itu terpotong.

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.

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`— Pengguna di akun Anda (root, IAM, federasi, SAMP, atau SwitchRole) masuk ke. AWS Management Console
- `AwsCloudTrailInsight`— Jika peristiwa Insights diaktifkan untuk jejak, buat peristiwa CloudTrail Insights saat CloudTrail mendeteksi aktivitas operasional yang tidak biasa seperti lonjakan penyediaan sumber daya atau ledakan tindakan (IAM). AWS Identity and Access Management

  `AwsCloudTrailInsight`event tidak menggunakan bidang berikut:

  - `eventName`
  - `eventSource`
  - `sourceIPAddress`
  - `userAgent`
  - `userIdentity`

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 AWSacara layanan. Bidang ini memiliki ukuran maksimum 100 KB; konten yang melebihi batas itu terpotong.

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 samasharedEventID, tetapi juga memiliki keunikan eventID danrecipientAccountID.

Untuk informasi selengkapnya, lihat Contoh ShareDeventid.

> **Note**
>
> sharedEventIDBidang 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 S3.

Sejak: 1.04

Opsional: Benar

eventCategory

Menampilkan kategori acara yang digunakan dalam LookupEventspanggilan.

- Untuk acara manajemen, nilainya adalahManagement.
- Untuk peristiwa data, nilainya adalahData.
- Untuk acara Wawasan, nilainya adalahInsight.

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`

Menunjukkan apakah suatu peristiwa berasal dari AWS Management Console 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

`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.

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 Untuk informasi selengkapnya tentang layanan mana yang akan mencatat detail TLSCloudTrail, lihatLayanan yang mendukung detail TLS di 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.

> **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

Kolom rekaman untuk acara Insights

Berikut ini adalah atribut yang ditampilkan dalam struktur JSON dari peristiwa Insights yang berbeda dari yang ada dalam peristiwa manajemen atau data.

`sharedEventId`

A `sharedEventID` for CloudTrail Insights event berbeda dari `sharedEventID` untuk manajemen dan tipe data CloudTrail peristiwa. Dalam acara Insights, a `sharedEventID` adalah 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.

Sejak: 1.07

Opsional: Salah

`insightDetails`

Wawasan acara saja. Menampilkan informasi tentang pemicu yang mendasari peristiwa Insights, seperti sumber peristiwa, agen pengguna, statistik, nama API, dan apakah acara tersebut merupakan awal atau akhir peristiwa Insights. Untuk informasi selengkapnya tentang isi `insightDetails` blok, lihatCloudTrail Wawasan`insightDetails`elemen.

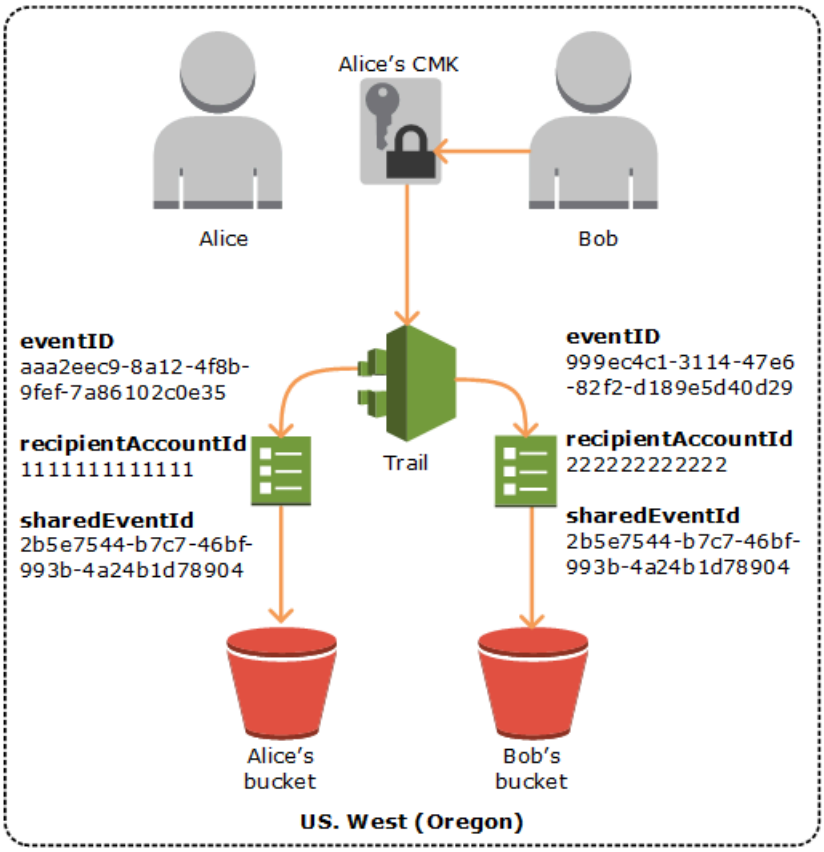
Sejak: 1.07

Opsional: Salah

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. 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.



ID acara bersama di CloudTrail Wawasan

A `sharedEventID` for CloudTrail Insights event berbeda dari `sharedEventID` untuk manajemen dan tipe data CloudTrail peristiwa. Dalam acara Insights, a `sharedEventID` adalah GUID yang dihasilkan oleh CloudTrail Insights untuk mengidentifikasi pasangan awal dan akhir peristiwa Insights secara unik. `sharedEventID`adalah umum antara awal dan akhir acara Wawasan, dan membantu menciptakan korelasi antara kedua peristiwa untuk mengidentifikasi aktivitas yang tidak biasa secara unik.

Anda dapat menganggapnya `sharedEventID` sebagai ID acara Insights keseluruhan.

Layanan yang mendukung detail TLS di CloudTrail

Mulai 28 Juni 2023, AWS mengharuskan konfigurasi Transport Layer Security (TLS) agar semua titik akhir API AWS layanan memiliki versi minimum TLS 1.2. Untuk informasi selengkapnya, lihat posting blog, TLS 1.2 untuk menjadi level protokol TLS minimum untuk semua titik akhir AWS API. `tlsDetails`Struktur di setiap CloudTrail record berisi versi TLS, cipher suite, dan nama host yang disediakan klien yang digunakan dalam panggilan API layanan, yang biasanya merupakan nama domain yang sepenuhnya memenuhi syarat (FQDN) dari titik akhir layanan. Anda kemudian

dapat menggunakan data dalam catatan untuk membantu Anda menentukan perangkat lunak klien Anda yang menggunakan versi TLS yang lebih lama, dan memperbaruinya sesuai dengan itu. Hampir setengah dari AWS layanan saat ini menyediakan informasi TLS di CloudTrail `tlsDetails` lapangan. Tabel berikut menunjukkan AWS layanan yang menampilkan informasi TLS dalam CloudTrail catatan.

> **Note**
>
> `tlsDetails`Bidang ini opsional. Ada beberapa kasus ketika `tlsDetails` bidang tidak ada dalam catatan peristiwa.

Layanan yang mendukung detail TLS
Alexa for Business
AWS Aktifkan
AWS AppConfig
AWS App Mesh
AWS App Runner
Amazon AppStream 2.0
AWS Auto Scaling
AWS Backup
AWS Backup Gerbang
AWS Billing
AWS Certificate Manager
AWS Cloud9
Direktori Cloud Amazon

Layanan yang mendukung detail TLS
AWS CloudFormation
Amazon CloudFront
AWS Cloud Map
Amazon CloudSearch
AWS CloudTrail
Amazon CloudWatch
Wawasan CloudWatch Aplikasi Amazon
CloudWatch Acara Amazon
CloudWatch Log Amazon
AWS CodeArtifact
AWS CodeBuild
AWS CodeCommit
AWS CodeDeploy
AWS CodePipeline
AWS CodeStar
AWS CodeStar Koneksi
Amazon Comprehend
Amazon Comprehend Medical
AWS Compute Optimizer
ID Suara Amazon Connect

Layanan yang mendukung detail TLS
AWS Control Tower
AWS Cost and Usage Report
AWS Cost Explorer
AWS Database Migration Service (DMS)
AWS Data Pipeline
AWS DataSync
AWS DeepRacer
AWS Device Farm
AWS Dioda
AWS Direct Connect
AWS Directory Service
Amazon DynamoDB
Akselerator Amazon DynamoDB (DAX)
Amazon Elastic Block Store (EBS)
Amazon Elastic Compute Cloud (EC2)
Connect Instans Amazon EC2
Registri Wadah Elastis Amazon (ECR)
Amazon Elastic Container Registry (ECR) Publik
Layanan Kontainer Elastis Amazon (ECS)
Amazon ElastiCache

Layanan yang mendukung detail TLS
Amazon Elastic File System (EFS)
Amazon Elastic Transcoder
AWS Elastic Load Balancing (ELB)
AWS Elastic Load Balancing (ELBV2)
AWS Elemental MediaStore
Amazon EMR
Amazon EventBridge
AWS Firewall Manager
Amazon Forecast
Amazon Fraud Detector
Amazon FSx
Amazon GameLift
AWS Global Accelerator
AWS Glue (Formasi Danau)
AWS HealthLake
AWS Identity and Access Management (IAM)
AWS Toko Identitas
Amazon Inspector
AWS IoT Analytics
AWS IoT Core

Layanan yang mendukung detail TLS
AWS IoT Events
AWS IoT Secure Tunneling
AWS IoT SiteWise
AWS IoT Wireless
Amazon Kendra
AWS Key Management Service (KMS)
Amazon Kinesis
Layanan Terkelola Amazon untuk Apache Flink
Amazon Data Firehose
Amazon Kinesis Data Streams
Amazon Kinesis Video Streams
AWS Lambda
AWS License Manager
Amazon Lightsail
Amazon Lookout for Equipment
Amazon Machine Learning
Layanan Terkelola Amazon untuk Prometheus
AWS Managed Services
AWS Marketplace Commerce Analytics
AWS Marketplace Penemuan

Layanan yang mendukung detail TLS
AWS Marketplace Entitlement Service
AWS Marketplace Metering Service
Amazon Mechanical Turk
Amazon MemoryDB for Redis
AWS Migration Hub
AWS Network Firewall
OpenSearch Layanan Amazon
AWS OpsWorks CM
AWS Organizations
Amazon Polly
Daftar Harga AWS
AWS Private Certificate Authority
AWS Proton
Amazon QuickSight
Amazon Redshift
Amazon Rekognition
Amazon Relational Database Service (RDS)
API Data Amazon Relational Database Service (RDS)
AWS Resource Groups Menandai
Amazon Route 53

Layanan yang mendukung detail TLS
Domain Amazon Route 53
Amazon Route 53 Resolver
Amazon SageMaker
Amazon SageMaker -Tepi
AWS Secrets Manager
AWS Security Token Service (STS)
AWS Service Catalog
AWS Service Quotas
AWS Shield
Amazon SimpleDB
Amazon Simple Email Service (SES)
Amazon Simple Notification Service (SNS)
Amazon Simple Queue Service (SQS)
Amazon Simple Storage Service (S3)
Amazon S3 Glacier
Amazon Simple Workflow Service (SWF)
AWS Snowball
AWS Step Functions
AWS Storage Gateway
AWS Support

Layanan yang mendukung detail TLS
AWS Systems Manager
Amazon Textract
Amazon Timestream
Layanan Streaming Amazon Transcribe
AWS Transfer Family
Amazon Translate
AWS Trusted Advisor
AWS WAF
Amazon WorkDocs
Amazon WorkMail
Alur WorkMail Pesan Amazon
Amazon WorkSpaces
AWS X-Ray

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 kredensil sementara digunakan, elemen menunjukkan bagaimana kredensil diperoleh.

Daftar Isi

- AWS STS identitas sumber

Contoh-contoh

`userIdentity`dengan kredensi pengguna IAM

Contoh berikut menunjukkan `userIdentity` elemen permintaan sederhana yang dibuat dengan kredensil 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 kredensil.

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
```

```
      }
    }
}
```

`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"
}
```

Bidang

Bidang berikut dapat muncul dalam `userIdentity` elemen.

`type`

Jenis identitasnya. 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 kredenal 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 QuickSight.
- `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.
- `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: Akses lintas akun yang diprakarsai oleh akun lain AWS

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: Akses lintas akun yang diprakarsai oleh layanan AWS

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	
`AssumedRole`	Tidak hadir	Untuk `AssumedRole` jenisnya, Anda dapat menemukan `userName` bidang `sessionCo ntext` sebagai bagian dari **`sessionIssuer`** elemen. Untuk entri contoh, lihatContoh-contoh.
`Role`	Ditentukan pengguna	`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	
`IdentityC enterUser`	Tidak hadir	`onBehalfOf` Bagian ini berisi informasi tentang ID pengguna Pusat Identitas IAM dan ARN toko

type	userName	Deskripsi
		identitas tempat panggilan dilakukan. Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Panduan AWS IAM Identity Center Pengguna.
Unknown	Bisa hadir	Misalnya, nilainya bisa berupa alias akun atau alamat email dari Akun AWS ID terkait.

> **Note**
>
> `userName`Bidang 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 ke`AssumeRole`,`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.

Opsional: Benar

`accessKeyId`

ID kunci akses yang digunakan untuk menandatangani permintaan. Jika permintaan dibuat dengan kredensil 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. Elemen ini memiliki atribut berikut:

- `creationDate`— Tanggal dan waktu ketika kredensil 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 berbasis SAML, atau pengguna yang diautentikasi melalui 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 kredensil diberikan menggunakan skema IMDS baru.

  AWS kredensil yang disediakan oleh Amazon EC2 Instance Metadata Service (IMDS) menyertakan kunci konteks ec2: IAM. RoleDelivery Kunci konteks ini memudahkan untuk menerapkan penggunaan skema baru atas resource-by-resource dasar service-by-service atau dengan menggunakan kunci konteks sebagai syarat dalam kebijakan IAM, kebijakan sumber daya, atau kebijakan kontrol AWS Organizations layanan. Untuk informasi lebih lanjut, lihat metadata instans dan data pengguna di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Opsional: Benar

`invokedBy`

Nama Layanan AWS yang membuat permintaan, ketika permintaan dibuat oleh Layanan AWS seperti Amazon EC2 Auto Scaling atau. AWS Elastic Beanstalk 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

`sessionIssuer`

Jika pengguna membuat permintaan dengan kredensil keamanan sementara, `sessionIssuer` berikan 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 kredensil 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 kredensil keamanan sementara.
- `accountId`— Akun yang memiliki entitas yang digunakan untuk mendapatkan kredensil.

Opsional: Benar

`onBehalfOf`

Jika permintaan dibuat oleh penelepon IAM Identity Center, `onBehalfOf` berikan informasi tentang ID pengguna IAM Identity Center dan ARN toko identitas tempat panggilan dilakukan. Elemen ini memiliki atribut berikut:

- `userId`— ID pengguna IAM Identity Center yang panggilan dilakukan atas nama.

- `identityStoreArn`— ARN dari toko identitas IAM Identity Center tempat panggilan dilakukan atas nama.

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

`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.

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 `saml:sub` tombol `saml:namequalifier` dan.
- 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 berbasis SAML, atau pengguna yang diautentikasi dengan menggunakan 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 `AssumeRole``AssumeRoleWithSAML`,, atau yang dibuat identitas pengguna ketika mengambil peran. `sourceIdentity`ditemukan di `requestParameters` blok AWS STS panggilan.
- `AssumeRoleWithWebIdentity`Panggilan AWS STS `AssumeRole``AssumeRoleWithSAML`,, 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 Mencatat 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"
    }
  }
}
```

CloudTrail Wawasan**`insightDetails`**elemen

AWS CloudTrail Wawasan catatan acara mencakup bidang yang berbeda dari yang lain CloudTrail peristiwa dalam struktur JSON mereka, kadang-kadang disebutmuatan. SEBUAH CloudTrail Catatan acara wawasan mencakup`insightDetails`blok yang berisi informasi tentang pemicu yang mendasari peristiwa Wawasan, seperti sumber peristiwa, identitas pengguna, agen pengguna, rata-rata historis, ataugaris dasar, statistik, nama API, dan apakah acara tersebut merupakan awal atau akhir dari acara Insights. The`insightDetails`blok berisi informasi berikut.

- **`state`**- Apakah acara tersebut merupakan acara Wawasan awal atau akhir. Nilai dapat berupa `Start` atau `End`.

  Sejak:1.07

  Opsional:Salah
- **`eventSource`**-AWStitik akhir layanan yang merupakan 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 dari jenis peristiwa. Nilai ini dapat`ApiCallRateInsight`,`ApiErrorRateInsight`, atau keduanya.

  Sejak:1.07

  Opsional:Salah

- **`insightContext`** -

  Informasi tentangAWSalat (disebutagen pengguna), pengguna dan peran (disebutidentitas pengguna), dan kode kesalahan yang terkait dengan peristiwa yang CloudTrail dianalisis untuk menghasilkan acara Wawasan. Elemen ini juga mencakup statistik yang menunjukkan bagaimana aktivitas yang tidak biasa dalam peristiwa Insights dibandingkan dengangaris dasaratau aktivitas normal.

  Sejak:1.07

  Opsional:Salah

  - **`statistics`**- Termasuk data tentanggaris dasar, atau rata-rata rata-rata panggilan ke atau kesalahan pada API subjek oleh akun yang diukur selama periode awal, tingkat rata-rata panggilan atau kesalahan yang memicu peristiwa Wawasan selama menit pertama peristiwa Wawasan, durasi, dalam menit, peristiwa Insights, dan durasi, dalam hitungan menit, dari periode pengukuran dasar.

    Sejak:1.07

    Opsional:Salah

    - **`baseline`**- 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.

      Sejak:1.07

      Opsional:Salah

    - **`insight`** -

      Untuk memulai peristiwa Insights, nilai ini adalah jumlah rata-rata panggilan API atau error 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.

      Sejak:1.07

      Opsional:Salah

- **`insightDuration`**- Durasi, dalam hitungan menit, 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 hitungan menit, 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 dari`baselineDuration`pengukuran selalu merupakan awal dari peristiwa Insights.

  Sejak:1.07

  Opsional:Salah

- **`attributions`**- Blok ini mencakup informasi tentang identitas pengguna, agen pengguna, dan kode kesalahan yang berkorelasi dengan aktivitas yang tidak biasa dan dasar. Maksimal lima identitas pengguna, lima agen pengguna, dan lima kode kesalahan ditangkap dalam acara Insights`attributions`blok, diurutkan berdasarkan rata-rata hitungan aktivitas, dalam urutan menurun dari tertinggi ke terendah.

  Sejak:1.07

  Opsional:Benar

  - **`attribute`**- Berisi jenis atribut. Nilai dapat`userIdentityArn`,`userAgent`, atau`errorCode`.
    - **`userIdentityArn`**- Blok yang muncul hingga lima besarAWSpengguna atau peran IAM yang berkontribusi pada panggilan atau kesalahan API selama aktivitas dan periode dasar yang tidak biasa. Lihat juga `userIdentity` di CloudTrail isi rekaman.

      Sejak:1.07

      Opsional:Salah

      - **`insight`**- Blok yang menampilkan hingga lima ARN identitas pengguna teratas yang berkontribusi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa, dalam urutan menurun dari jumlah panggilan API terbesar hingga terkecil. Ini juga menunjukkan jumlah rata-rata panggilan API yang dilakukan oleh identitas pengguna selama periode aktivitas yang tidak biasa.

Sejak:1.07

Opsional:Salah

- **`value`**- ARN dari salah satu dari lima identitas pengguna teratas yang berkontribusi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa.

  Sejak:1.07

  Opsional:Salah

- **`average`**- Jumlah panggilan API atau kesalahan per menit selama periode aktivitas yang tidak biasa untuk identitas pengguna di`value`bidang.

  Sejak:1.07

  Opsional:Salah

- **`baseline`**- Blok yang menampilkan hingga lima ARN identitas pengguna 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 identitas pengguna selama periode aktivitas normal.

  Sejak:1.07

  Opsional:Palsu

  - **`value`**- ARN dari salah satu dari lima identitas pengguna teratas yang berkontribusi pada panggilan API atau kesalahan selama periode aktivitas normal.

    Sejak:1.07

    Opsional:Salah

  - **`average`**- Rata-rata historis panggilan API atau error per menit selama tujuh hari sebelum waktu mulai aktivitas Insights untuk identitas pengguna di`value`bidang.

    Sejak:1.07

    Opsional:Salah

- **`userAgent`**- Blok yang muncul hingga lima teratasAWSalat yang dengannya identitas pengguna berkontribusi pada panggilan API selama aktivitas dan periode dasar yang tidak

biasa. Alat-alat ini termasukAWS Management Console,AWS CLI, atauAWSSDK. Lihat juga `userAgent` di CloudTrail isi rekaman.

Sejak:1.07

Opsional:Palsu

- **`insight`**- Blok yang menampilkan hingga lima agen pengguna teratas yang berkontribusi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa, dalam urutan menurun dari jumlah panggilan API terbesar hingga terkecil. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dicatat oleh agen pengguna selama periode aktivitas yang tidak biasa.

  Sejak:1.07

  Opsional:Palsu

  - **`value`**- Salah satu dari lima agen pengguna teratas yang berkontribusi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa.

    Sejak:1.07

    Opsional:Palsu

  - **`average`**- Jumlah panggilan API atau kesalahan yang dicatat per menit selama periode aktivitas yang tidak biasa untuk agen pengguna di`value`bidang.

    Sejak:1.07

    Opsional:Palsu

- **`baseline`**- Blok yang menampilkan hingga lima agen pengguna teratas yang berkontribusi paling besar terhadap panggilan API yang dilakukan selama periode aktivitas normal. Ini juga menunjukkan jumlah rata-rata panggilan API atau kesalahan yang dicatat oleh agen pengguna selama periode aktivitas normal.

  Sejak:1.07

  Opsional:Palsu

  - **`value`**- Salah satu dari lima agen pengguna teratas yang berkontribusi pada panggilan API atau kesalahan yang dicatat selama periode aktivitas normal.

    Sejak:1.07

Opsional:Palsu

- **`average`**- Rata-rata historis panggilan API atau error per menit selama tujuh hari sebelum waktu mulai aktivitas Insights untuk agen pengguna di`value`bidang.

  Sejak:1.07

  Opsional:Palsu

- **`errorCode`**- Blok yang menampilkan hingga lima kode kesalahan teratas yang terjadi pada panggilan API selama aktivitas dan periode dasar yang tidak biasa, dalam urutan menurun dari jumlah panggilan API terbesar hingga terkecil. Lihat juga `errorCode` di CloudTrail isi rekaman.

  Sejak:1.07

  Opsional:Palsu

- **`insight`**- Blok yang menampilkan hingga lima kode kesalahan teratas yang terjadi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa, dalam urutan menurun dari jumlah panggilan API terkait terbesar hingga terkecil. Ini juga menunjukkan jumlah rata-rata panggilan API di mana kesalahan terjadi selama periode aktivitas yang tidak biasa.

  Sejak:1.07

  Opsional:Palsu

  - **`value`**- Salah satu dari lima kode kesalahan teratas yang terjadi pada panggilan API yang dilakukan selama periode aktivitas yang tidak biasa, seperti`AccessDeniedException`.

    Jika tidak ada panggilan yang memicu peristiwa Insights yang menghasilkan kesalahan, nilai ini adalah`null`.

    Sejak:1.07

    Opsional:Palsu

  - **`average`**- Jumlah panggilan API per menit selama periode aktivitas yang tidak biasa untuk kode kesalahan di`value`bidang.

Jika nilai kode kesalahan adalah`null`, dan tidak ada kode kesalahan lain di`insight`blok, nilai dari`average`sama dengan yang di`statistics`blok untuk acara Insights secara keseluruhan.

Sejak:1.07

Opsional:Palsu

- **`baseline`**- Blok yang menampilkan hingga lima kode kesalahan teratas yang terjadi pada panggilan API yang dilakukan selama periode aktivitas normal. Ini juga menunjukkan jumlah rata-rata panggilan API yang dilakukan oleh agen pengguna selama periode aktivitas normal.

  Sejak:1.07

  Opsional:Palsu

  - **`value`**- Salah satu dari lima kode kesalahan teratas yang terjadi pada panggilan API yang dilakukan selama periode aktivitas normal, seperti`AccessDeniedException`.

    Sejak:1.07

    Opsional:Palsu

  - **`average`**- Rata-rata historis panggilan API atau error per menit selama tujuh hari sebelum waktu mulai aktivitas Wawasan untuk kode kesalahan di`value`bidang.

    Sejak:1.07

    Opsional:Palsu

Contoh**`insightDetails`**blok

Berikut ini adalah contoh dari jenis peristiwa ini`insightDetails`memblokir peristiwa Insights yang terjadi saat Application Auto Scaling API`CompleteLifecycleAction`disebut beberapa kali yang tidak biasa. Untuk contoh acara Insights lengkap, lihatCloudTrail referensi acara log.

Contoh ini berasal dari acara Insights awal, yang ditunjukkan oleh`"state": "Start"`. Identitas pengguna teratas yang memanggil API yang terkait dengan peristiwa Insights,`CodeDeployRole1`,`CodeDeployRole2`, dan`CodeDeployRole3`, ditunjukkan dalam`attributions`blokir, bersama dengan tarif panggilan API rata-rata untuk acara Insights ini,

dan garis dasar untukCodeDeployRole1peran. Theattributionsblok juga menunjukkan bahwa agen pengguna adalahcodedeploy.amazonaws.com, yang berarti identitas pengguna teratas menggunakanAWS CodeDeploykonsol untuk menjalankan panggilan API.

Karena tidak ada kode kesalahan yang terkait dengan peristiwa yang dianalisis untuk menghasilkan peristiwa Wawasan (nilainya adalahnull),insightrata-rata untuk kode kesalahan sama dengan keseluruhaninsightrata-rata untuk seluruh acara Insights, ditampilkan distatisticsblok.

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

Peristiwa non-API ditangkap oleh CloudTrail

Selain loggingAWSPanggilan API, CloudTrail menangkap peristiwa terkait lainnya yang mungkin memiliki dampak keamanan atau kepatuhan padaAWSakun atau yang mungkin membantu Anda memecahkan masalah operasional.

Topik

- AWSacara layanan
- AWS Management Console acara masuk

AWSacara layanan

CloudTrail mendukung pencatatan peristiwa layanan non-API. Peristiwa ini dibuat olehAWSlayanan tetapi tidak secara langsung dipicu oleh permintaan ke publikAWSAPI. Untuk peristiwa-peristiwa ini,`eventType`Bidang adalah`AwsServiceEvent`.

Berikut ini adalah contoh skenario dariAWSperistiwa layanan ketika kunci yang dikelola pelanggan diputar secara otomatisAWS Key Management Service(AWS KMS). Untuk informasi lebih lanjut tentang merotasi kunci KMS, lihatmerotasi kunci KMS.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
```

```
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```

AWS Management Console acara masuk

CloudTrail log mencoba untuk masuk ke AWS Management Console, Forum AWS Diskusi, dan Pusat AWS Dukungan. Semua peristiwa masuk pengguna dan pengguna root IAM, serta semua peristiwa masuk pengguna gabungan, menghasilkan catatan dalam file log. CloudTrail Untuk informasi tentang menemukan dan melihat log, lihat Menemukan file CloudTrail log Anda danMengunduh CloudTrail file log.

> **Note**
>
> Wilayah yang direkam dalam suatu `ConsoleLogin` peristiwa bervariasi berdasarkan jenis pengguna dan apakah Anda menggunakan titik akhir global atau regional untuk masuk.
>
> - Jika Anda masuk sebagai pengguna root, CloudTrail catat peristiwa di us-east-1.
> - 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` peristiwa 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, CloudTrail catat `ConsoleLogin` peristiwa di us-east-1. Ini karena proxy konsol mengalihkan kembali ke proses masuk global.
> - Jika Anda masuk dengan pengguna IAM dan menggunakan titik akhir Regional, CloudTrail mencatat `ConsoleLogin` peristiwa di Wilayah yang sesuai untuk titik akhir. Untuk informasi selengkapnya tentang AWS Sign-In titik akhir, lihat AWS Sign-In titik akhir 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 login 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 (tipe 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 ke AWS Management Console 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 AWS Management Console 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 (tipe perangkat MFA tunggal)

Berikut ini menunjukkan bahwa proses masuk memeriksa apakah otentikasi multi-faktor (MFA) diperlukan untuk pengguna IAM selama login. Dalam contoh ini, `mfaType` nilainya adalah`U2F MFA`, yang menunjukkan bahwa pengguna IAM mengaktifkan perangkat MFA tunggal atau beberapa perangkat MFA dengan tipe 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 masuk memeriksa apakah otentikasi multi-faktor (MFA) diperlukan untuk pengguna IAM selama login. Dalam contoh ini, `mfaType` nilainya 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 login `root` pengguna. Saat Anda masuk menggunakan pengguna root, CloudTrail merekam `ConsoleLogin` peristiwa di us-east-1.

Topik

- Pengguna root, berhasil masuk tanpa MFA
- Pengguna root, berhasil masuk dengan MFA
- Pengguna root, masuk tidak berhasil
- Pengguna root, MFA berubah
- Pengguna root, kata sandi diubah

Pengguna root, berhasil masuk tanpa MFA

Berikut ini menunjukkan peristiwa login 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 peristiwa login 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, masuk tidak berhasil

Berikut ini menunjukkan peristiwa login 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 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 kredensi keamanan sementara untuk mengakses AWS sumber daya melalui permintaan. `AssumeRole`

Berikut ini menunjukkan contoh peristiwa untuk permintaan enkripsi federasi. ID kunci akses asli disediakan di `accessKeyId` bidang `userIdentity` elemen. `accessKeyId`Kolom di `responseElements` berisi ID kunci akses baru jika diminta `sessionDuration` diteruskan dalam permintaan enkripsi, jika tidak maka berisi nilai ID kunci akses asli.

```
{
    "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 peristiwa login 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"
    }
}
```

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
- Update dokumentasi terbaru: 2024-04-02

Perubahan	Deskripsi	Tanggal
Menambahkan dukungan layanan	Rilis ini mendukung AWS Deadline Cloud. Untuk informasi selengkapnya, lihat Layanan AWS topik untuk CloudTrail.	April 2, 2024
Ditambahkan fungsionalitas	Versi AWS CloudTrail acara sekarang 1.10. Untuk informasi selengkapnya, lihat CloudTrail merekam konten.	Maret 26, 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 CloudTrai l data pada AWS X-Ray jejak dan node AWS Systems Manager terkelola dengan menggunakan pemilih acara	7 Maret 2024

	lanjutan. Untuk informasi selengkapnya, lihat Peristiwa data.	
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 ListInsightsMetricDatadi Referensi AWS CloudTrail API.	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.	Desember 20, 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.	Desember 20, 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 acara.	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 CloudTrail 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 CloudTrail konsol AWS CLI, atau operasi API. UpdateEve ntDataStore Untuk informasi selengkapnya tentang opsi AWS CloudTrail penetap an 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 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 SageMaker titik akhir Amazon 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 tutorial CloudTrail Lake baru untuk menunjukkan cara membuat penyimpanan data acara, melihat dasbor CloudTrail Danau, menyalin peristiwa jejak ke penyimpanan data acara, melihat dan menjalankan kueri sampel, dan menyimpan hasil kueri ke bucket Amazon S3 menggunakan file. AWS Management Console Untuk informasi lebih lanjut, lihat Tutorial 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 CloudTrail.	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-results perintah. Untuk informasi selengkapnya, lihat Memvalidasi 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

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 CloudTrail Processing Library: 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 SageMaker fitur Amazon dengan menggunak an pemilih acara lanjutan. 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.	Desember 15, 2022
Ditambahkan fungsionalitas	Sekarang Anda dapat mencatat peristiwa CloudTrai l data di komponen uji coba eksperimen SageMaker metrik Amazon dengan menggunak an pemilih peristiwa lanjutan. Untuk informasi selengkapnya, lihat Mencatat peristiwa data.	Desember 15, 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 menjalankan 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.	22 Oktober 2022
Ditambahkan fungsionalitas	Anda sekarang dapat menyalin peristiwa CloudTrail 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
Dokumentasi diperbarui	Menambahkan daftar layanan yang melaporkan detail TLS ke CloudTrail. Untuk informasi selengkapnya, lihat Layanan yang mendukung detail TLS di CloudTrail.	19 Juli 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 Akses hanya-baca.	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 AWS Management Console sesi di mana klien proxy digunakan. Untuk acara ini, CloudTrail ganti nilai `userAgent` dan `sourceIPAddress` bidang dengan`AWS Internal`. CloudTrail membuat 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 Menyuntikan 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 Grafana Terkelola Amazon dan Layanan Terkelola Amazon 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 di 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
Ditambahkan fungsionalitas	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 selengkapnya, lihat peristiwa Logging Insights untuk jejak.	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.	Juli 15, 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	AWS KMS Tindakan volume tinggi sepertiEncrypt,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 sepertiDisable, Delete danScheduleKey .	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 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 CloudTrail 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 CloudTrail Didukung.	17 Oktober 2019
Menambahkan dukungan layanan	Rilis ini mendukung Amazon Translate. Lihat Layanan dan Integrasi yang AWS CloudTrail 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 Kebijakan Berbasis Identitas.	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 diperbarui dengan informasi tentang keamanan untuk CloudTrail. 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 AppStream 2.0. Lihat Layanan dan Integrasi yang AWS CloudTrail Didukung.	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 CloudTrail 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 yang 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 sebelumnya

Tabel berikut menjelaskan riwayat rilis dokumentasi AWS CloudTrail sebelum 29 Juni 2018.

Perubahan	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 Billing and Cost Management. 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	Pemutakhiran ini mendukung rilis patch berikut untuk CloudTrail Processing Library: • Perbarui referensi file.jar di panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library -1.1.2.jar. Untuk informasi selengkapnya, lihat Menggunakan CloudTrail Perpustakaan Pengolahan dan Pustaka CloudTrail Pemrosesan di GitHub.	16 Mei 2018
Menambahkan dukungan layanan	Rilis ini mendukung AWS Billing and Cost Management. Lihat CloudTrail layanan dan integrasi yang didukung.	7 Juni 2018

Perubahan	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	Pemutakhiran ini mendukung rilis patch berikut untuk CloudTrail Processing Library: • Perbarui referensi file.jar di panduan pengguna untuk menggunakan versi terbaru, aws-cloudtrail-processing-library -1.1.2.jar. Untuk informasi selengkapnya, lihat Menggunakan CloudTrail Perpustakaan Pengolahan 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

Perubahan	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. 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

Perubahan	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 Pencatatan peristiwa data.	30 November 2017
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung pencatatan peristiwa data untuk AWS Lambda fungsi. Untuk informasi selengkapnya, lihat Pencatatan 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 CloudTrail Perpustakaan Pengolahan 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

Perubahan	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 Pencatatan 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. Untuk informasi selengkapnya, lihat Bagaimana cara CloudTrail kerja.	14 Agustus 2017

Perubahan	Deskripsi	Tanggal Rilis
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
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

Perubahan	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 CloudTrail Perpustakaan Pengolahan 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

Perubahan	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, lihatPemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.	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 QuickSight. 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.	11 April 2017
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

Perubahan	Deskripsi	Tanggal Rilis
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, dan AWS Managed Services dalam riwayat aktivitas CloudTrail API.	26 Januari 2017
Menambahkan fungsionalitas	Rilis ini mendukung integrasi dengan file AWS Health Dashboard. Anda dapat menggunakan file AWS Health Dashboard untuk mengidentifikasi apakah jejak Anda tidak dapat mengirimkan log ke topik SNS atau bucket S3. Hal ini dapat terjadi jika ada masalah dengan kebijakan untuk bucket S3 atau topik SNS. AWS Health Dashboard 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

Perubahan	Deskripsi	Tanggal Rilis
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 peristiwa CloudTrail manajemen terbaru di CloudTrail 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
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

Perubahan	Deskripsi	Tanggal Rilis
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
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 fungsionalitas dan dokumentasi	Rilis ini mendukung pencatatan peristiwa AWS layanan non-API. Untuk informasi selengkapnya, lihat AWSacara layanan.	September 23, 2016
Menambahkan fungsionalitas 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

Perubahan	Deskripsi	Tanggal Rilis
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-selatan-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 Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.	6 Mei 2016
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 Support. 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

Perubahan	Deskripsi	Tanggal Rilis
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
Menambahkan dukungan layanan	Rilis ini mendukung Amazon GameLift (Amazon GameLift). 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

Perubahan	Deskripsi	Tanggal Rilis
Menambahkan fungsionalitas dan dokumentasi	Rilis ini mendukung CloudTrail pengaktifan di semua Wilayah dan dukungan untuk beberapa jalur per Wilayah. Untuk informasi selengkapnya, lihat Bagaimana CloudTrail berperilaku regional dan global?.	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 dengan AWS KMS kunci (SSE-KMS), Memvalidasi CloudTrail integritas berkas log, dan Memperbarui jejak.	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.	16 September 2015
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

Perubahan	Deskripsi	Tanggal Rilis
Menambahkan dukungan layanan	Rilis ini mendukung CloudWatch Log di Wilayah AS Barat (California Utara). Lihat catatan CloudTrail rilis. Untuk informasi selengkapnya tentang CloudTrai l dukungan untuk pemantauan CloudWatch Log, lihatPemantauan CloudTrail Log Files dengan Amazon CloudWatch Log.	19 Mei 2015
Menambahkan dukungan layanan	Rilis ini mendukung AWS 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
	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 CloudTrai l Acara.	12 Maret 2015

Perubahan	Deskripsi	Tanggal Rilis
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
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 (AS-Barat)). Lihat CloudTrail Daerah yang didukung.	Desember 16, 2014
Menambahkan dukungan layanan	Rilis ini mendukung Amazon S3 Glacier. Lihat CloudTrail layanan dan integrasi yang didukung.	11 Desember 2014

Perubahan	Deskripsi	Tanggal Rilis
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,Pemantauan CloudTrail Log Files dengan Amazon CloudWatch Log, telah ditambahk an ke panduan. Ini menjelaskan cara menggunakan Amazon CloudWatch Logs untuk memantau peristiwa CloudTrail log.	10 November 2014
Dokumentasi baru	Bagian baru,Menggunakan CloudTrail Perpustak aan Pengolahan, 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-centra l-1 (Eropa (Frankfurt)). Lihat CloudTrail Daerah yang didukung.	23 Oktober 2014
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

Perubahan	Deskripsi	Tanggal Rilis
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 AWS Management Console acara masuk.	Juli 24, 2014
Penambahan konten baru	Elemen EventVersion untuk rilis ini telah ditingkatkan ke versi 1.02 dan tiga bidang baru telah ditambahkan. Lihat CloudTrail isi rekaman.	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-tengga ra 1 (Asia Pasifik (Singapura)), ap-timur laut-1 (Asia Pasifik (Tokyo)), sa-timur-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 AWS OpsWorks. Lihat CloudTrail layanan dan integrasi yang didukung.	Juni 5, 2014
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-barat-1 (AS Barat (California Utara)), eu-barat-1 (Eropa (Irlandia)), ap-tenggara 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

Perubahan	Deskripsi	Tanggal Rilis
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 AWS 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 AWS CloudFormation. Lihat CloudTrail layanan dan integrasi yang didukung.	Maret 7, 2014
Panduan baru	Rilis ini memperkenalkan AWS CloudTrail.	November 13, 2013

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

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